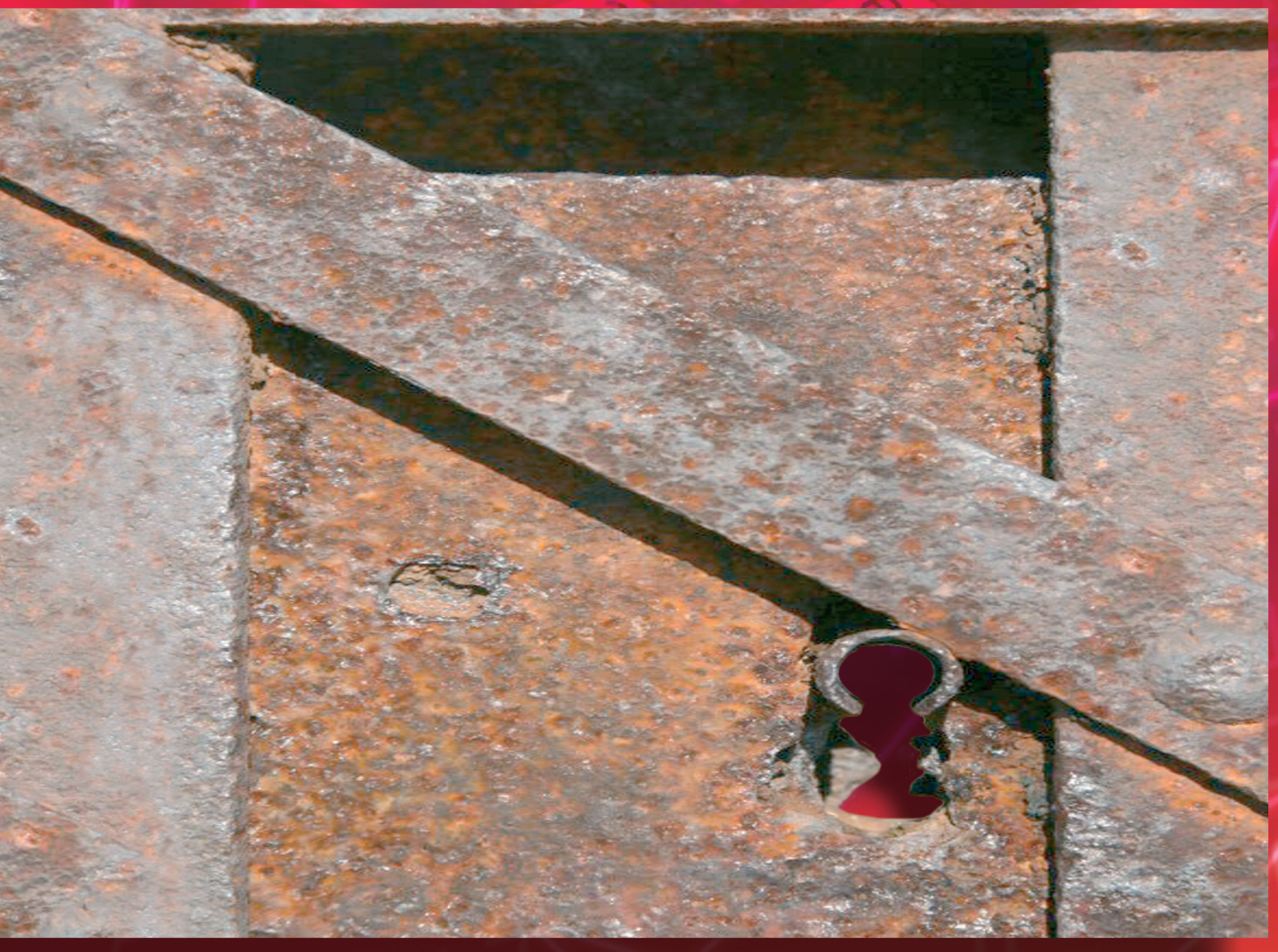
الاتحاد الدولي للاتصالات

دليل الأمن السيبراني للبلدان النامية

طبعة 2007



الاتحاد الدولي للاتصالات

الاتحـــــــــــاد الـــــــــــدولي للاتصـــــــــــالات

دليل
الأمن السيبراني
للبلدان النامية

طبعة 2007

ولا تعني أي من التسميات والتصنيفات المستعملة في هذا المطبوع ضمناً أي رأي للاتحاد الدولي للاتصالات فيما يتعلق بالوضع القانوني أو أي وضع آخر لأي إقليم، مصادقة على أي من الحدود أو قبول لها. وعندما تظهر اسم "بلد" في هذه المنشورة فإنه يشمل البلد والأراضي.

إخلاء مسؤولية

إن الإشارة إلى بلدان، شركات، منتجات، مبادرات محددة أو خطوط توجيهية لا تعني حتماً بأي حال من الأحوال أن الاتحاد الدولي للاتصال يصادق على، أو يوصي بالبلدان، الشركات، المنتجات، المبادرات والمبادئ التوجيهية المعنية دون غيرها المماثلة لها والتي لم يرد ذكرها، والآراء المعرب عنها في هذه المنشورة هي آراء المؤلف ولا يشترك فيها الاتحاد الدولي للاتصالات.

تقديـــم

جمعت القمة العالمية لمجتمع المعلومات بمرحلتيها في جنيف وتونس المنظمات الدولية والحكومات وشركات الأعمال والمجتمع المدني للاتفاق على رؤية مشتركة لمجتمع المعلومات.

ومع ذلك فإننا لا نستطيع أن نترجم هذه الرؤية المشتركة إلى واقع ملموس لدى جميع شعوب العالم إلى إذا استطعنا أن نؤمِّن الصفقات الإلكترونية وأن نحمي البنية التحتية للمعلومات، وهي تتسم بأهمية حاسمة، وأن نصون أنظمة المعلومات والبيانات التي تعتمد عليها شركات الأعمال والمواطنون والحكومات.

وتشمل التحديات التي يجب أن نواجهها مجتمعين عدم كفاية حلول الأمن السيبراني وعدم وجود فهم مشترك للقضايا والحاجة إلى معالجة هذه المشكلة على الصعيد العالمي.

والاتحاد الدولي للاتصالات ملتزم بموجب دوره كجهة تنسيق/تسهيل بشأن خط العمل جيم5 للقمة العالمية – *بنـــاء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات*، بأن يعمل مع جميع أصحاب المصلحة للتوصل إلى فهـــم مشترك للتحديات ولتعبئة مواردنا الجماعية لبناء إطار عالمي لتحقيق الأمن والطمأنينة.

وأنا أدعوكم جميعاً إلى الانضمام إلينا في جهودنا لتحويل رؤيتنا لبناء مجتمع معلومات عالمي وآمن إلى واقع ملموس.

الدكتور حمدون إ. توريه

الأمين العام
للاتحاد الدولي للاتصالات

تمهيـــد

كان من شأن ظهور مجتمع معلومات عالمي بلا حدود أن أتاح فرصاً جديدة لجميع بلدان العالم، حيث تؤدي التكنولوجيا دوراً متزايد الأهمية في التنمية الاجتماعية والاقتصادية. وقد أصبحت الخدمات في مجالات الصحة والتعليم والأعمال التجارية والتمويل والإدارة العامة ممكنة بفضل تطبيقات تكنولوجيا المعلومات والاتصالات.

وتنشأ عن تكنولوجيا المعلومات والاتصالات أيضاً تحديات جديدة يجب معالجتها إذا كان لنا أن نؤمن إجراء عمليات الصحة الإلكترونية ونمكن المواطنين من النفاذ إلى خدمات الحكومة الإلكترونية ونتيح الثقة اللازمة لإجراء الأعمال التجارية الإلكترونية وصفقات التجارة على الخط وأن نحافظ على سلامة ما لدينا من أنظمة وموارد تكنولوجيا المعلومات.

ولذلك كانت إقامة حلول كافية على صعيد الأمن والثقة تمثل واحداً من التحديات الرئيسية التي يتعين أن يعالجها مكتب تنمية الاتصالات في الاتحاد الدولي للاتصالات في متابعة جهوده لمساعدة البلدان على استعمال الاتصالات وتكنولوجيا المعلومات والاتصالات.

واختفاء الحدود من مجتمع المعلومات يعني أيضاً أن دراسة الحلول تقتضي فهماً مشتركاً بين جميع الأمم للإمكانيات التي توفرها تطبيقات تكنولوجيا المعلومات والاتصالات الآمنة والتحديات التي تواجهنا في بناء الثقة والأمن. ولذلك كان حتماً علينا، بالإضافة إلى العمل على سد الفجوة الرقمية، أن نبذل الجهود أيضاً لسد الفجوة المعرفية برفع الوعي الأساسي وبناء القدرات البشرية والمؤسسية.

والغرض من هذا الدليل هو تزويد البلدان النامية بأداة تسمح لها بفهم أفضل لبعض القضايا المتصلة بأمن تكنولوجيا المعلومات، وتقديم أمثلة للحلول التي اتبعتها بلدان أخرى للتغلب على هذه المشاكل. ويشير الدليل أيضاً إلى مطبوعات أخرى تتضمن مزيداً من المعلومات المحددة عن الأمن السيبراني. وليس المقصود من هذا الدليل أن يكون وثيقة جامعة أو تقريراً كاملاً عن هذا الموضوع ولكن المقصود منه بالأحرى أن يكون ملخصاً للمشاكل الرئيسية التي تواجهها الآن البلدان التي ترغب في الانتفاع بفوائد مجتمع المعلومات.

وقد اختيرت محتويات هذا الدليل للوفاء باحتياجات البلدان النامية، وخاصة أقل البلدان نمواً، من ناحية استعمال تكنولوجيا المعلومات والاتصالات لتقديم خدمات أساسية في مختلف القطاعات، مع مواصلة الالتزام بتطوير الإمكانات المحلية وزيادة الوعي بين جميع أصحاب المصلحة.

ولتجنب أي ازدواج في معالجة هذه الموضوعات، أخِذ في الاعتبار العمل الذي سبق إنجازه في إطار لجنة الدراسات 17 لقطاع تقييس الاتصالات عند صياغة محتوى هذا المنشور، كما أخِذت في الاعتبار أيضاً الدراسات والمنشورات الأخرى التي سبق إعدادها في هذا الميدان.

سامي البشير المرشد

مدير

مكتب تنمية الاتصالات

موجز تنفيذي

إن القضايا الاجتماعية، والسياسات العامة، والقضايا البشرية: من أي زاوية ينظر إليها الإنسان، ومهما كانت التسميات (أمن تكنولوجيا المعلومات، أمن الاتصالات)، فإن الأمن السيبراني يلمس أمن الثروة الرقمية والثقافية للناس، والمنظمات والبلدان. فالتحديات المعنية معقدة، كما أن التصدي لها يحتاج إلى وجود إرادة سياسية لوضع وتنفيذ استراتيجية لتنمية البنى الأساسية والخدمات الرقمية التي تشمل استراتيجية للأمن السيبراني قابلة للتحقق منها ويسيرة الإدارة وفعالة ومتماسكة.

إن الحصول على مستوى لأمن المعلومات كافٍ لمواجهة مخاطر التكنولوجيا والمعلومات أمر ضروري للأداء السليم للحكومات والمنظمات. كما أن الاستخدام الشائع والواسع للتكنولوجيات الرقمية يسير يداً بيد مع الاعتماد المتزايد على تلك التكنولوجيات والاعتماد المتبادل من جانب البنى التحتية الحرجة. وهذا من شأنه أن يهدد أداء المؤسسات على نحو لا يستهان به، وربما أدى إلى تعريضها للخطر بل وربما إلى تقويض سيادة الدولة.

إن هدف الأمن السيبراني هو المساعدة على حماية أصول المنظمات ومواردها من النواحي التنظيمية، والبشرية، والمالية، والتقنية والمعلوماتية بحيث يسمح لها بمواصلة مهمتها. والهدف النهائي هو ضمان عدم تضررها ضرراً دائماً. وهذا يتمثل في تقليل احتمالات تجسد أي تهديد، والحد من الضرر الناجم أو سوء الأداء، وضمان استعادة العمليات العادية لحالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة – في أعقاب وقوع حادث أمني.

وتشمل عملية الأمن السيبراني المجتمع بأسره، من حيث يكون كل فرد فيه معنياً بتنفيذها. ويمكن دعم ذلك بتطوير مدونة سلوك سيبرانية لأجل الاستخدام السليم لتكنولوجيا المعلومات والاتصالات، وإعلان سياسات أمن واقعية تقنن المعايير التي يكون متوقعاً من مستخدمي الأمن السيبراني (الكيانات والشركاء والموردون) الوفاء بها.

ولإنشاء عملية أمن سيبراني، يكون من المهم التحديد الدقيق للأصول والموارد اللازمة للوقاية الفعالة. ويستلزم ذلك نهجاً عالمياً للأمن، نهجاً متعدد التخصصات وشاملاً إذ لا يصلح الأمن السيبراني في عالم يسوده التسيب ويعتنق الإباحية. والمطلوب هو مجموعة من المبادئ الأساسية للسلوك الأخلاقي، والمسؤولية والشفافية المتجسدة في إطار قانوني مناسب، ومجموعة عملية من الإجراءات والقواعد. ويجب إنفاذ تلك المبادئ محلياً، بالطبع، ولكن ينبغي أيضاً تطبيقها عبر المجتمع الدولي وأن تكون متوافقة مع التوجيهات الدولية القائمة.

ولتفادي إتاحة الفرص أمام تنامي الجريمة، يجب على البنى التحتية للاتصالات أن تشتمل على تدابير أمن مناسبة ذات طبيعة تقنية وقانونية مناسبة. ويمكن للهجمات عبر الفضاء السيبراني أن تتخذ أشكالاً كثيرة: الاختطاف السري لنظام، رفض تقديم الخدمة، تدمير أو سرقة بيانات حساسة، اقتحام المتسللين للشبكة، كَسْرْ حماية البرمجيات، الفركنة أو التنصت الإلكتروني (phreaking) (والذي يشمل التخريب واختطاف المبادلات الهاتفية وأكثر من ذلك). وتقع تكلفة ذلك في الغالب الأعم على عاتق الضحايا، أي المنظمات والأفراد المستهدفين.

وتمثل الاتصالات، باعتبارها نظاماً، (سواء البنى التحتية أو الخدمات) تحدياً أمنياً مشابهاً إلى حد بعيد للتحدي الذي تمثله موارد تكنولوجيا المعلومات. وينبغي ملاحظة وجود نفس العقبات التقنية والتنظيمية والبشرية في محاولة مواجهة هذا التحدي. وحماية المعلومات وهي في حالة الانتقال أمر ضروري، وإن كانت غير كافية في حد ذاتها حيث إن درجة التعرض تزداد بمجرد دخول المعلومات مرحلة التجهيز والخزن. ومن ثم يجب النظر إلى الأمن السيبراني من منظور شامل. فالحلول التقنية الأمنية البحتة لا يمكن أن تعوض عن غياب إدارة متماسكة وصارمة للاحتياجات والإجراءات والتدابير والأدوات الأمنية. ذلك أن الاندفاع المتعجل وغير المنظم للحصول على أدوات الأمن من شأنه أن يعوق الاستخدام، ويضر بالعمليات وينال من أداء أنظمة تكنولوجيا المعلومات. إن أمن تكنولوجيا المعلومات

السليم هو مسألة إدارية، وأن الأدوات والخدمات ذات الصلة مرتبطة بإدارة تشغيل النظام. فمثلاً تجفير البيانات بغرض حمايتها أثناء الإرسال عملية لا فائدة منها إذا كانت ستخزن لاحقاً بطريقة غير أمنية. وبالمثل، فإن إنشاء نظام أمني مثل "حائط النيران" سيكون قليل القيمة إذا سُمِحَ للتوصيلات أن تتجاوز هذا النظام.

وحتى يمكن للأنشطة القائمة على معالجة المعلومات أن تنمو وتضيِّق الفجوة الرقمية، فإن ذلك يستلزم:

- بنى تحتية موثوقة وآمنة (ذات نفاذية للخدمات وتوافر واعتمادية واستمرارية لتلك الخدمات)؛
- سياسات لخلق الثقة؛
- إطاراً قانونياً مناسباً؛
- سلطات قضائية وشرطية متمرسة بالتكنولوجيات الجديدة، وقادرة على التعاون مع نظيراتها لدى البلدان الأخرى؛
- أدوات الإدارة الأمنية للمعلومات وإدارة المخاطر؛
- أدوات أمنية قادرة على خلق الثقة في التطبيقات والاستخدامات المقدمة (المعاملات التجارية والمالية، الصحة الإلكترونية، الحكومة الإلكترونية، التصويت الإلكتروني، إلخ) وفي إجراءات حماية حقوق الإنسان وبخاصة سرية البيانات الشخصية.

إن حُسْن سدانة أصول المعلومات الرقمية، وتوزيع السلع غير الملموسة، واستغلال المحتوى وتضييق الفجوة الرقمية كلها أمثلة للمشاكل الاقتصادية والاجتماعية التي لا يمكن تناولها فقط بالنظر إلى الجانب التكنولوجي من أمن تكنولوجيا المعلومات. إن إبداء استجابة تراعي الأبعاد البشرية والقانونية والتكنولوجية لاحتياجات أمن البنية التحتية الرقمية واحتياجات المستخدمين، يمكن أن يساعد على تعزيز الثقة، وأن يؤدي إلى النمو الاقتصادي الذي يفيد المجتمع قاطبة.

كيـــف تقـــرأ هـــذا الدليـــل

يشكل دليل الأمن السيبراني مدخلاً إلى هذا الموضوع المهم، ويؤكد التغييرات التي صاحبت قدوم البيانات الرقمية، والتمثيل الافتراضي للمعلومات والاستخدام واسع النطاق لشبكات الاتصالات. ويعرض الدليل المخاطر التي ينطوي عليها نمو المجتمعات لأجل إعطاء فكرة عن حتمية الأمن في عالم تكنولوجيا المعلومات والاتصالات (الأمن السيبراني).

ويركز الجزء الأول على احتياجات الأمن السيبراني، ويوجز بعض عناصر الحلول. ويخضع مفهوم أمن البنية التحتية للاتصالات للتحليل في ضوء نقاط الضعف التي لوحظت وأوجه النقص في أمن تكنولوجيا المعلومات والاتصالات. فمن خلال استقاء الدروس المستفادة من فحص أفضل الممارسات، والواقع اليومي للأمن على الإنترنت، والخبرة التي اكتسبها المجتمع الدولي، يعرف الدليل باحتياجات الأمن السيبراني لدى البلدان النامية.

ويتم تحليل أبعاد الإدارة، والسياسات العامة، والأبعاد الاقتصادية والاجتماعية والقانونية للأمن السيبراني. ويقدم الدليل توصيات عامة تتعلق بالنفاذ إلى البنى التحتية للاتصالات، بهدف التحكم في المخاطر – سواء كانت جنائية المنشأ أم لا – وخلق الثقة في الخدمات الإلكترونية التي هي محرك مهم للتنمية الاقتصادية.

ويتناول الجزء الثاني مشكلة مكافحة الجريمة السيبرانية. وهو يبحث العناصر التي تشجع النشاط الإجرامي بهدف كشف حدود النهج الحالية نحو الأمن ومكافحة الجريمة السيبرانية وكذلك بيان مدى تعقد هذه المشكلة التي تواجهنا وأبعادها.

كما يعرض الدليل مختلف المخالفات والجرائم التي يمكن اقترافها عبر الإنترنت مع التركيز على منظور الجريمة الاقتصادية. ويتم تحليل السلوك الإجرامي الملاحظ وتحليل سمات المتسللين الإجراميين، وعرض وصف عام للهجمات والبرامج المسيئة. ويقدم الدليل بعض الخطوط التوجيهية وتحليل بروفيل المتسللين الإجراميين في محاولة للإعداد لمواجهة تهديدات الجريمة السيبرانية.

ويستعرض الجزء الثالث بعض الأساسيات الضرورية لعالم الاتصالات ويقترح نهجاً وظيفياً ونظرة شاملة نقدية لأدوات أمن البنية التحتية.

ويصف الجزء الرابع نهجاً شاملاً تجاه الأمن السيبراني يراعي الجوانب المختلفة القانونية للتكنولوجيات الحديثة، ويوجز الأهداف المحتملة من وضع حلول أمنية للبنية التحتية للاتصالات.

وفي نهاية دليل الأمن السيبراني سوف يجد القارئ مسرداً لمصطلحات الأمن ومجموعة من المراجع المهمة والوثائق الأخرى.

شكر وعرفان

يود مكتب تنمية الاتصالات لدى الاتحاد الدولي للاتصالات في أن يعرب عن امتنانه لسوانغ غيرناوتي-هيلي وأن يوجه لها ولزملائها الشكر لما قدموه من دعم، وبخاصة محمد علي صفاقصي، وايغلي تاشي، وسارة بن لاغا، وهند منظور، وآرنود دوفور (استشاري استراتيجيات الإنترنت).

ويستفيد هذا الكتيب من المعلومات والدراسات التي قدمها العديد من المنظمات، ونخص بالذكر منظمات أمن الحاسوب "كلوسيف" (*Club de la sécurité informatique français*) وفرقة طوارئ الحاسوب والاستجابة لها "Cert". فهي تستحق منا الامتنان الخالص.

و لم يكن إعداد هذا الكتيب ليتم لولا التعاون الممتاز من جانب أعضاء وحدة الاستراتيجيات الإلكترونية لدى الاتحاد الدولي للاتصالات وبخاصة الكسندر نتوكو. ونرغب كذلك في أن نعرب عن تقديرنا لرينيه زبندن موسلين (قسم تجهيز المنشورات لدى الاتحاد الدولي للاتصالات) والفريق العامل معها لما قدموه من عمل لإصدار دليل الأمن السيبراني.

جـــدول المحتـــويات

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الجـــزء I

الأمن السيبراني: التحديات والسياق والحلول

القسم 1.I – الفضاء السيبراني ومجتمع المعلومات

1.1.I الرقمنة

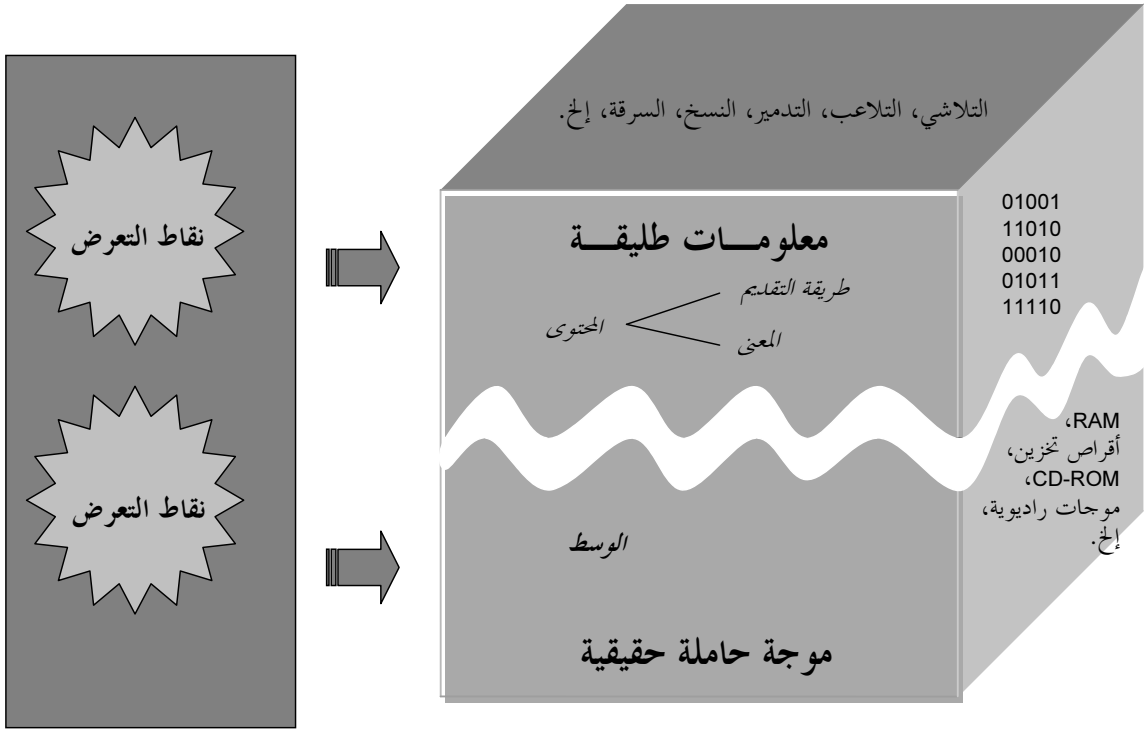
تُحدث تكنولوجيا المعلومات تحولاً في الأسلوب الذي نفكر به في كل شيء ونفعل به أي شيء في حياتنا تقريباً. فهي تستحدث تغييرات هيكلية مهمة عن طريق السماح لنا بنمذجة *الأشياء المحسوسة* من جميع الأنواع على شكل معلومات، ومن وثم تصبح طيعة للمعالجة الإلكترونية.

1.1.1.I المعلومات الرقمية

تخلق الرقمنة صورة رقمية لشيء من الواقع (نسخة افتراضية من الشيء المحسوس). ويمكن لكل المعلومات، مهما كانت طبيعتها – سواء كانت صوتاً، أو بيانات أو صورة – أن تُرَقْمَن وأن تُقَدم بصورة موحدة.

وتصبح المعلومات المرقمنة طليقة غير مادية، أي لا تَعُدْ مرتبطة بالوسط الذي تقدم به أو تخزن به. وتضيف المعلومات في حد ذاتها (المحتوى) قيمة، لأن تكلفة تقاسمها وخزنها تقل كثيراً عن تكلفة إنتاجها (الشكل 1.I). يضاف إلى ذلك، أن البيانات يمكن أن تُمركز وأن تُعالج في عدة أماكن في آن واحد. إن إمكانية استخراج نُسخ مطابقة (*إلى ما لا نهاية*) تجعل فكرة البيانات "الأصلية" بلا جدوى وتحمل في ثناياها تداعيات مقلقة محتملة بالنسبة لفكرة حماية حقوق النشر أو التأليف.

الشكل 1.I – المحاكاة الافتراضية والمعلومات الرقمية



2.1.1.I التكنولوجيا الرقمية

إن التكنولوجيا الرقمية، عن طريق توحيد إنتاج البيانات ومعالجتها ونقلها، قد جعلت من المستطاع إنشاء سلسلة معلومات رقمية متصلة. فبالائتلاف مع تقانات دمج البيانات، يخلق هذا التقارب الرقمي فرصاً لأوجه التآزر بين

تكنولوجيا المعلومات والاتصالات والوسائل السمعية البصرية. وآية ذلك ظاهرة الشبكة الدولية للمعلومات (الإنترنت)، وهكذا تحققت الثورة التكنولوجية الحقيقية بفضل رقمنة المعلومات، وتجاوزت نتائجها عالم الاتصالات بكثير.

ويؤثر هذا البعد الجديد لمعالجة المعلومات في جميع مجالات جهد وعمل الإنسان. ذلك أن كلاً من تحديد قيمة الإنتاج وأنماطه، ابتداءً من تصميم المنتج وانتهاءً بالتوزيع قد تطورا خلال السنوات الأخيرة. وأدى ذلك إلى إعادة تنظيم سلسلات القيم فيما بين مختلف الأطراف الفاعلة في الاقتصاد.

3.1.1.I البنية التحتية والمحتوى

لقد غدا التحكم في سلسلة المعلومات الرقمية، أي في البنية التحتية والمحتوى هو التحدي الرئيسي في القرن الحادي والعشرين. فالسوق الجديدة، المفتوحة أمام الجميع، تتسم بالحشد غير المسبوق لجميع الناشطين في الاقتصاد العالمي، كمشغلي الاتصالات، ومشغلي البرق، ومصنعي أجهزة الحاسوب والبرمجيات، ومذيعي التلفزيون وغيرهم.

أما التحدي الاقتصادي الجديد أمام التنظيم في يومنا هذا فهو ذلك الذي ينشأ عن المنافسة الحرة غير المقيدة، وعن إعادة ترتيب الأدوار والنشاطات.

فعندما طَبَع غوتنبرغ أول كتاب له، لم يكن لديه من سبيل ليتخيل الأصداء التي سيطلقها اختراعه هذا في عالم الصناعة، وكانت الأصداء في تلك الحالة تمثل الخطوة الأولى على الطريق إلى الأتمتة الصناعية. وقد حدث شيء مماثل في نهاية الستينات من القرن العشرين عندما بدأت الجامعات وجهات الاستخدام العسكرية، وكل منها مدفوع بأهدافه الخاصة المتعارضة على ما يبدو، تنشئ شبكة اتصالات قُدر لها أن تصبح شبكة الاتصالات العالمية. وقد كانوا يتصرفون، مثل أسلافهم في القرن الخامس عشر، دون إدراك كامل للنتائج التي سيتمخض عنها ابتكارهم هذا. أما اليوم، فإن الفضاء السيبراني يؤذِنُ بانتقال المجتمعات إلى عصر المعلومات.

2.1.I ثورة المعلومات

إن ثورة المعلومات تحدث تغييرات عميقة الغور في الطريقة التي تتم بها معالجة المعلومات وتخزينها. وهي تغير الطريقة التي تؤدي بها المنظمات، بل المجتمع ككل في حقيقة الأمر، وظائفه. فهي ليست الابتكار التقني الوحيد الذي حدث خلال السنوات الأخيرة، وإنما تبرز بسبب تأثيرها على معالجة المعلومات، ومن ثَم على المعارف. ولأن ثورة المعلومات تؤثر في الآليات التي تُخْلَقُ بها المعارف وبها يتم تقاسمها، فيمكن اعتبارها منبعاً للابتكار في المستقبل لا ينبغي استبعاد البلدان النامية عنه.

إن ثورة المعلومات وتكنولوجيات الاتصالات تؤدي إلى ثورة حقيقية في كيفية تفكيرنا في المبادلات الاقتصادية والاجتماعية والثقافية. وهي تزودنا كذلك بنموذج جديد لتكنولوجيا المعلومات يستند إلى الشبكة التي يحتاج أمن انسياب المعلومات عبرها إلى تأمين حتى يمكن تطوير الاستخدامات التطبيقية الجديدة التي ستزيد من فعالية التنظيمات. إذْ لا يمكن لأي شكل من أشكال النشاط الاقتصادي أن يبقى بدون المبادلات وبدون التفاعل بين المشاركين فيه، ولا يمكن أن يحدث أي تبادل للمعلومات دون وجود نوع من ضمانات الأمن الأساسية. ولا يمكن تخطيط أي خدمة بدون مراعاة نوعية تلك الخدمة. غير أنه يجب علينا، مع ذلك، أن نضع نصب أعيننا أن نجاح اتصال ما يعتمد على قدرة الأطراف الضالعة فيه على التعامل مع العقبات التقنية وإدارة العادات التي تدخل في أي مبادلة للمعلومات.

1.2.1.I الابتكار والتطوير

إذا كان للمنظمات والبلدان أن تحافظ على بقائها وأن توطد أقدامها كأطراف فاعلة ذات نفس طويل في معترك البيئة التنافسية الجديدة، فعليها أن تُركز على القدرات الإبداعية وعلى سرعة التكيف، يساندها في ذلك نظام معلومات متين وآمن.

وتنفتح مجالات جديدة للنشاط عن طريق تنويع الاتصالات والإمكانيات التي تخلقها تكنولوجيا المعلومات الموسعة، والتي ينبغي أن تعود منافعها على البلدان النامية أيضاً.

إن التحسينات التكنولوجية والاقتصادية التي حققها انتشار بنى تحتية أساسية مضمونة للاتصالات لتحمل الكثير من الآمال للأُناس العاديين. ومع ذلك فإنها تُدخل في نفس الوقت درجة غير مسبوقة من التعقيد التكنولوجي والتنظيمي. ولذا ينبغي التحكم في المخاطر الكبيرة المرتبطة بذلك لأجل تجنب إفساد فكرة التقدم ذاتها. ففي أعطاف الخطر التكنولوجي، كفشل معالجة المعلومات وأنظمة الاتصال الناجم عن عُطل عَرضَي أو خبيث، يسير الخطر المعلوماتي القمين بتقويض قدرة منظمة ما على الاستفادة من المعلومات.

ومن النقاط المهمة التي يجب ألا تغيب عن البال أنه بالرغم من أن الوصول إلى تكنولوجيا المعلومات متاح على نطاق واسع ومتنام، ما فتئ قطاع لا بأس به من السكان مستبعداً عن الثورة المعلوماتية. ويعود ذلك إلى أسباب مُركبة، تشتمل على عوامل ثقافية ومالية، كما تشتمل على صعاب أساسية كالأمية في بعض الحالات. إن التدريب والتثقيف في مجال تكنولوجيا المعلومات، أكثر من أي مجال آخر، مهمان للغاية لوضع التكنولوجيا في متناول الجميع ولمكافحة استبعاد المعلومات. وسوف يحتاج الأمر إلى التفكير مجدداً في الأسطح البينية للاتصالات بحيث تخدم السكان على نحو أفضل، وتحترم تنوع السياقات الثقافية. وينبغي تكييف الحاسوب لكي يناسب البيئة البشرية التي ينبغي أن يُدمج داخلها وذلك بدلاً من فرض نظام اتصالات جديد.

2.2.1.I دعم ثورة المعلومات

إن تكنولوجيا المعلومات والاتصالات مثلها مثل جميع التكنولوجيات، تنشأ وتعمل داخل إطار تاريخي وجغرافي خاص، وهي تعكس عامة توازناً ما داخل المجتمع. وتتمثل مسؤولية العاملين فيها في دعم ثورة المعلومات وذلك بالأدوات والتدابير والقوانين والأخلاقيات اللازمة للتعامل مع الأمن، ولتحقيق توقعات المجتمع واحتياجاته.

إن استغلال وسائل الاتصال، في الوقت الحاضر، وحرية إرسال وتلقي الرسائل يخضعان لطائفة من الأنظمة والقواعد الجزئية التي يضعها الاتحاد الدولي للاتصالات، والمنظمة الدولية للتربية والعلم والثقافة (اليونسكو) والأمم المتحدة، ومنظمة التعاون والتنمية في الميدان الاقتصادي، ومجلس أوروبا وجهات أخرى. كما أن التطورات التي اعترت تكنولوجيا المعلومات والاتصالات، والطريقة التي يستخدمها بها الناس، قد حققت سبقاً على الأنظمة والقواعد التي تحكمها، ولذلك فإن ثمة حاجة إلى وجود إطار قانوني مناسب يخاطب قضايا مثل: الطبيعة غير الإقليمية للشبكات، مثل الشبكة الدولية للمعلومات (الإنترنت)، ومشاكل المسؤولية، وحماية الخصوصية، وحقوق الملكية. ويحتاج التطور التكنولوجي إلى تطور موازٍ في النظام الاجتماعي والسياسي والقانوني. إن هذا البحث المتعجل يعطي بالفعل فكرة عن أهمية التحديات التي يفرزها عصر المعلومات. وعن الدور الحاسم للاتصالات في التصدي لتلك التحديات، وضرورة التعامل مع قضايا الأمن قبل أن تتحول إلى عقبة في طريق التنمية.

لقد كشف الانتقال إلى عصر المعلومات النقاب عن أهمية تكنولوجيا المعلومات كما أوضح الحاجة إلى التمرس الكامل بالتكنولوجيا. وبالنظر إلى الأبعاد الجديدة التي تخلقها تكنولوجيا المعلومات، من الناحيتين الاجتماعية والاقتصادية يتضح أن تكنولوجيا المعلومات وأنظمة الاتصالات والبنى التحتية قد غدت من الاحتياجات الجوهرية. فهي تُبرز الطبيعة الاستراتيجية والحرجة لمناط تخطيط وتنفيذ الأمن السيبراني بالنسبة للبلدان وللمنظمات وللأفراد.

وبالنظر إلى المواد المالية والمادية والبشرية التي استثمرتها البلدان لخلق بناها التحتية للمعلومات والاتصالات، يكون من الضروري بالنسبة لها ضمان أن تنعم هذه البنية الأساسية بالأمان، وأن تدار إدارة حسنة ومراقبة.

القسم 2.I – الأمن السيبراني

1.2.I السياق الأمني للبنية التحتية للاتصالات

ثمة وعي متزايد بأهمية الإلمام الكامل بالمخاطر التشغيلية لتكنولوجيا المعلومات التي تصاحب تزايد استخدام التكنولوجيات الجديدة، ووجود بنية أساسية عالمية لتكنولوجيا المعلومات وظهور مخاطر جديدة.

إن تحول المجتمعات إلى مجتمعات *معلوماتية*، وهو التحول الذي يحدث بفضل إدماج تكنولوجيات جديدة في كل مجال من مجالات النشاط، وفي كل نوع من أنواع البنية التحتية ليزيد من اعتماد الأفراد، والمنظمات، والبلدان على أنظمة المعلومات والشبكات. وهذا مصدر رئيسي من مصادر المخاطر تَجِبْ معاملته كخطر أمني.

وتواجه البلدان النامية إشكالية الحاجة للانضمام إلى المجتمع المعلوماتي دون أن يغيب عن بالها مخاطر تحولها إلى الاعتماد على التكنولوجيات وعلى مقدمي التكنولوجيا واحتياجها لتفادي خطر الفجوة الرقمية التي تنشأ عنها ثغرة أمنية أو حتى الاعتماد الزائد على الهيئات التي تتحكم في احتياجاتها وفي سبل تحقيق أمن تكنولوجيا المعلومات[1].

ويجب أن يتم التفكير ملياً في تصميم وإنشاء وإدارة البنى الأساسية للاتصالات والخدمات والأنشطة التي توفرها مع مراعاة الجانب الأمني، ذلك لأن الأمن هو الركن الركين لأي نشاط، وينبغي النظر إليه كخدمة تُمكِن من خلق خدمات أخرى وتولد القيمة (مثل الحكومة الإلكترونية، والصحة الإلكترونية، والتعليم الإلكتروني). فليس الأمر مقصوراً على التكنولوجيا وحدها[2]، ومع ذلك فإن أدوات الاتصال الأساسية المتوافرة حتى الآن لا تظفر بالموارد الضرورية والكافية لتوفير أو لضمان القدر الأدنى لها من الأمن.

إن أنظمة تكنولوجيا المعلومات المترابطة شبكياً هي موارد يمكن الوصول إليها عن بعد، ومن ثم فهي أهداف يحتمل أن تتعرض للهجوم السيبراني. كما أن الأنظمة معرضة لخطر زائد هو الاختراق، حيث تتزايد فرص شن الهجمات عليها واقتراف الجرائم. وعلى الرغم من أن الأنظمة هي التي تكون هدفاً للهجوم فإن الغنيمة التي يسعى المهاجمون للفوز بها هي المعلومات التي تجري معالجتها (الشكل 2.I). ويمكن لهذه الهجمات أن تنال من القدرة على المعالجة والتخزين وتقاسم الرصيد المعلوماتي، بل ويمكن لها أن تُنـــزِل الضرر بالسلع غير الملموسة والرمزية، وبعمليات الإنتاج، وبعمليات صنع القرار لدى المنظمة. وتحمل الأنظمة السيبرانية المخاطر التشغيلية إلى المنظمات التي تمتلكها.

وهكذا يمكن للتعامل مع مشاكل الأمن السيبراني المعقدة والمتعددة الأوجه أن يكون صعباً نسبياً، كما يمكن لمضاعفاتها المحتملة وتأثيراتها على تشغيل المنظمات والبلدان أن تكون مدمرة. وقد تتوقف العوامل المهمة للغاية لإنجاح الاقتصادات على قدرة توفير الأمن للمعلومات وللعمليات وللأنظمة وللبنية التحتية.

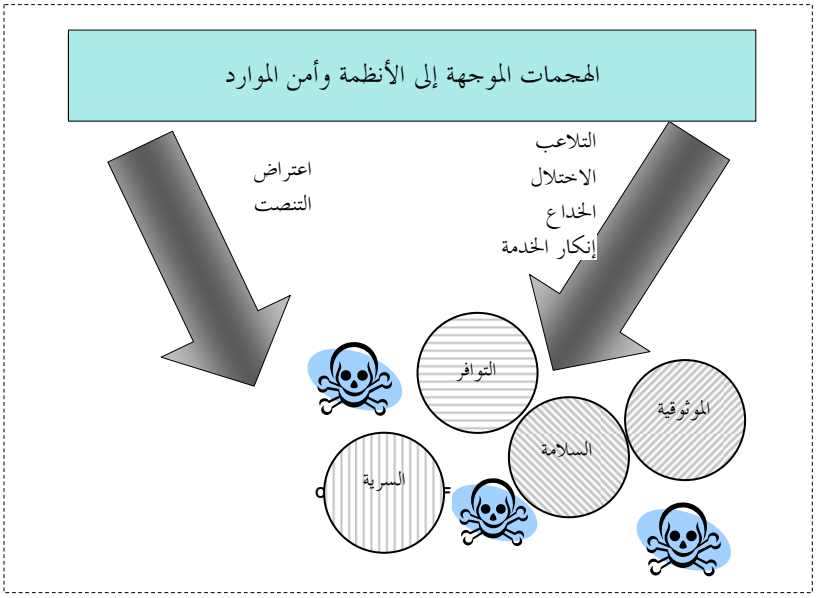
إن التوصيل البيني واسع النطاق للأنظمة، وازدياد الارتباط بين البنى التحتية، وتزايد الاعتماد على التكنولوجيات الرقمية، وتزايد التهديدات والمخاطر تجعل من الضروري بالنسبة للأفراد والمنظمات والبلدان اتخاذ خطوات، واتباع تدابير واقتناء أدوات لتحسين طريقة إدارة المخاطر التكنولوجية والسيبرانية. كما أن التحديات التي تنطوي على السيطرة على المخاطر التكنولوجية هي تحديات نابعة من طبيعة القرن الحادي والعشرين. وهي تستلزم اتباع نهج عالمي شامل إزاء الأمن ينسحب أيضاً على البلدان النامية.

---

[1] S. Ghernauti-Helie: "*من الفجوة الرقمية إلى عدم الأمن الرقمي*: تحديات تطوير ونشر إطار موحد للأمن الإلكتروني في سياق متعدد الأبعاد" *في التعاون الدولي ومجتمع المعلومات*، القسم السويسري في دليل وضع السياسات، مطبوعات المعهد الجامعي للدراسات الإنمائية (IUED). جنيف، نوفمبر 2003.

[2] A. Ntoko "الولاية والأنشطة في الأمن السيبراني – ITU-D " الاجتماع المواضيعي للقمة العالمية لمجتمع المعلومات بشأن الأمن السيبراني. الاتحاد الدولي للاتصالات، جنيف 28 يونيو – 1 يوليو 2005.

الشكل 2.I – الهجمات الموجهة إلى الأنظمة وأمن الموارد



ولا يكفي إنشاء نقاط للنفاذ إلى شبكات الاتصالات. إذْ من الضروري نشر البنى التحتية لتكنولوجيا المعلومات والخدمات السيبرانية التي يُعَوَّل عليها، وتكون قابلة للصيانة ومتينة وآمنة، مع الحرص في نفس الوقت على حقوق الإنسان وحقوق الدول. إن الحاجة إلى حماية الأنظمة والمعلومات القَيِّمَةْ، عليها أن تتعايش وتتوافق مع الحماية الموازية لحقوق الأفراد وخصوصياتهم.

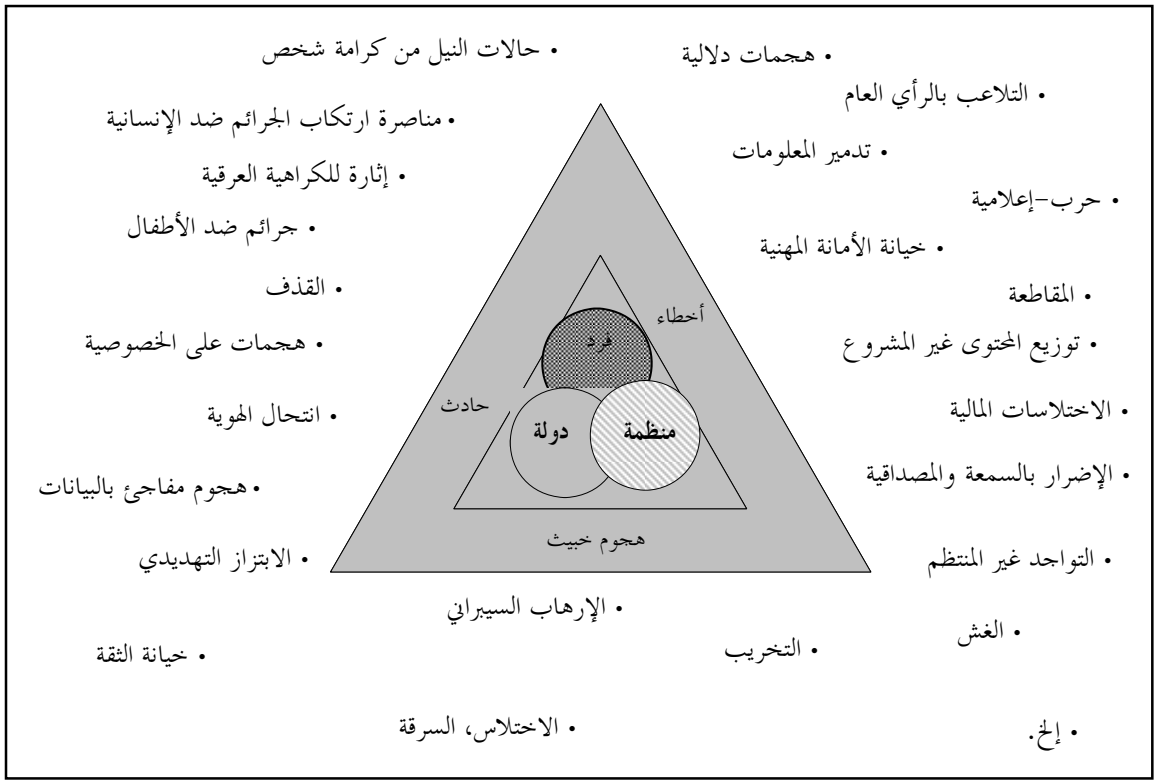
والبلدان النامية بحاجة إلى ولوج مجتمع المعلومات دون أن تُعَرِضْ أنفسها لمخاطر زائدة عن الحد، وأن تنهل من الخبرات التي حَصَّلتها البلدان المتقدمة، وأن تتفادى خطر استبعادها بسبب العامل الجديد المتمثل في الأمن السيبراني.

2.2.I ما هي التحديات التي يمثلها الأمن السيبراني

إن القضايا الاجتماعية، والاقتصاد، والسياسات العامة الجماهيرية والقضايا الإنسانية: مهما تكن الجهة التي يبيمم الإنسانُ نظره شَطرها، ومهما تتغير مسمياتها (أمن تكنولوجيا المعلومات وأمن الاتصالات)، فإن الأمن السيبراني يمس أمن الثروة الرقمية والثقافية للناس وللمنظمات وللبلدان (الشكل 3.I). بل إن التحديات التي ينطوي عليها ذلك مُعَقدة، ويحتاج التصدي لها إلى ضرورة توافر الإرادة السياسية اللازمة لتصميم وتنفيذ استراتيجية لتطوير بنى تحتية وخدمات رقمية تشمل استراتيجية للأمن السيبراني تكون متماسكة، وفعالة، وقابلة للتحقق منها ومن إدارتها. ويجب أن تكون استراتيجية الأمن السيبراني جزءاً من نهج متعدد التخصصات، مع وجود حلول جاهزة على المستويات التثقيفي، والقانوني، والإداري والتقني. ويمكن للاستجابة القوية للأبعاد البشرية والقانونية والاقتصادية لاحتياجات أمن البنية الأساسية الرقمية أن تبنى الثقة، وأن تُولِد النمو الاقتصادي المرغوب فيه، والذي يفيد المجتمع كافة.

إن تملك زمام رصيد المعلومات الرقمية، وتوزيع السلع غير الملموسة، وإضافة القيمة إلى المحتوى، وسد الثُغرة الرقمية كلها مشاكل ذات طبيعة اقتصادية واجتماعية، تستلزم شيئاً أكثر من مجرد اتباع نهج وحيد البُعد وتكنولوجي بحت تجاه الأمن السيبراني.

الشكل 3.I – مستويات الأمن السيبراني: الأفراد والمنظمات والبلدان



ويلزم للأنشطة القائمة على معالجة المعلومات لكي تنمو وتساعد على تضييق الفجوة الرقمية ما يلي:

- وجود بنى أساسية للمعلومات الدقيقة والآمنة (ذات نفاذية مضمونة، وتوافر، مع استمرار الخدمات مع إمكانية التعويل عليها)؛
- سياسات لخلق الثقة؛
- أُطر قانونية مناسبة؛
- سلطات قضائية وشرطية مُلِمَة بالتكنولوجيات الجديدة وقادرة على التعاون مع نظيراتها مع البلدان الأخرى؛
- أدوات لإدارة مخاطر وأمن المعلومات؛
- أدوات لتنفيذ الأمان قمينة بتوليد الثقة في التطبيقات والخدمات المقدمة (الأعمال، والتمويل، والصحة والحكم والتصويت بالطريق الإلكتروني، إلخ.) وفي التدابير الموضوعة لحماية حقوق الإنسان ولا سيما فيما يتعلق بالسرية.

إن غرض الأمن السيبراني هو المساعدة على حماية أصول وموارد منظمة ما من النواحي التنظيمية، والبشرية، والمالية والتقنية والمعلوماتية بحيث تتمكن من أداء المهمة الموكلة إليها.

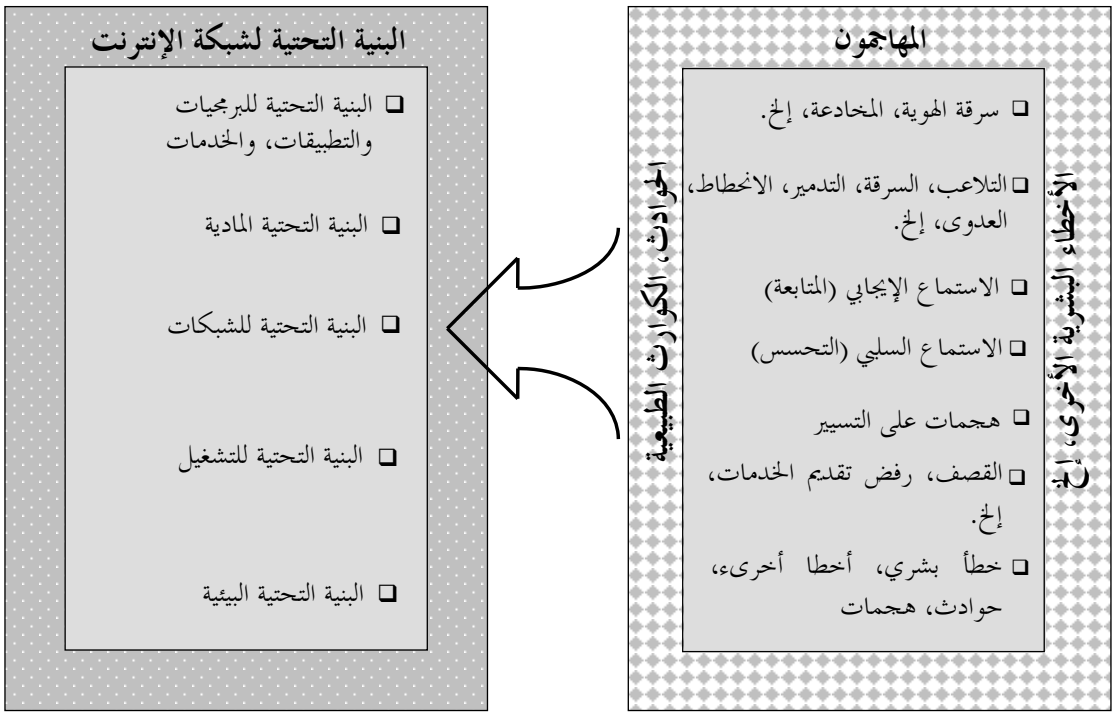
والهدف الأسمى لذلك هو ضمان عدم حدوث ضرر دائم للمنظمة. ويتألف ذلك من تقليل احتمالات تجسد خطر ما، والحد من الضرر أو سوء الأداء الناجمْين، وتأمين عودة العمليات العادية إلى مسيرتها الأولى بعد وقوع حادث أُمني، خلال فترة زمنية مقبولة وبتكلفة ومعقولة.

وتشمل عملية الأمن السيبراني المجتمع بأسره، بحيث يكون كل فرد مهتم بتنفيذه. ويمكن جعل هذه العملية أكثر أهمية عن طريق بلورة مدونة سلوك سيبراني، والإعلان عن سياسات أمن حقيقية تنص على المعايير التي يكون من المتوقع وفاء المستعملين، والكيانات والشركاء والموردين بها.

3.2.I القصور الأمني

القصور الأمني في تكنولوجيا المعلومات والاتصالات هو انعكاس لطبيعة تكنولوجيا المعلومات والفضاء السيبراني. وحقيقة أن المستخدمين يتحركون في عالم افتراضي، ويعملون عن بعد وعلى نحو مجهول الهوية نسبياً، يزيد من مصاعب تصميم هذه التكنولوجيا، وتنفيذها وإدارتها والتحكم فيها. فإذا أضاف المرء حالات التوقف، واختلال الوظائف، والأخطاء والتعارض بينها وحتى الكوارث الطبيعية إلى هذه المعادلة، فإن النتيجة تبدو، وبصورة لا تثير الدهشة، هالة من عدم الأمن تنال من البنية التحتية لتكنولوجيا المعلومات (انظر الشكل 4.I).

الشكل 4.I – البنية التحتية للإنترنت والمصادر الكثيرة للمشاكل



وفي هذا السياق توجد عدة طرق يمكن للمهاجم الخبيث أن يستغل بها نقاط التعرض[3].

إن كثرة هذه الهجمات – بما فيها سرقة الهوية ومخادعة النظام، والاقتحام، واختطاف الموارد، والعدوى، والتدهور، والتدمير، والتلاعب، وخرق السرية، إنكار الخدمة، السرقة، الابتزاز، إلخ.– تلقي بالضوء على جوانب القصور في استراتيجيات الأمن الحالية، ولكنها على النقيض من ذلك توضح أن البنى التحتية على درجة معينة من الصلابة.

ومهما تكن دوافع مجرمي الحاسوب الفرديين، فإن النتائج تنطوي دائماً على تأثير ليس بالبسيط من الناحية الاقتصادية. ذلك أن الجريمة السيبرانية تتحول بسرعة إلى وحش دولي متعدد الرؤوس.

والحلول الأمنية موجودة، ولكنها لا تكون مطلقة أبداً، ولا تمثل بصورة عامة أكثر من الاستجابة لمشكلة معينة داخل سياق محدد. والنتيجة هي أن المشكلة الأمنية تراوح مكانها، ومن ثم تتحول المسؤولية الأمنية، يضاف إلى ذلك أن الحلول بدورها تصبح في حاجة للتأمين وللإدارة بصورة تتوافر فيها الحماية.

[3] الجريمة السيبرانية والهجمات السيبرانية والمخالفات السيبرانية موضوع مناقشة مستفيضة في الجزء II.

وهي تمثل، في أفضل الحالات، محاولة تجريبية للتعامل مع الحقيقة الدينامية التي تواجهها والتي تتمثل في التكنولوجيا السيالة، والأهداف المتغيرة، ومهارات المتسللين المتطورة، والتهديدات والمخاطر دائمة التغير. ولذلك لا يمكن أن يتوافر هناك ضمان بأن نهجاً بعينه إزاء الأمن سوف يوفر حماية دائمة، أو، كنتيجة فرعية لذلك، ضمان لتحقيق عائد للنفقات على الأمن.

وغالباً ما تقتصر استراتيجية الأمن على إنشاء آليات أمنية لتقليل المخاطر التي تتعرض لها الأصول المعلوماتية لشركة ما، باتباع نهج تكنولوجي بحت عادة. في حين أن الاستراتيجية الأفضل هي تلك الاستراتيجية التي تأخذ في اعتبارها جميع أبعاد المشكلة، وتعالج احتياجات الأفراد من الأمن، وبخاصة من حيث ما يتعلق بالسرية وبالحقوق الأساسية. وينبغي للأمن السيبراني أن يشمل كل فرد، وأن يَمُدَ الحماية إلى البيانات ذات الطبيعة الشخصية.

إن الحلول الأمنية متوافرة بالفعل. وهي، في الكثير من الحالات، تكنولوجية بحته بطبيعتها، وتتناول مشكلة بعينها في سياق محدد. ولكن، مثلها مثل جميع الأشياء التكنولوجية، غير معصومة من العيوب ويمكن التحايل عليها. فهي، في معظم الحالات، لا تفعل أكثر من مجرد إزاحة مشكلة الأمن عن مكانها الأصلي وتحويل المسؤولية إلى جزء آخر من النظام من المفترض أنها تحميه. يضاف إلى ذلك أنها هي نفسها محتاجة إلى الحماية وإلى الإدارة المأمونة. وهي لا تستطيع أن توفر حماية مطلقة أو نهائية وذلك بسبب الطبيعة التطورية للسياق الأمني الذي ينشأ في حد ذاته نتيجة لبيئة دينامية (احتياجات ناشئة، ومخاطر، وتكنولوجيات، ومهارات المتسللين، إلخ) وهكذا تكون هناك مشكلة ذلك لأن الحلول الحالية تكون قصيرة الأجل في أحسن الحالات. وثمة مشكلة أخرى هي أن كثرة الحلول المختلفة غير المتجانسة قد تضر بالتماسك الكلي لاستراتيجية الأمن، ومن الواضح أن التكنولوجيا وحدها لا تكفي إذْ لا بد من إدماجها في نهج للإدارة.

إن التماسك الكلي لإستراتيجية الأمن معقدة بسبب تلك الطائفة الواسعة من الكيانات المختلفة والأفراد الضالعين فيها (المهندسون، مطورو المشروعات، المراجعون، مهندسو الأنظمة، المحققون، العملاء، الموردون إلخ.) وبسبب المجموعة الواسعة للمصالح، والرؤى والبيئات، واللغات. ويحتاج الأمر إلى فهم موحد ونُظُمِي للمخاطر والتدابير الأمنية. كما يلزم الإقرار بكل مسؤولية من المسؤوليات التي ينطوي عليها ذلك إذا كان من المرتجي تحقيق ذلك المستوى الأمني اللازم للقيام في سرية بإجراء النشاطات باستخدام تكنولوجيا المعلومات والاتصالات، والمساهمة في بناء الثقة في الاقتصاد الرقمي.

4.2.I الدروس المستفادة

1.4.2.I تولي مسؤولية الأمن

في مطلع القرن الحادي والعشرين، قبلت معظم المنظمات الكبرى – والكثير من المنظمات الأصغر حجماً – بصفة عامة التصدي للتحديات التي يفرضها أمن تكنولوجيا المعلومات. فلم تعد استراتيجية الأمن ينظر إليها كمجموعة اعتباطية من أدوات الأمن. بل بات يُنْظَر إليها، بدلاً من ذلك، وعن حق، كعملية مستمرة.

إن الهدف من أسلوب الإدارة الأمنية السليمة هو ضمان استخدام التدابير الأمنية المناسبة للغاية في كل مكان وكل وقت. ويستند هذا المفهوم إلى الأسئلة البسيطة التالية:

- من يفعل ماذا، كيف وعندما؟
- من هم اللاعبون الذين يضعون القواعد، ويُعَرِّفُونَها ويتحققون من سلامتها، ثم يقومون بتنفيذها وممارسة السيطرة عليها؟

2.4.2.I تحديد طبيعة المخاطر وإدارتها

ينبغي أن تستهدى استراتيجية أمن البنى التحتية الرقمية بتحليل المخاطر المرتبطة بمعالجة المعلومات، والاتصالات والفضاء السيبراني وذلك كجزء من عملية إدارة المخاطر. ويحتاج الأمر إلى تحديد المخاطر الأمنية لتكنولوجيا المعلومات (التي يشار إليها أيضاً كمخاطر الحاسوب، أو مخاطر المعلومات أو مخاطر التكنولوجيا) إلى جانب جميع المخاطر الأخرى التي تواجه المنظمة (استراتيجية، اجتماعية، بيئية، إلخ).

إن مخاطر تكنولوجيا المعلومات مخاطر تشغيلية تحتاج إلى السيطرة عليها. ففي الصميم من إدارة المخاطر يأتي تحليل مخاطر الأمن التي تجعل من الممكن تعريف استراتيجية الأمن والسياسات العامة المتعلقة بالأمن ويثور عدد من الأسئلة في هذه المرحلة:

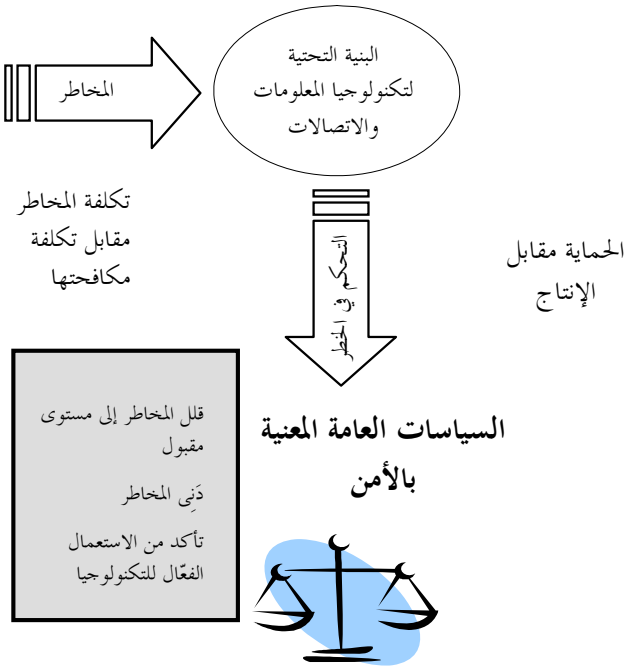
- من الذي سيكون مسؤولاً عن تحليل المخاطر وإدارة المخاطر؟
- ما هي أفضل طريقة لإجراء تحليل؟
- ما هي الأدوات والطرق المتوافرة؟
- إلى أي مدى يمكن التعويل على هذه السياسات وهذه الاستراتيجية؟
- ما مقدار التوكيد على النتائج؟ ما هي التكاليف؟
- هل يكون من الأفضل إسناد هذه الوظيفة لجهة خارجية؟
- إلخ.

ويمكن تعريف المخاطر على أنها خطر يمكن توقعه وتلافيه إلى حد ما. ويتم تلميته على أساس احتمالات الإتلاف والضرر الناجم. وتعبر المخاطر عن احتمالية فقدان أصل من الأصول أو قيمة بسبب التعرض المرتبط بخطر شديد (danger) أو متوسط الشدة (hazard) .

ومن الضروري عند البت في المستوى المرغوب فيه من الحماية وأنواع تدابير الأمن التي يجب تحقيقها الموازنة بين حجم المخاطر (من الناحية المالية) وبين التكاليف التي قد تلزم للتقليل منها (انظر الشكل 5.I). وكحد أدنى، يجب تحديد الأصول التي يجب حمايتها وذلك كحد أدنى، بالإضافة إلى مسوغات حمايتها، تبعاً للعقبات الفعلية والموارد التنظيمية والمالية والبشرية والتقنية المتوافرة. وينبغي للتدابير المتخذة أن تكون فعالة كما يجب أن تعكس توازناً بين الأداء وبين الفعالية التكاليفية.

إن السيطرة على مخاطر تكنولوجيا المعلومات، بالنسبة لمنظمة ما، تعني بلورة استراتيجية تعرف سياسة عامة للأمن وتبت بشأن تنفيذها من الناحيتين التكتيكية والتشغيلية.

الشكل 5.I – الموازنة بين اعتبارات السيطرة على المخاطر، قرار يتعلق بالسياسات المتبعة



3.4.2.I تعريف السياسات العامة للأمن

تترجم السياسات العامة المعنية بالأمن المفهوم الخاص بالمخاطر وتأثيرها إلى تدابير أمن خاصة بالتنفيذ وهي تيسر كلاً من المنع والتدابير العلاجية التي تتخذ استجابة لمشاكل الأمن، كما تساعد على تقليل المخاطر وما يترتب عليها من تأثيرات.

وعلى الرغم من أنه يستحيل القضاء المبرم على المخاطر، ومن الصعب التأهب لجميع التهديدات البازغة، فإن المهم هو تقليل تعرض البيئات والموارد المطلوب حمايتها حيث إن ذلك التعرض هو منشأ الكثير من المشكلات الأمنية.

وينبغي للسياسات العامة المعنية بالأمن أن يُعَيِّنَ العديد من الأمور، من بينها على وجه التحديد الموارد، والشكل والتدابير والخطط الخاصة بالدفاع، وبالتقليل من حدة المخاطر وذلك لضمان إمكانية التحكم في المخاطر التشغيلية، والتكنولوجية والمعلوماتية.

وتقترح الأيزو 17799 مدونة ممارسات لإدارة الأمن، ويمكن اعتبارها مرجعاً لتعريف السياسات العامة المعنية بالأمن، وقائمة مرجعية لتحليل المخاطر، وأداة مراجعة خاصة بالأمن سواء كان ذلك لأغراض الاعتماد certification أم لا، أو كمحور اتصالات خاص بالأمن. ويمكن تفسير هذا المعيار وتنفيذه بطرق عدة. وتكمن قيمته في حقيقة أنه يتناول الجوانب التنظيمية، والبشرية، والقانونية، والتكنولوجية للأمن في كل مرحلة من المراحل المختلفة لتصميم وتنفيذ الأمن وصيانته. ويشدد إصدار عام 2005 للمعيار (ISO/IEC 17799 :2005)[4] على تقييم المخاطر وتحليلها، وإدارة الأصول والموارد، والحوادث. وهذا يشير إلى الأهمية التي يحظى بها البُعْد الإداري من بين أبعاد الأمن.

الشكل 6.I – لكي تدير الأمن، عَرِّفْ السياسات المعنية بالأمن

مكونات السياسة العامة المعنية بالأمن	
تنظيم الأمن	ما الذي ينبغي حمايته؟ من من؟ وضد أي شيء نحمي أنفسنا؟ ولماذا؟
اسند مسؤوليات للمختصين مع السلطات الضرورية والموارد	ما هي المخاطر الحقيقية؟ هل يمكن تحملها؟
حدد الأهداف الأمنية لكل مجال وكل عنصر في نظام المعلومات	ما هو المركز الأمني الراهن للمنظمة؟ ما هو المستوى المرغوب فيه من الأمن؟
عرّف التهديدات وحدد نقاط التعرض	ما هي المعوقات الحقيقية؟ وما هي الموارد المتوافرة؟ وكيف يمكن توزيع تلك الموارد؟
عرّف التدابير الأمنية	
عرّف الممارسات الأمنية	

[4] يرد جدول محتويات هذا المعيار في المرفق باء بهذا الدليل.

لا ينبغي قياس فعالية السياسة العامة للأمن بحجم ميزانيتها، وإنما تعتمد هذه الفعالية بدلاً من ذلك على سياسات إدارة المخاطر، وعلى نوعية تحليل المخاطر (الشكل 6.I). ومن بين العوامل التي تحدد المخاطر، مجال نشاط المنظمة، وحجمها، وصورتها، ومدى حساسية نظامها، والبيئة السائدة في هذا النظام والتهديدات المرتبطة بها، ودرجة اعتماد المنظمة على نظام معلوماتها.

تعتمد جودة أمن تكنولوجيا المعلومات بالدرجة الأولى على تحديد قيمة أصول المعلومات، والتوزيع التشغيلي لتدابير الأمن المناسبة المبنية على سياسات أمنية عامة مدروسة بتأنٍ وإدارة فعالة.

4.4.2.I أنشر الحلول

هناك العديد من أنواع التدابير التي ينبغي توطيدها لزيادة أمن البنية التحتية للاتصالات وتكنولوجيا المعلومات. ومن بين هذه التدابير:

- بناء الوعي وتثقيف وتدريب جميع أصحاب المصلحة في الأمن السيبراني؛
- خلق وحدات يمكنها أن تؤدي وظيفة المركز الوطني للإنذار المبكر والاستجابة للأزمات، وتجميع الموارد الضرورية لأداء ذلك بفعالية وتقاسمها عبر العديد من البلدان لخدمة إقليم ما؛
- إنشاء المراقبة والتفتيش (الشبيهة ما تكون بنقاط التفتيش على الطرق)؛
- بناء الخبرة داخل فريق شرطة سيبراني يمكنه المساهمة في عملية تعاونية دولية للبحث في الجريمة المرتبطة بالحاسوب والمحاكمات الخاصة بذلك؛
- بلورة حلول تكنولوجية لإدارة الهوية، والتحكم في النفاذ، واستخدام العتاد الآمن للحاسوب، والأنظمة الأساسية للبرمجيات، والبنى التحتية المساندة، وبروتوكولات التشفير والإدارة التشغيلية.

5.2.I منظور الإدارة

1.5.2.I الإدارة الدينامية[5]

إن تناول مسألة الأمن من خلال عملية إدارة دينامية مستمرة، يؤهل المنظمة للتعامل مع الطبيعة الدينامية للمخاطر وللاحتياجات البازغة وذلك عن طريق التكييف المستمر وتحسين حلولها. وتحدد نوعية الإدارة الأمنية مستوى الأمن المُقدَم. وينبغي تعريف السياسات العامة للأمن السيبراني على مستوى قمة الإدارة. وتتعدد استراتيجيات وسياسات وإجراءات الأمن وتدابيره وحلوله بتعدد المنظمات التي لديها احتياجات أمن تَود سَدَها في أي وقت معين.

وللحصول على مثال للسياق الدينامي الذي يجب أن تعمل إدارة الأمن داخله، انظر في عملية الكشف عن نقاط التعرض الأمني والحيلولة دون استغلالها. ويتم هذا عن طريق إصدارات دورية من الإسعافات لسد الثغرات، الرسائل الإخبارية الإعلامية، التي تُفَصَّل حسب الطلب تقريباً، وتجعل من الممكن المعرفة المستمرة بشأن نقاط التعرض التي تم كشفها وكيفية علاجها. وللمحافظة على القدر الأدنى من الأمن، سوف يكون على مسؤول الأمن أو مسؤول النظام تنفيذ الإسعافات الأمنية الإلكترونية بمجرد صدورها. ولذلك فإن الإلمام بنقاط التعرض الخطيرة في أي نظام أمر مفيد ليس فقط بالنسبة لمسؤول الأمن، وإنما أيضاً للمتسللين الذين قد يحاولون استغلالها قبل تطبيق الإسعافات الأمنية. ولذلك فإن من الحتمي تخصيص موارد كافية لتنفيذ إدارة دينامية تقوم بتحديث الحلول الأمنية ومن ثم تحافظ على مستوى مستمر من الأمن.

[5] القسمان التاليان مقتبسان من مقالة بعنوان: "*Sécurité informatique, la piège de la dependence*" A. Dufour, G. Ghernaouti-Hélie, *Revue Information et Système*, 2006.

إن الإنذارات والرُقَعْ التي تُنْشَر تسمح للمسؤول بالتحكم في عملية التحديث (باختيار تطبيق تلك الرُقَعْ الأمنية أم لا). ومن الممكن أيضاً عمل ذلك بطريقة تلقائية عن طريق النقل الفعال لمسؤولية تثبيت الرقع بصورة منتظمة ونظامية في ناشر البرمجيات.

ويثير ذلك قضية المسؤولية. فمثلاً، ما هي النتائج القانونية التي تترتب على تحديث لبرمجيات تم رفضه حينما تظهر المشاكل وذلك نتيجة لاستغلال نقطة تعرض لم يتم ترقيعها؟ وحيث إن العديد من الهجمات تفعل ذلك بالضبط، فإن السؤال عمن الذي يقرر الرفض أو القبول، ومسؤولية مسؤول النظام، يكون سؤالاً مناسباً إلى حد كبير.

إن البعد الدينامي للأمن يمثل تحدياً حرجاً ليس فقط لموردي أدوات الأمن وناشري البرمجيات، وإنما أيضاً بالنسبة لمسؤولي الأنظمة ومسؤولي الأمن الذين نادراً ما يتاح لهم الوقت اللازم لإدراج جميع الرقع والتحديثات المتاحة.

إن مسؤولي الأمن ومسؤولي الأنظمة – بصفتهم مديري الحاسوب، يملكون منافذ الوصول الكامل إلى موارد تكنولوجيا المعلومات لدى المنظمة، وليس من الضروري فقط تطبيق المراقبة الصارمة وتدابير المراقبة على ما يقومون به من أعمال (بالتناسب مع المخاطر التي يخلقون احتمالات حدوثها للأنظمة الخاضعة لمراقبتهم)، وإنما يجب على هؤلاء الموظفين أن يتحلوا بالنـــزاهة الشخصية المطلقة.

2.5.2.I الإسناد الخارجي والتبعية[6]

يتولى مقدمو الخدمات الذين يقدمون مرشحات مكافحة الفيروسات والرسائل الاقتحامية في الواقع جزءاً من إدارة الأمن بالنسبة لزبائنهم. ولقد بدأ هذا الاتجاه في تغيير توزيع الأدوار والمسؤوليات في المسائل الأمنية. وسوف يتحول الأمن بصورة متزايدة صوب مقدم الخدمة أو المورد الفني. وهذا التحول، لا يحل بالطبع، مشكلة الأمن، وإنما يقوم فقط بمجرد تحويلها إلى مقدم الخدمة الذي يصبح مسؤولاً ليس فقط عن توفير الخدمة وأدائها، وإنما أيضاً عن إدارة وصيانة مستوى معين من الأمن.

وعادة ما يقدم ناشرو برمجيات مكافحة الفيروسات خدمة تحديث أوتوماتيكية. إن إضافة هذا البعد الجديد في الخدمة يجعل استئجار البرمجيات جذاباً بصورة متزايدة حيث إن مسؤولية الصيانة تُنْقَل إلى الناشر لفترة طويلة. كما يُغَذِي اتجاهاً أعرض نحو إسناد التطبيقات إلى جهات خارجية بما يلازم ذلك من نشوء نموذج جديد للأعمال.

إن مسألة إخراج أو إسناد كل أو جزء من مهمة الأمن لجهة خارجية ليست مسألة تقنية بحتة بل إنها ذات طبيعة استراتيجية وقانونية، وتثير قضية جوهرية خاصة بالاعتماد على الموردين.

إن أي استراتيجية لإسناد الأمن لجهة خارجية قد تشمل تعريف السياسة وتنفيذها وإدارة الحصول عليها، وإدارة حوائط النيران (firewalls). وصيانة الأنظمة والشبكات عن بعد، وصيانة البرامج التطبيقية على يد طرف ثالث، وإدارة تأمين الملفات back-up management وما إلى ذلك. ويجب أن يصاحب عملية اختيار المتعاقد عملية لمراقبة الجودة، ويمكن أن تراعى أموراً مثل خبرات المتعاقد، والخبرات المتوافرة لدى المنظمة، والتكنولوجيات المستخدمة، وزمن الاستجابة، وخدمة الدعم والترتيبات التعاقدية (مثل النتائج المضمونة) أو تقاسم المسؤوليات القانونية.

3.5.2.I الإجراءات الوقائية والعلاجية

إن الوقاية الأمنية، هي بالتحديد عملية إيجابية تأخذ بزمام المبادرة وهي تشتمل على أبعاد بشرية وقانونية وتنظيمية واقتصادية (النسبة بين تكلفة/مستوى تنفيذ الأمن/الخدمات المقدمة) وتكنولوجية. ويُعني أمن بيئة تكنولوجيا المعلومات والاتصال حتى الآن، إلى حد بعيد، بالبعد التقني. كما أن هذه الطريقة لفهم أمن أنظمة المعلومات، بالدرجة الأولى من وجهة النظر التقنية، مُهْمِلَةَ البعد البشري، هي مشكلة حقيقية في التحكم في مخاطر التكنولوجيا المرتبطة بالأعمال

[6] هذا القسم مقتبس من كتاب بعنوان: "*Sécurité informatique et réseaux*"، S. Ghernaouti-Hélie، Dunod، 2006.

الإجرامية. وذلك لأن الإجرام هو قضية بشرية بالدرجة الأولى وليست قضية تقنية. ومن ثم فإن الاستجابة التقنية البحتة تكون غير مناسبة للتحكم فيما هو بشري بالأساس.

إن نهج معالجة إجرام تكنولوجيا المعلومات هو نهج نموذجي يقوم على رد الفعل وعلى المقاضاة ومن ثم فهو يأتي بعد الواقعة، أي بعد حدوث حادث كشف تحديداً عن وجود ثغرة في تدابير الوقاية. فمن الضروري ليس فقط منع وردع الهجمات السيبرانية عن طريق تطوير الآليات التحقيقية/الإجرامية، وإنما أيضاً تحديد تلك التدابير في سياسات الأمن التي كان من واجبها الاستجابة للهجمات ومقاضاة المهاجمين. لذلك وجب تصميم ووضع خطط المساندة والاستمرارية، وإدماج العقبات ذات الصلة بالتحقيق في الجريمة السيبرانية والتقاضي بشأنها، في صميم مختلف عمليات وأهداف الأعمال، وبجداول زمنية محددة.

6.2.I البُعد السياسي

1.6.2.I مسؤولية الدولة

تقع على عاتق الدولة مسؤولية كبيرة لتحقيق الأمن الرقمي. ويُصدق ذلك بصفة خاصة على تعريف الإطار القانوني المناسب، وهو الإطار الموحد والعملي. ولا ينبغي لعمل الدولة أن يقتصر على مجرد تعزيز وتشجيع البحث والتطوير في مجال الأمن، وإنما يجب أن يتعدى ذلك أيضاً إلى تعزيز ثقافة أمنية، والامتثال للطلب بقدر أدنى من معايير الأمن (إذ ينبغي للأمن أن يكون جزءاً لا يتجزأ من النواتج والخدمات)، والقيام في نفس الوقت بتقوية إنفاذ القانون فيما يتعلق بالجريمة السيبرانية. ويثير هذا مسألة النموذج المالي الأساسي والشراكة العامة–الخاصة لخطط العمل الوطنية والدولية.

ومن الضروري على المستوى الاستراتيجي تأمين إدارة الوقاية، والإبلاغ، وتقاسم المعلومات والإنذار. ومن الضروري زيادة الوعي بأفضل الممارسات في مجال الأمن وإدارة المخاطر. وثمة مطلب مهم آخر هو تنسيق الأنظمة القانونية والتوفيق بينها. وينبغي كذلك تعريف المساعدة لتقوية إنفاذ القانون والأمن، وصياغة المشروعات التعاونية المقترحة (الرسمية/غير الرسمية، متعدد الأطراف/الثنائية، الإيجابية/السلبية، الوطنية والدولية).

ومن الضروري في نفس الوقت توفير التثقيف والإعلام والتدريب على معالجة المعلومات وتكنولوجيا الاتصالات، وليس فقط على الأمن وتدابير الردع. إن بناء الوعي بقضايا الأمن لا ينبغي أن يقتصر على تشجيع ثقافة أمنية ومدونة سلوك سيبرانية بعينها. إذْ ينبغي لثقافة الأمن أن ترتكز على ثقافة لتكنولوجيا المعلومات منذ البداية.

ويجب توفير الوسائل لجميع العاملين في هذا المجال لتعلم كيفية إدارة المخاطر التكنولوجية، والتشغيلية والإعلامية التي تهددهم من حيث ما يتعلق باستخدام التكنولوجيات الجديدة. وفي هذا السياق، ينبغي للدولة كذلك أن تشجع على الإبلاغ عن الحالات التي تُقترف فيها جرائم سيبرانية وأن تضمن وجود الثقة بين مختلف الفرقاء في المجال الاقتصادي وبين السلطات القانونية وجهات إنفاذ القوانين.

وثمة دور تكتيكي وتشغيلي ينبغي لتلك السلطات، وأيضاً لسلطات الدفاع المدني، وخدمات الطوارئ والقوات المسلحة وقوات الأمن أن تضطلع به في الكفاح ضد الجريمة السيبرانية لأجل تحقيق الوقاية والتقاضي والإصلاح. ويجب تشغيل مراكز المراقبة والكشف والمعلومات المعنية بتكنولوجيا المعلومات والمخاطر الإجرامية من أجل توفير الوقاية الضرورية للتحكم في هذه المخاطر.

وتقع مسؤولية تعريف السياسات الإنمائية لمجتمع المعلومات التي تعكس قيمتها الخاصة، وتوفير الموارد الضرورية لتحقيقها على كاهل كل دولة. ويشمل ذلك سبل الوقاية والكفاح ضد الجريمة السيبرانية.

ويلزم لكي يتم احتواء الجريمة السيبرانية بصورة عالمية، مركزية ومنسقة وجود استجابة على المستوى السياسي والاقتصادي والقانوني والتكنولوجي، أي استجابة يعتمدها جميع الفرقاء في السلسلة الرقمية كشركاء مزاملين في الأمن.

2.6.2.I سيادة الدولة

تتعارض الرغبة في اتباع البساطة والفعالية في الأمن مع تعقُّد الاحتياجات والبيئات الأمر الذي يجعل إسناد الخدمات وأمن الأنظمة والمعلومات إلى موردين متخصصين خارجيين أمراً أكثر جاذبية. ويخلق هذا الاتجاه درجة عالية أو كلية من التبعية وهذه من المخاطر الرئيسية للأمن. وعلى الدول أن تحاذر من أن تصبح معتمدة في إدارتها الاستراتيجية والتكتيكية والتشغيلية لأمنها على كيانات خارجية تقع خارج سيطرتها.

وللحكومات دور في فرض ما يلي:

- بناء القدرات الأمنية (الأمن بالتغيب) اليسيرة الاستعمال، والتي تفهم بالحَدْس، وتكون شفافة وقابلة للتحقق منها؛
- جعل الأفراد والمنظمات ينأون بأنفسهم عن المواقف الخطرة (بتفادي عمل التشكيلات القابلة للاقتحام، والسلوك الخطر والتبعية الزائدة، إلخ)؛
- الامتثال لمعايير الأمن؛
- تقليل خطورة نقاط التعرض في التكنولوجيات والحلول الأمنية.

7.2.I البُعد الاقتصادي

ليس مناط الأمن كسب المال وإنما تفادي فقده، فعلى الرغم من أنه قد يبدو من الأمور المباشرة نسبياً تقدير تكلفة الأمن (الميزانيات المرتبطة به، وتكلفة نواتج الأمن، التدريب، إلخ) فإن تقدير إرباحية الأمن أمر أكثر صعوبة. وإذا اتبع المرء نهجاً شخصياً، لأمكنه افتراض أن التدابير الأمنية تمتلك في ثناياها الذاتية "شكلاً سالباً" من أشكال الفعالية يحول دون حدوث خسائر محتملة معينة.

غير أنه من الصعب حساب تكلفة الأمن والتكاليف المرتبطة بالخسائر الناجمة عن الحوادث والأخطاء أو الأعمال الخبيثة. فاحتياجات المنظمة هي التي تحدد تكلفة الأمن، وترتهن بالموجودات التي يراد حمايتها وتكلفة الأضرار الناجمة عن عدم كفاية الأمن. وهكذا لا يوجد رد جاهز عن الأسئلة التالية:

- كيف يمكن تقييم تعرض المنظمة للمخاطر، وبخاصة المخاطر المتكررة الناجمة عن الارتباط البيني للبنى التحتية فيما بين المنظمات؟
- كيف يمكن للتكاليف غير المباشرة الناجمة عن عدم توافر الأمن أن تُقَيَّم، كذلك التكاليف المرتبطة بالأضرار التي تلحق بصورة المنظمة أو بالتجسس؟
- بماذا يمكن للأمن أن يفيد المنظمة التي تنفذه؟
- ما هي القيمة الاقتصادية للأمن؟
- ما هو مردود الأموال التي تُنفق على الأمن؟

ويجب فهم القيمة الاقتصادية للأمن بأوسع المعاني الاجتماعية، مع مراعاة تأثير التكنولوجيات الجديدة على الأفراد والمنظمات والدول. ولا يمكن اختصار تلك القيمة لتعني فقط تكاليف التركيب والصيانة.

8.2.I البعد الاجتماعي

من المهم جعل جميع المشتركين في الشبكة الدولية للمعلومات يدركون أهمية فهم الأمن فهماً سليماً، وكذلك الخطوات الأساسية التي تقوي مستوى الأمن لو أنها صيغت صياغة واضحة وعُرِّفت ونفذت بذكاء.

ويلزم إجراء الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسؤول، بحيث تغطي التحديات والمخاطر وتدابير الأمن الوقائية والرادعة لأجل تثقيف جميع المواطنين السيبرانيين للتعاطي مع عملية الأمن.

وينبغي التشديد على واجب الأمن، والمسؤولية الفردية والتدابير الرادعة، وكذلك التداعيات المحتملة – في إطار القانون الجنائي – التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن. وبصورة أكثر عمومية، فإن من الضروري توفير التثقيف والتدريب على تكنولوجيا المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة. وينبغي أن يقتصر الوعي بالقضايا الأمنية على تشجيع ثقافة أمنية معينة. إذْ يجب للثقافة الأمنية أن تُغْرس داخل ثقافة تكنولوجيا المعلومات، وربما حدث ذلك في شكل تصريح مستعمل الحاسوب الذي يوصي به النادي المعلوماتي للمشروعات الفرنسية الكبرى (*Club Informatique des Grandes Entreprises Françaises*) ((CIGREF)). وهو عبارة عن رابطة تضم المؤسسات الفرنسية المعنية بقضايا تكنولوجيا المعلومات[7].

ينبغي جعل الشبكة الدولية للمعلومات مشاعاً مفتوحاً للجميع بحيث يمكن لجميع المواطنين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية زائدة. ويحتاج الأمر إلى بلورة مدونة أخلاقيات للأمن تكون مقبولة ومحترمة من جانب جميع العاملين في الفضاء السيبراني.

9.2.I البُعْد القانوني

1.9.2.I عامل النجاح الحرج

إن بعض هيئات القانون الوطني والاتفاقيات الدولية تُلزم المنظمات قانونياً باتباع التدابير الأمنية. ونتيجة لذلك فإن مدراء المنظمة، ومسؤولي الأمن لديهم بحكم السلطة المخولة لهم، عليهم التزام إزاء تدابير الأمن (وليس التزاماً بتحقيق نتائج معينة). إن أي كيان قانوني يقترف ذلة أمنية تؤدي إلى مخالفة قد يتحمل مسؤولية ذات طبيعة جنائية، أو مدنية أو إدارية من جراء ذلك. وسواء تم إثبات هذه المسؤولية أم لا فلا تأثير له على المسؤولية الجنائية التي يتحملها المذنبون للأفراد المذنبين باقتراف المخالفة.

إن سَن التشريع الملائم بشأن معالجة البيانات يجعل بالإمكان تقوية ثقة الشركاء الاقتصاديين بالبنية الأساسية الوطنية، مما يسهم في التنمية الاقتصادية للبلد. وهكذا، فإن مساعدتهم في خلق سياق مواتٍ لتبادل البيانات يعتمد على الامتثال للقانون، وبجعلهم عاملاً في إقبال الجمهور العام على الخدمات القائمة على المعلومات والاتصالات. ويمكن النظر إلى التشريع والأمن كعمادين من عُمُد الاقتصاد الوطني. فالأمن السيبراني الذي يفهم على أساس الثقة والجودة يضع الأسس لتطوير اقتصاد خدمات سليم.

2.9.2.I تعزيز التشريع والإنفاذ

لا تخضع الجريمة السيبرانية، في الوقت الحالي، للسيطرة القوية كما يتضح من تفحص المرء للإحصاءات السنوية التي ينتجها معهد أمن الحاسوب (CSI)[8] أو الفريق المعني بطوارئ الحاسوب والاستجابة لها (CERT)[9] وهكذا يمكن رؤية كيف أن تدابير الأمن المتخذة من جانب المنظمات تميل إلى توفير الحماية لبيئة معينة، في سياق خاص، ولكنها عاجزة عن منع النشاط الإجرامي عبر الإنترنت. وتتعلق أسباب هذه الحالة، بصفة خاصة بما يلي:

- طبيعة الجريمة السيبرانية (الأتمتة، البرمجيات الخبيثة الذكية، التشغيل عن بعد)؛
- السهولة والإفلات من العقاب اللذين يُمكن للمتسللين من خلالهما انتحال هويات المستخدمين الشرعيين وبذلك يقضون على قدرة النظام القانوني على تحديد هويات مرتكبي العمل الإجرامي؛

7 www.cigref.fr
8 www.gocsi.com
9 www.cert.org

- الحاجة إلى حل مشاكل الاختصاص قبيل إجراء التحقيق؛
- نقص الموارد البشرية والمادية داخل الخدمات المسؤولة عن مكافحة الأعمال السيبرانية الإجرامية؛
- الطبيعة عبر الوطنية للجريمة السيبرانية التي تحتم الدعوات المتكررة للمساعدة الدولية والتعاون القضائي، وفرض مُهْلاتْ زمنية متعارضة مع سرعة المهاجمين وطلب الاستئناف الفوري لتشغيل أنظمة تكنولوجيا المعلومات التي تعرضت للهجوم؛
- عدم وجود فئات مناسبة لدى بعض الولايات القضائية؛
- التعريف غير الكافي والطبيعة المؤقتة لمعظم القرائن ذات الصلة بتكنولوجيا المعلومات.

ولكل هذه الأسباب مجتمعة، يظل النظام القانوني غير فعال في سياق الإنترنت. يضاف إلى ذلك أنه مثلما أن هناك سواتر للتهرب من الضرائب هناك مرافئ قانونية آمنة. إن تكاثر الجريمة ذات الصلة بالحاسوب ليس بالضرورة علامة على عدم وجود قدر كافٍ من القوانين. فالقوانين القائمة تغطي بالفعل الكثير من أنشطة مجرمي ومتسللي تكنولوجيا المعلومات.

ما يؤاخذ عليه القانون بصفة عامة، يؤاخذ عليه في عالم الاتصالات

يلزم سن تشريع جديد نابع من الحاجة إلى تعريف إطار قانوني مناسب مصمم ليناسب استخدام التكنولوجيات الجديدة وذلك لإكمال الكثير من القوانين الحالية التي تنطبق أيضاً بطبيعة الحال على الفضاء السيبراني.

ولا يكفي تعزيز التشريع ما لم تتوافر وسائل تطبيق هذا التعزيز. ويكون القانون قليل النفع ما لم يكن إنفاذ القانون من القوة بحيث يسمح بجمع وتحليل القرائن والتعرف على مقترفي الأعمال الإجرامية وتقديمهم إلى القضاء. وإذا كان لدى المتسللين ثقة في أنهم سيهربون من العقاب فإن هذا يكون دليلاً على عدم فعالية القانون.

3.9.2.I مكافحة الجريمة السيبرانية واحترام السرية الرقمية في نفس الوقت: حل توفيقي مخادع

إن الوسائل اللازمة لمكافحة التهديد الدولي المتنامي للجريمة السيبرانية لتحتاج إلى إطار قانوني تم توفيقه وتنسيقه على المستوى الدولي ويمكن تطبيقه بفعالية، مع وسائل التعاون الدولي الحقيقي على مستوى السلطات الشرطية والقضائية.

وتقع على كاهل الحكومات الوطنية مسؤوليات مهمة لتأمين الأمن السيبراني. ويصدق ذلك بصفة خاصة على تعريف الإطار القانوني المناسب، أي الإطار المُوحد الشكل والقابل للتطبيق لأجل التشجيع على وجود ثقافة أمنية تحترم حق الأفراد في السرية الرقمية وتُعزز في نفس الوقت جهود مكافحة الجريمة السيبرانية.

ويجب على النضال ضد الجريمة السيبرانية أن يتمثل هدفاً رئيسياً هو حماية الأفراد والمنظمات والبلدان مع وضع المبادئ الأساسية للديمقراطية نصب الأعين.

إن الأدوات التي تستخدم لمكافحة الجريمة السيبرانية تنطوي على قدر محتمل بحقوق الإنسان، وربما قوضت سرية المعلومات الشخصية. فالأمن يحتاج إلى المراقبة والتحقق وعمل سجلات البيانات الشخصية. كما أن عمليات التدقيق والموازنة تكون ضرورية لمنع حالات سوء استغلال القوة أو المراكز، ومقاومة إغراءات الطرق الشمولية، ضمان احترام حقوق الإنسان بما في ذلك الحق في الخصوصية السيبرانية، وحماية المعلومات السرية الشخصية.

وبالإضافة إلى التوجيه الأوروبي الصادر عام 1995، سُنَتْ قوانين أخرى لحماية المعلومات الشخصية لدى العديد من البلدان لعدة سنوات:

ألمانيا:	قانون 21 يناير 1977
الأرجنتين:	قانون حماية المعلومات الشخصية، 1996
النمسا:	قانون 18 أكتوبر 1978

أستراليا	قانون سري، 1978
بلجيكا:	قانون 8 ديسمبر 1992
كندا:	قانون حماية المعلومات الخاصة، 1982
الدانمارك:	قانون 8 يونيو 1978
إسبانيا:	قانون 29 أكتوبر 1992
الولايات المتحدة الأمريكية:	قانون بشأن حماية الحقوق الفردية، 1974، القانون بشأن قواعد بيانات المعلومات الخاصة، 1988
فنلندا:	قانون 30 أبريل 1987
فرنسا:	قانون بشأن تكنولوجيا المعلومات والحرية الصادر في 6 يناير 1978، والذي عُدِلَ في 2004
اليونان:	قانون 29 مارس 1997
هنغاريا:	قانون بشأن حماية المعلومات الخاصة وتوصيل المعلومات الخاصة وتوصيل المعلومات العامة، 1992.
أيرلندا:	قانون 13 يوليو 1988
أيسلندا:	قانون بشأن تسجيل المعلومات الشخصية، 1981
إسرائيل:	قانون بشأن حماية السرية، 1981، 1985، 1996، قانون بشأن حماية المعلومات في الإدارة، 1986
ايطاليا:	قانون 31 ديسمبر 1996
اليابان:	قانون بشأن حماية المعلومات الشخصية المعالجة بالحاسوب، 1988
لكسمبرغ:	قانون 31 مارس 1979
النرويج:	قانون بشأن سجلات البيانات الشخصية، 1978
نيوزيلندا:	قانون بشأن المعلومات الرسمية، 1982
هولندا:	قانون 28 ديسمبر 1988
بولندا:	قانون بشأن حماية المعلومات الشخصية، 1997
البرتغال:	قانون 29 أبريل 1991
الجمهورية التشيكية:	قانون بشأن حماية المعلومات الشخصية في أنظمة الحاسوب، 1995
المملكة المتحدة:	قانون 12 يوليو 1988
روسيا:	القانون الاتحادي بشأن المعلومات، تجهيز المعلومات وحماية المعلومات
سلوفينيا:	قانون بشأن حماية المعلومات، 1990
السويد:	11 مايو 1973
سويسرا:	القانون الاتحادي لحماية المعلومات، 1992
تايوان:	قانون بشأن حماية المعلومات، 1995

4.9.2.I التشريعات الدولية بشأن الجريمة السيبرانية

كانت الاتفاقية بشأن الجريمة السيبرانية[10] التي أبرمها مجلس أوروبا (واعُتِمدَت في بروكسل يوم 23 نوفمبر 2001) هي أول اتفاقية توضع للتعاطي مع الطابع الدولي للجريمة السيبرانية ودخلت تلك الاتفاقية حيز السريان في يوليو 2004 (في أعقاب التصديق عليها من جانب خمسة بلدان موقعة، كان من الضروري لثلاثة بلدان منها أن تكون من مجلس أوروبا). وتضم الاتفاقية النقاط التالية:

- القانون الجنائي الأساسي:
  - المخالفات التي ترتكب ضد السرية، والسلامة والتوافر الخاص ببيانات وأنظمة الحاسوب؛
  - المخالفات ذات الصلة بالحاسوب؛
  - المخالفات ذات الصلة بمخالفات حقوق التأليف والنشر والحقوق ذات الصلة.
- قانون الإجراءات:
  - المحافظة المُسَرَّعَة على بيانات الحاسوب وحركة البيانات والإفشاء السريع للأخيرة للسلطات المختصة؛
  - حفظ وصيانة سلامة بيانات الحاسوب لفترة من الوقت تمتد حسب الضرورة وذلك لتمكين السلطات المختصة من طلب إشهارها؛
  - أمر الإنتاج؛
  - البحث عن بيانات الحاسوب المختزنة والإمساك بها؛
  - جميع بيانات الحاسوب في الزمن الحقيقي؛
  - الحماية الكافية لحقوق الإنسان والحريات؛
- وينبغي لكل دولة أن تعتمد التدابير التشريعية وغيرها من التدابير الضرورية لفرض ولايتها القضائية على المخالفات التالية ودون الإضرار بقانونها المحلي:
  - عندما يحدث عن قصد النفاذ إلى كل أو إلى أي جزء من النظام الحاسوبي بدون وجه حق؛
  - عندما يحدث عن قصد الاعتراض بدون وجه حق لعمليات إرسال البيانات غير العامة إلى أو من نظام حاسوبي أو داخله؛
  - عندما يحدث عن قصد، إتلاف، شطب، تدهور، أو تغيير أو كبت بيانات حاسوبية بدون وجه حق؛
  - عندما تحدث عن قصد، إعاقة خطيرة لأداء نظام بدون وجه حق؛
  - إنتاج، بيع، الشراء للاستخدام، استيراد، توزيع أو توفير البيانات بطرق أخرى لأداة مُصمَمة أو مُجهَزة لغرض اقتراف أي من هذه المخالفات؛
  - عندما يحدث عن قصد وبدون قصد وجه حق، إدخال، تغيير، شطب أو كبت بيانات حاسوبية مما ينتج عنه بيانات غير يقينية وذلك بغرض النظر فيها، أو العمل على أساسها لأغراض قانونية كما لو كانت بيانات يقينية؛
  - عندما يحدث عن قصد وبدون وجه حق، التسبب في فقدان شيء مملوك لشخص آخر عن طريق أي مُدْخَل، تغيير، شطب أو كبت لبيانات حاسوبية، أو أي تدخل في أداء نظام حاسوبي بنيةٍ مخادعة أو غير شريفة للحصول، بدون وجه حق، على منفعة اقتصادية للشخص أو لشخص آخر؛
  - التكييف كمخالفات جنائية مساعدة أو المساعدة على ارتكاب أي من تلك المخالفات، وكذلك أي محاولة لاقتراف أي من هذه المخالفات.

[10] www.conventions.coe.int/Treaty/FR/Treaties/Html/185.htm

- وينبغي لكل طرف من الأطراف الموقعة أن يثبت ولايته القضائية على أي مخالفة تقترف:
  - داخل إقليمه؛
  - على ظهر سفينة ترفع علم ذلك البلد؛
  - على يد أي من رعاياها، إذا كانت المخالفة يعاقب عليها جنائياً في مكان ارتكابها، أو إذا ارتُكِبَت المخالفة خارج الولاية القضائية الإقليمية لأي دولة.
- قواعد التعاون الدولي المتصلة بـــ:
  - تسليم المجرمين؛
  - المساعدة المتبادلة لأغراض التحقيق؛
  - الإجراءات الخاصة بالأعمال الجنائية ذات الصلة بأنظمة الحاسوب والبيانات؛
  - جمع القرائن الإلكترونية للعمل الإجرامي.
- خلق شبكة مساعدة متبادلة:
  - متوافرة على مدار 24 ساعة/7 أيام في الأسبوع؛
  - ذات مراكز اتصال وطنية؛
  - بمساعدة فورية في حالة وقوع المخالفات.

تسود الإدارة السياسية للتعامل مع الجريمة السيبرانية على المستوى الدولي. وليست المشكلة هي دائماً عدم وجود القوانين أو المبادئ التوجيهية كتلك التي أعلنتها منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) في عبارة "المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي لأمن شبكات وأنظمة المعلومات – نحو ثقافة أمنية – 2002"[11] (الشكل 7.I)، وإنما هي صعوبة وتعقد المهمة، والموارد الضرورية لتنفيذ أهداف النضال ليس فقط لمكافحة الجريمة السيبرانية وإنما أيضاً الجريمة المنظمة التي تسفر عن تسخير شبكة المعلومات الدولية في أغراض خبيثة.

الشكل 7.I – مبادئ منظمة التعاون والتنمية في الميدان الاقتصادي بشأن أمن المعلومات (يوليو 2002)

الوعي	جميع المشاركين مسؤولون عن أمن الشبكات وأنظمة المعلومات
المسؤولية	جميع الضالعين يشتركون في أمن الأنظمة وشبكات المعلومات
الاستجابة	يجب على المشاركين العمل بصورة متعاونة ومنسقة زمنياً لمنع واكتشاف حوادث الأمن
الأخلاقيات	ينبغي للمشاركين احترام المصالح المشروعة للآخرين
الديمقراطية	ينبغي لأمن أنظمة وشبكات المعلومات أن يكون متوافقاً مع القيم الأساسية للمجتمع الديمقراطي
تقييم المخاطر	ينبغي للمشاركين إجراء تقييمات للمخاطر
تصميم الأمن والتنفيذ	ينبغي للمشاركين إدراج الأمن كعنصر أساسي في أنظمة وشبكات المعلومات
إدارة الأمن	ينبغي للمشاركين اعتماد نهج شامل تجاه إدارة الأمن
إعادة التقييم	ينبغي للمشاركين استعراض، وإعادة تقييم أمن أنظمة وشبكات المعلومات، وإدخال التعديلات المناسبة على السياسات العامة للأمن وممارساته وإجراءاته وتدابيره.

[11] انظر الملحق F من هذا الدليل – www.oecd.org/dataoecd/16/22/15582260.pdf.

10.2.I أساسيات الأمن السيبراني

يجب أن تسهم الحلول الأمنية في الوفاء بمعايير الأمن الأساسية مثل التوافر والسلامة والسرية (the AIC criteria). أما المعايير الأخرى التي غالباً ما تساق إليها الإشارة في هذا السياق فهي الاستيقان (الذي يجعل من الممكن التحقق من هوية كيان ما)، وعدم الرفض والمساعدة (التي تجعل من الممكن التحقق من الإجراءات أو الوقائع التي تمت) (انظر الشكل 8.I).

1.10.2.I التوافر

لتأمين توافر الخدمات، والأنظمة، والبيانات، يجب تحديد الأحجام المناسبة لأنظمة البنية التحتية، وأن تتوافر لها الأعداد الاحتياطية البديلة الضرورية، يضاف إلى ذلك أنه يجب توفير الإدارة التشغيلية للموارد والخدمات.

ويقاس التوافر على أساس الفترة الزمنية التي تكون الخدمة المقدمة خلالها في حالة تشغيل. كما أن الحجم المحتمل للأعمال التي يمكن تناولها أثناء فترة توافر الخدمات هو الذي يحدد قدرة المورد (المُخدم أو الشبكة، مثلاً). وثمة ارتباط شديد بين التوافر ويُسْر النفاذية (accessibility).

2.10.2.I السلامة

إن المحافظة على استقامة البيانات أو معالجة الخدمات تعني وقايتها من التعديل العارض أو المقصود، ومن التلاعب والتدمير. وهذا أمر لازم لضمان أن تبقى صحيحة ودقيقة.

وللحيلولة دون التلاعب، يلزم وجود طريقة للتصديق على أنها لم تتعرض للتعديل أثناء الخزن أو النقل.

إن السبيل الوحيد لضمان سلامة البيانات هو حماية تلك البيانات المعمول بها من أساليب اقتناص المعلومات عن طريق تحويل مسارها الأصلي (Tapping techniques) والتي يمكن استخدامها لتعديل المعلومات المُعْترضَة. ويمكن توفير هذه الحماية بواسطة آليات أمن مثل:

- مراقبة صارمة على النفاذ؛
- تجفير البيانات؛
- الحماية من الفيروسات والديدان وأحصنة طروادة.

الشكل 8.I – أساسيات الأمن السيبراني

يجب على النظام أن ...	أهداف الأمن	أدوات الأمن
... يكون قابلاً للاستخدام	• التوافر • الاستدامة • الاستمرار • الثقة	• تحديد الأبعاد • هامش احتياطي (أطناب) • تدابير التشغيل والمؤازرة
... يعمل بصورة سليمة	• أمن التشغيل • الاعتمادية • المتانة • الاستمرارية • الصواب	• التصميم • الأداء • علم تصميم الآلات بما يناسب الجسم البشري • نوعية الخدمة • صيانة التشغيل
... يوفر النفاذ للكيانات المرخص لها (بينما يمنع النفاذ غير المرخص)	• السرية • السلامة (لا تغييرات)	• التحكم في النفاذ • الاستيقان • مراقبة الأخطاء • التأكد من التماسك • التجفير
... يتحقق من الإجراءات	• عدم الرفض • اليقين (بعيد عن الشك) • عدم المماراة	• شهادة التصديق • التسجيل، إمكانية الاقتفاء • التوقيع الإلكتروني • آليات البرهان

3.10.2.I السرية

السرية هي الحفاظ على سرية المعلومات، وتدفقات المعلومات، والمعاملات، والخدمات أو الإجراءات التي تجري في الفضاء السيبراني. وهي تضمن حماية الموارد من الإفشاء غير المرخص به.

يمكن تنفيذ السرية عن طريق مراقبة النفاذ والتجفير.

يساعد التجفير على حماية سرية المعلومات أثناء الإرسال أو التخزين بتحويلها إلى شكل غير مفهوم لأي شخص لا يمتلك وسائل فَكْ هذا التجفير.

4.10.2.I تحديد الهوية والاستيقان

إن الهدف من الاستيقان هو إماطة أي قدر من عدم اليقين عن هوية مَوْرِدْ ما. وهو يفترض مسبقاً أن جميع الكيانات (عتاد الحاسوب، البرمجيات والأشخاص) قد تم تحديدها بصورة سليمة، وأن خاصيات معينة يمكن أن تنهض كبرهان على تحديد هوياتهم. وبصفة خاصة، تحتاج أنظمة مراقبة النفاذ ذات الأساس المنطقي إلى موارد تكنولوجيا المعلومات لتحديد هويات الكيانات التي ستتم إدارتها والاستيقان من ذلك.

ويتم تنفيذ تدابير تحديد الهوية والاستيقان للمساعدة على تحقيق ما يلي:

- سرية البيانات وسلامتها (فالنفاذ إلى الموارد يقتصر على المستعملين المرخص لهم، وتتم حماية الموارد من التغيير على يد أي شخص من الأشخاص غير المرخص لهم بذلك)؛
- عدم الرفض والاستدلال على الفاعل (يمكن اقتفاء الإجراءات حتى الوصول إلى كيان معروف الهوية ومُستيقن منه)، إمكانية اقتفاء أثر الرسائل والعمليات (ويمكن اقتفاء أثر عمليات الإرسال إلى كيان معروف الهوية ومستيقن منه)، والبرهان على المَقْصِدْ (يمكن البرهنة على أن الرسالة موجهة إلى كيان محدد الهوية ومستيقن منه).

5.10.2.I عدم الرفض

من الضروري في بعض الظروف التحقق من أن واقعة ما أو معاملة ما قد تمت بالفعل. فعدم الرفض (عدم التنصل)، يكون مرتبطاً بمفاهيم المساءلة، والاستدلال على الفاعل وإمكانية الاقتفاء وفي بعض الحالات، القابلية للمراجعة.

إن تحديد المسؤولية يفترض مسبقاً وجود آليات للتحقق من الأفراد والاستدلال على الفاعل. إن إمكانية تسجيل المعلومات للتمكين من متابعة أداء عمل ما تصبح مهمة حينما تكون هناك حاجة لإعادة تشكيل سياق الوقائع وبصفة خاصة عند إجراء تحقيقات حاسوبية للعثور على عنوانٍ لنظام كان يرسل البيانات، مثلاً. إن المعلومات اللازمة لإجراء تحليل تالٍ لأغراض المراجعة على النظام تحتاج إلى المحافظة عليها (تسجيل المعلومات). وتسمى هذه بقابلية التدقيق لدى النظام.

6.10.2.I الأمن المادي

إن المسافات الفاصلة بين مواقع محطات العمل، والمخدمات، ومساحات وخدمات تكنولوجيا المعلومات (تكييف الهواء، لوحات الإمداد بالكهرباء، إلخ) تحتاج إلى حماية مادية ضد النفاذ غير المرخص به ومن الحوادث (الحريق، التلفيات الناتجة عن المياه، إلخ). والأمن المادي هو النوع الجوهري للغاية والشائع للغاية من أنواع الرقابة على أنظمة تكنولوجيا المعلومات.

7.10.2.I الحلول الأمنية

بالنظر إلى الواقع اليومي للمشاكل المتصلة بالأمن بالنسبة لمعظم البيانات التحتية الأساسية، وتكاثر الحلول المقترحة وازدهار سوق الأمن، يثور عدد من الأسئلة مثل:

- هل الحلول الأمنية المقترحة متماشية مع المتطلبات؟
- هل هي مركبة ومدارة بصورة سليمة؟
- هل يمكن استعمالها، أو تكييفها مع بيئة فوارة بالتطورات؟
- هل يمكنها التخفيف من التركيز غير المتوازن للسلطة التي يتمتع بها مسؤول النظام؟
- كيف يمكن استعمالها لمعالجة المشكلات الأمنية التي تنشأ عن الإهمال، والخطأ البشري، وعيوب التصاميم، ومشاكل التركيب وسوء إدارة التكنولوجيا والحلول الأمنية؟
- وأشياء أخرى.

الجـــزء II

مكافحة الجريمة السيبرانية

القسم 1.II – الجريمة السيبرانية

1.1.II الجريمة ذات الصلة بالحاسوب والجريمة السيبرانية

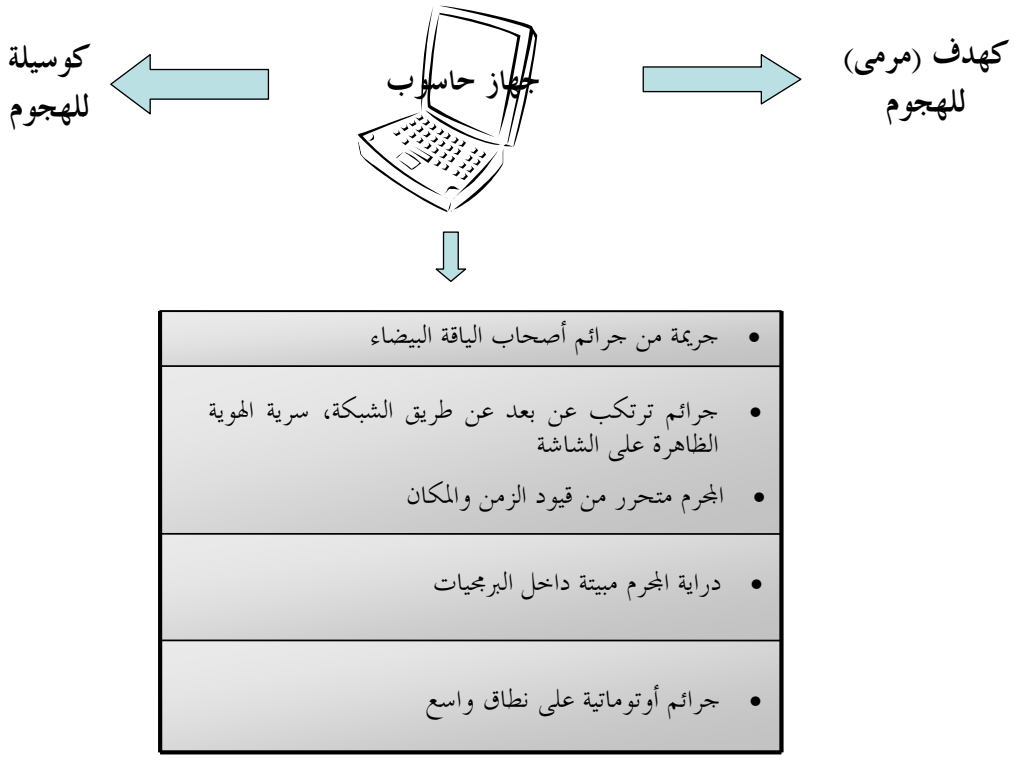
تتكاتف نقاط التعرض في التكنولوجيا الرقمية والتحكم غير الكافي فيها تجتمع معاً لتخلق بيئة من عدم الأمن. وبالطبع، يستغل المجرمون هذه الحالة. ذلك أن تكنولوجيا من التكنولوجيات تنطوي على احتمالات استغلال المجرمين لها لأغراض غير مشروعة، وليست الشبكة الدولية للمعلومات استثناء لذلك كما يدل على ذلك بدرجة كافية الوجود الإجرامي في الفضاء السيبراني.

ففي عام 1983، عرفت منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) الجريمة ذات الصلة بالحاسوب بأنها أي سلوك غير مشروع، غير أخلاقي أو غير مرخص به ويشمل الإرسال أو معالجة المعطيات.

والجريمة المتصلة بالحاسوب هي الجريمة التي يكون فيها النظام الحاسوبي هو هدف الجريمة، ووسيلة ارتكاب الجريمة أو كلاهما، إنها جريمة متصلة بالتكنولوجيا الرقمية، وهي فئة فرعية من جرائم ذوي الياقات البيضاء. والجريمة السيبرانية هي شكل من أشكال الجريمة المرتبطة بالحاسوب وتستخدم تكنولوجيا الشبكة الدولية للمعلومات "الإنترنت" وهي تغطي جميع الجرائم التي ترتكب في الفضاء السيبراني.

وفي العالم الافتراضي (virtual world) يمكن للجريمة أن تكون أوتوماتية، وأن تخلق إمكانيات انتشار الوباء السيبراني على نطاق واسع يمكن أن تنطلق شرارته عن بعد عن طريق الشبكة (تحرير المجرم من القيود الزمنية والمكانية) مع إمكانيات تأخر الإجراء (الشكل 1.II).

الشكل 1.II – طبيعة الجريمة ذات الصلة بالحاسوب



أن تكنولوجيا الشبكة الدولية للمعلومات (الإنترنت) تيسر ارتكاب طائفة واسعة من المخالفات: السرقة، تخريب المعلومات، مخالفات حقوق التأليف والنشر، خيانة الأمانة المهنية، السرقة الرقمية، الملكية الفكرية، توزيع المحتوى بصورة غير مشروعة، هجمات غير تنافسية، التجسس الصناعي، مخالفات العلامة التجارية، التضليل المعلوماتي، منع الخدمة، ومختلف أنواع الغش، إلخ.

من بين الأحداث البارزة في زيادة الوعي بتهديدات الجريمة السيبرانية – بالإضافة إلى البق Y2k الذي وجه الانتباه إلى تعرض البرمجيات، ومدى اعتماد المجتمع على الحواسب – هجمات رفض بالخدمة كتلك التي شنت ضد ياهو Yahoo (10 فبراير 2000)، وهجوم فيرس "I love you" سيئ السمعة (4 مايو 2000). ومنذ ذلك الحين أدت تغطية وسائل الإعلام للهجمات الفيروسية (مثل فيرس كود ريد "Code red" 4 يوليو 2001 أو "نيمدا" في سبتمبر 2001) وهجمات منع الخدمة (كذلك التي شُنَتْ ضد شبكة الـــDNS (مخدم اسم الميدان في سبتمبر 2002) إلى جانب الكثير من الأمثلة الأخرى، مما زاد من وعي الجمهور العام بحقيقة التهديدات التي تعمل عبر الإنترنت. ولا زالت وسائط الأخبار تخصص الوقت الكبير للتوعية بحقيقة المخاطر والتهديدات التي تعمل عبر الشبكة الدولية للمعلومات. وما فتئت وسائل الإعلام الإخبارية تخصص وقتاً كبيراً لتغطية المشاكل المرتبطة بالحاسوب.

2.1.II العوامل التي تجعل الإنترنت جذابة للعناصر الإجرامية

1.2.1.II المحاكاة الافتراضية والعالم الافتراضي

إن فصل العمليات عن الوسائط المادية (إعطائها طبيعة افتراضية)، وأدوات الاتصال التي تشمل التجفير، والاختزال، وإخفاء الهوية الحقيقية: فهذه عوامل يستغلها المجرمون في مختلف البلدان لأجل التعاون بينما يستغنون بها عن الاجتماعات المادية، ويعملون بها بطريقة مرنة ومأمونة وبإفلات كامل من العقاب. فيمكنهم أن يكونوا الفَرق، وأن يخططون للجرائم وينفذوها سواء كان ذلك بصورة تقليدية أو باستخدام تكنولوجيات جديدة. ويسمح النطاق العالمي للإنترنت للمجرمين وأن يعملوا على مستوى عالمي، وعلى نطاق واسع وبسرعة شديدة.

وهذه الإمكانيات القوية التي يخلقها العالم الرقمي والاتصالات تأتي على قمة المشاكل الداخلية المرتبطة بتصميم وتنفيذ تكنولوجيا المعلومات وإدارتها والتحكم فيها، بكل ما يصاحب ذلك من الإغلاق، وتعطل الوظائف، وحدوث أخطاء الجهاز أو الأخطاء البشرية، بل وحتى الكوارث الطبيعية وكذلك الاعتماد المتبادل للبنى الأساسية وكلها تنطوي فعلاً على مستوى معين من عدم الأمان في البنى الأساسية الرقمية.

وهكذا فإن إمكانيات الاستغلال الخبيث لنقاط التعرض رحبة جداً وتتحول في الواقع إلى:

انتحال الهوية، الخُدَعْ، النفاذ غير المرخص به، الاستخدام الاحتيالي للموارد، العدوى، التخريب، التدمير، التلاعب، هتك السرية، سرقة البيانات، الابتزاز التهديدي، والقضاء على الحماية وإنكار الخدمة، إلخ.

وهذا يبين بوضوح السيطرة الناقصة على المخاطر ذات الصلة بالحاسوب ذات المنشأ الجنائي التي تتعرض لها المنظمات، وحدود استراتيجيات الأمن الحالية.

إن الفضاء السيبراني الذي يسمح للمستخدمين بالعمل عن بعد عبر شبكة وهم مستترون وراء شاشة، ليخلق الظروف المثالية للنشاط الإجرامي. وفي الحقيقة أن بعض الأفراد قد يجوسون عبر الحدود فيقومون بالنشاط الإجرامي دون دراية تامة بالطبيعة الإجرامية لأعمالهم.

2.2.1.II التوصيل البيني لشبكات الموارد

إن التوصيل البيني واسع النطاق لشبكات موارد الحاسوب والمعلومات ليجعلها أهدافاً جذابة للجريمة الاقتصادية باستخدام التكنولوجيات الحديثة. كما أن الأشكال المختلفة لهجمات الحاسوب الموجودة تشترك كلها في سمة واحدة ألا وهي الانخفاض النسبي للخطر الواقع على المجرم في مقابل إمكانيات الإضرار والأعطاب التي تتجاوز بكثير الموارد

الضرورية لشن الهجوم. إن انتحال الهوية الإلكترونية، وسهولة التخفي، وإمكانية السيطرة على الحواسيب تجعل من اليسير اقتراف أعمال غير مشروعة دون تعريض المرء لأي خطر جسيم.

3.2.1.II تكاثر عمليات التسلل ونقاط التعرض

إن التوافر واسع النطاق "لعمليات التسلل"، التي تستغل نقاط تعرض نظام ما ومكتبات الهجمات والبرمجيات التي تستفيد من الخبرات الإجرامية، تجعل مهمة اقتراف هجوم حاسوبي أمراً أسهل وهذا، بالإضافة إلى إمكانية العمل الافتراضي. يشجع خبراء الحاسوب ذوي الاتجاهات الإجرامية الذين تتوافر لديهم مهارات الحاسوب أن يترجموا خبراتهم إلى الاستخدام الخبيث. وفي بعض الأحيان، يسهل الفضاء السيبراني الانتقال إلى عمل إجرامي دون إدراك تقريباً.

4.2.1.II الأخطاء ونقاط التعرض

يستغل المجرمون الأخطاء ونقاط التعرض التنظيمية والتقنية للإنترنت، وعدم توافر إطار قانوني منسق بين البلدان، ونقص التنسيق الفعال بين الوكالات الوطنية لإنفاذ القوانين. وقد ينطوي ذلك على أشكال تقليدية للإجرام (الجرائم التقليدية التي يتم اقترافها بواسطة تكنولوجيات جديدة: غسل الأموال، والابتزاز التهديدي والابتزاز إلخ) أو أنواع جديدة من الجرائم القائمة على التكنولوجيات الرقمية: اقتحام الأنظمة، سرقة وقت المعالج، سرقة رموز المصدر، قواعد البيانات إلخ. والبيئة في جميع هذه الحالات مُوصِلة بدرجة استثنائية: أقل قدر ممكن من المخاطر، وتغطية واسعة وأرباح كثيرة.

الشكل 2.II يلخص مصادر نقاط التعرض في البيئة التحتية للإنترنت.

الشكل 2.II – الصفات الرئيسية للإنترنت التي تُستَغل لأغراض إجرامية

5.2.1.II إماطة اللثام عن المجرمين السيبرانيين

والجريمة المتصلة بالحاسوب متقدمة ومعقدة، وتُرتكبُ عادة عبر الحدود الوطنية وغالباً بتأخير زمني. والآثار التي تتركها في الأنظمة غير ملموسة ويصعب تجميعها وخزنها. وهي تأخذ شكل معلومات رقمية مخزونة في جميع أنواع الوسائط: الذاكرة العاملة، نهايات التخزين الطرفية، والأقراص الصلبة والأقراص الخارجية "عصيْ الذاكرة USB"، والمكونات الإلكترونية، وغيرها. وتتمثل المشكلة في كيفية الإمساك بالقرائن المتنوعة الكثيرة التي يتم الحصول عليها أثناء البحث الرقمي. وتوضح الأسئلة التالية إلى أي مدى يظل نطاق مفهوم الدليل الرقمي محيراً لا يمكن الإمساك به:

- كيف تتعرف على البيانات ذات الصلة؟
- كيف تقتفي أثرها؟
- كيف تخزنها؟
- ما هي قواعد الاستدلال القضائية للبرهان؟
- كيف تستعيد الملفات التي شطبت؟
- كيف تبرهن على منشأ الرسالة؟
- كيف تحدد هوية شخص على أساس أثر رقمي فقط، بالنظر إلى صعوبة الربط الأكيد للمعلومات الرقمية بفاعلها المادي (التقدير) وكثرة انتحال الهوية؟
- كيف تثبت أن الدليل الرقمي حاسم في إثبات الحقيقة أمام محكمة (مفهوم الدليل الرقمي)، وأن تعرف أن وسائط الخزن التي أُخِذَ منها الدليل ليست فوق مستوى الشبهات (فمعلومات التاريخ — والوقت تعالج بصورة مختلفة من نظام حاسوبي إلى نظام آخر، وهي عرضة للتلاعب)؟
- إلى آخره.

ومن الأكثر صعوبة الحصول على دليل رقمي عندما يكون الدليل مبعثراً عبر الأنظمة الموجودة لدى مختلف البلدان. وفي مثل هذه الحالات، يعتمد النجاح بالكامل على فعالية التعاون الدولي بين السلطات القانونية وسرعة اتخاذ الإجراءات. إن الاستخدام الفعال لمثل هذا الدليل لتحديد هوية الأفراد تعتمد على سرعة معالجة الطلبات: فإذا كانت المعالجة بطيئة أصبح تحديد الهوية شبه مستحيل.

الشكل 3.II يبين مختلف أنواع المشاكل التي تسببها الأعمال الخبيثة مثل التدمير المادي، أو سرقة المعدات، ومنع النفاذ إلى الأنظمة والبيانات، وعدوى الموارد، والإضرار بصنع القرارات أو عمليات الاتصال عن طريق هجمات منع تقديم الخدمة (أو كنتيجة للتجسس أو اقتحام الأنظمة)، وسرقة المعلومات والتلاعب (وتسخير الرأي حسب الهوى، الحرب – الإعلامية). وهو يوجز الخصائص الرئيسية للجريمة السيبرانية التي تجعل من الصعب تحديد هوية المجرمين.

يضاف إلى ذلك، أن هناك عدم تكافؤ بين مهارات المجرمين الذي يرتكبون جرائم تكنولوجيات – متقدمة وبين الموارد المتوافرة لسلطات إنفاذ القوانين والسلطات القضائية اللازمة للاقتصاص منهم. ذلك أن استخدام تكنولوجيات الحاسوب من جانب هذه السلطات، سواء على المستوى الوطني أو الدولي، يبقى ضعيفاً ويتفاوت بشدة من بلد لآخر.

وفي معظم الحالات، تعتمد الشرطة والسلطات القضائية على طرق التحقيق التقليدية التي تستخدم في حالة الجرائم العادية وذلك للاقتصاص من المجرمين السيبرانيين لكي تتعرف على هوياتهم وتلقي عليهم القبض.

الشكل 3.II – المصاعب التي تعترض تحديد هوية مهاجم

6.2.1.II المرافئ الآمنة رقمياً

يستغل المجرمون الطبيعة اللاإقليمية لشبكة الإنترنت ونقص التشريعات لدى بعض البلدان، التي تُجرِّمْ الجرائم ذات الصلة بالحاسوب وكما تستغل مجموعة حاشدة من الولايات القانونية التي تغطي الإنترنت.

وبصورة أشبه بالمرافئ الضريبية، تسمح المرافئ الآمنة الرقمية باستضافة المخدمات، وتوزيع محتوى غير قانوني أو تقوم بإجراءات غير قانونية بدون خوف من العقاب. إن تركيب مثل هذه المخدمات على أراضي بلدان ضعيفة يخلق مرفأ للعمليات التي تتم عبر الحدود.

إن نقص التنظيم الدولي والرقابة الدولية والطبيعة غير الفعالة للتعاون الدولي في التحقيقات القانونية والمحاكمات تسمح للإنترنت بأن تكون بمثابة حاجزٍ واقٍ للمجرمين.

لا يوجد الآن نهج فعال قانوني أو تقني للتعامل مع مختلف أنواع الجريمة التي يتم رصدها على الإنترنت، مثل:

- القرصنة عالية التنظيم واسعة النطاق الموازية على البرمجيات والأفلام والموسيقى التي اتخذت أبعاداً غير مسبوقة في الفضاء السيبراني؛
- انتهاكات حقوق التأليف والنشر، وخيانة الأمانة المهنية، وانتهاك السرية الرقمية والملكية الفكرية؛
- مخالفات المِلْكية، والسرقة وإتلاف أو تدمير الملكية، والتدخل في ملكية شخص آخر؛
- توزيع المحتوى القانوني؛
- الهجمات على المتنافسين، والتجسس الصناعي، ومخالفات العلامة التجارية، والتضليل الإعلامي وهجمات منع تقديم الخدمة للمتنافسين.

3.1.II الجريمة التقليدية والجريمة السيبرانية

الجريمة السيبرانية هي الامتداد الطبيعي للنشاط الإجرامي العادي، وترتكب الأفعال الإجرامية اليوم عبر الفضاء السيبراني باستخدام الوسائل غير التقليدية بصورة مكملة للجريمة العادية.

إن الإنترنت لا تهيئ فقط ظروفاً مثالية لمشروعات وأنشطة جديدة غير قانونية، إنما تجعل من الممكن أيضاً خلق تنويعات محتملة للاحتيال أو للجرائم الأخرى بواسطة الحاسوب.

وتجعل الإنترنت من اليسير إيجاد واستغلال وسائل جديدة لكسب المال. وهذه السمة الموفرة للقوة، بطبيعة الحال، لا تَخْفي على عالم الإجرام. ذلك أن المجرمين باحتضانهم لتكنولوجيا المعلومات إنما يأملون في زيادة مكاسبهم بينما يقللون إلى أبعد حد من تعرضهم للمخاطر.

4.1.II الجريمة السيبرانية، الجريمة الاقتصادية وغسل الأموال

لا تقتصر الجريمة الاقتصادية عبر الإنترنت على الجريمة المنظمة. ذلك أن تكنولوجيا المعلومات الحديثة والاتصالات تسمح لأفراد منعزلين بالانغماس في الجريمة الاقتصادية سواء بالعمل وحدهم أو بالتنسيق مع مجموعات متفاوتة الأحجام تتشكل لهذا الغرض.

ويمكن للمجرمين أن ينظموا أنفسهم حول تبادل المعلومات وذلك بفضل استخدام تكنولوجيا المعلومات. ويمكن للشبكات أن تُجمع الأفراد والخبرات لتنظيم عصابة إجرامية خائلية (افتراضية Virtual).

ونظراً لارتفاع درجة الخبرة الاقتصادية والمهارات التي تتطلبها الجريمة الاقتصادية، فإنها تكون مرشحة "للتبلور" بفضل تكنولوجيا المعلومات الحديثة.

وتسهم الإنترنت في حيازة المعلومات والمعارف بشأن القوانين والتكنولوجيا، الخ، اللازمة لارتكاب جرائم اقتصادية. ويمكن استعمالها أيضاً في التنقيب عن ضحايا.

وللتكنولوجيات الجديدة تأثير على الجريمة الاقتصادية التي تصبح جزءاً من جِعَابْ المجرمين وتضع المعلومات في صميم استراتيجياتهم وعمليات صناعة القرارات.

يمكن للتكنولوجيات الجديدة أن تسهل جميع أنواع السرقات، والتلاعب، وتخريب المعلومات والاحتيال. وقد استطاع الابتزاز بالتهديد، والابتزاز، وحماية خطط الابتزاز بالتهديد أو الإيذاء وطلبات الفدية أن يقفز قفزة كبيرة إلى الإنترنت.

تتحول موارد المعلومات في حقيقة الأمر إلى رهائن محتملة في أيدي المجرمين السيبرانيين. فقد حول المبتزون عملياتهم إلى الفضاء السيبراني، ويمكن لأي أحد أن يجد نفسه فجأة ضحية لمحاولة ابتزاز تهديدي، أو تضليل أو دعاية. يضاف إلى ذلك، أن الانفجار في سرقة الهويات الذي يحدث منذ 2003 يدلل على منافع الغفلية التي تتيحها الإنترنت، واستخدام هويات زائفة لتفادي الملاحقة القضائية أو المسؤولية الجنائية أو الإرهابية التي لم يغفل عنها المجرمون. ذلك أن انتحال الهوية، التي تتم بالفعل على الإنترنت، من العوامل الداخلة في الأنشطة غير المشروعة.

ومثلهم مثل جميع المجرمين الذين يستغلون البنى التحتية التقنية القائمة، يستخدم غسالو الأموال الإنترنت بصورة متزايدة للحصول على الأموال التي يتم توليدها بواسطة الأنشطة الإجرامية مثل تهريب المخدرات، وتهريب الأسلحة، والرشوة، والبغاء، وسوء استغلال الأطفال، والتحايل الضريبي، إلخ وتحريك هذه الأنشطة إلى حيز الأعمال القانونية.

وعلى الرغم من أن غسيل الأموال لا يلقي الإبلاغ الكافي عنه، وغالباً ما يكون غير مرئي، فإنه يزداد شهرة على الإنترنت. فالإنترنت أداة مثالية له نظراً لطبيعتها الخائلية (الغُفْلِيَة، الفضاء السيبراني وسرعة التحويل) وتحررها من القيود الإقليمية (طبيعتها العابرة للحدود، وتعارض الاختصاصات والولايات القضائية). وهو ما تعلم عملاء غسل

الأموال استغلاله. والإنترنت تجعل من الممكن تحويل الأموال ذات المنشأ الإجرامي إلى دوائر اقتصادية قانونية وذلك باستخدام الحوالات المالية والاستثمار والرسملة.

فالاستثمارات والمقامرة والتجارة على شبكة الإنترنت، كبيع سلع وخدمات خيالية مقابل نقود حقيقية، تجعل في المستطاع توليد دخول تبدو مشروعة ويصعب رصدها ويكاد يستحيل مقاضاتها. فالعمليات المصرفية الإلكترونية والعمليات العقارية عبر الشبكة، واستخدام شركات كواجهات خائلية والنقد الإلكتروني يمكن استخدام كل ذلك في غسل غنائم الجريمة. والمستعملون العاديون قد يدعمون عن جهل غسل الأموال عندما يستخدمون خدمات خائلية معينة. كما أن المنظمات التجارية قد تصبح دون قصد ضالعة في ذلك بكل ما يرافق ذلك من تداعيات كارثية من الناحيتين القانونية والتجارية. وهذا مصدر رئيسي للمخاطر بالنسبة للشركات.

ويوجد الآن عدد قليل من الوسائل الفعالة للتحكم في هذه الظاهرة الخاصة بغسل الأموال المتصل بتكنولوجيا المعلومات.

5.1.II الجريمة السيبرانية – امتداد للجريمة العادية

تتخذ الجريمة السيبرانية في الغالب الأعم شكل الجريمة العادية، وهي غير مرئية إلى حد كبير ومع ذلك فهي قوية بسبب التوصيل الشبكي بين الموارد والأفراد. فليست الشركات وحدها وإنما تكنولوجيا المعلومات الخاصة بها أيضاً وأصولها من المعلومات يمكن أن تصبح أهدافاً مغرية بالنسبة للتنظيمات الإجرامية الساعية للكسب. وهذا تهديد استراتيجي، حيث إن المال يمكث لدى أنظمة المعلومات، في المؤسسات، وفي صناديق المعاشات التقاعدية إلخ. وليس فقط لدى المصارف.

إن الشركات بفتحها أبوابها أمام الإنترنت، عبر مخدمات الشبكة، والبوابات والبريد الإلكتروني، إنما تعرض أنفسها لخطر شد الانتباه الإجرامي لها وتعطي للمجرمين موطئ قدم احتمالي. وعلى الرغم من أن الإنترنت أداة اتصال قوية، فإنها أيضاً بيئة فوضوية، معقدة وديناميكية ومعادية يمكن استخدامها لتقويض المنظمة ولأن تكون مطية لارتكاب الجرائم. وينبغي معاملة الإنترنت بحيطة كمنطقة ترتكب فيها جرائم كبرى. وبالنظر إلى الأهمية التي توليها المنظمات لوجود الإنترنت فإنها تسهم على أرجح الاحتمالات في توسيع نطاق الإجرام ليصل إلى الإنترنت.

يواجه الأمن القومي اليوم تحديات تتزي بزي التهديدات الإجرامية المرتبطة بتكنولوجيا المعلومات. وتقع تكنولوجيا المعلومات في الصميم من فكرة الحرب المعلوماتية، التي تكون أهدافها اقتصادية بالدرجة الأولى، وهي الحرب التي يمكن أن تترتب عليها تأثيرات ضخمة على سلوك العمليات التجارية. فالإنترنت لا تجعل من الممكن فقط التلاعب بالمعلومات، وإنما هي أيضاً طاحونة شائعات مثالية يمكن أن تغذى بالوقود الحملات الرامية إلى نشر المعلومات المضللة أو عدم اليقين. وهي تيسر كذلك الجاسوسية وأنشطة جمع المعلومات الأخرى نظراً للسهولة التي يمكن بها اعتراض سبيل المعلومات المسافرة عبر الإنترنت.

6.1.II الجريمة السيبرانية والإرهاب

يمكن للجريمة السيبرانية أن تكتسب بعداً إرهابياً عندما تكون الأنظمة المستهدفة جزءاً من بنية تحتية حرجة. ذلك أن تعرض البنى التحتية الأساسية في بلد ما (كالطاقة، والمياه، والنقل، ولوجستيات الأغذية، والاتصالات، والصرافة، والمالية، والخدمات الطبية، والمهام التي تؤديها الحكومة، إلخ) يزداد كلما تعمقت استخدامات تكنولوجيات الإنترنت.

ويلزم التشديد بصفة خاصة على توليد الطاقة الكهربية وأنظمة التوزيع الضرورية لتشغيل معظم البنى التحتية. ويبدو أن من الأهداف الرئيسية للإرهابيين السيبرانيين السيطرة على عناصر البنية التحتية الحرجة كما يتبدى ذلك من الزيادة في عدد عمليات التنقيب scans (كالبحث عن نقاط التعرض التي يمكن استخدامها للتسلل إلى النظام في وقت ما مستقبلاً) واستهداف مشغلي البنية التحتية.

ولا يوجد تعريف متفق عليه لما يمثل الإرهاب السيبراني في الوقت الحالي. وقد يكون أبسط تعريف له هو اعتبار الإرهاب هو الإرهاب الذي يُقْتَرف في الفضاء السيبراني. فالإرهاب، بدوره، يُفهم على أنه يعني الاستخدام المنظم للعنف لتحقيق أهداف سياسية.

ومن المُبَرَرْ تماماً أن نتساءل عما إذا كان انهيار الإنترنت، أو جزء منها، نتيجة لأعمال خبيثة قد لا يغرس الرعب في قلوب مجتمع مستخدمي الشبكة، وبعض مجموعات النشطين الاقتصاديين والجمهور العام.

أو، أننا قد نكون – بصفة عامة – نتعامل مع حوادث إرهاب اقتصادي يرمي إلى إلحاق الضرر بالمنظمات التي تستخدم الإنترنت للقيام بأنشطتها.

إن مصطلح الإرهاب السيبراني الذي كثر تداوله منذ هجمات 11 سبتمبر، يجب استخدامه بتحفظ. ولا ينبغي أن ننسى أن أول حالة قوبلت بطنطنة إعلانية واسعة لهجمات رفض تقديم الخدمة DDOS يوم 10 مايو 2000 كانت من عمل شخص عمره 15 عاماً كان يحمل اسم شهرة "مافيا بوي" وكان ذلك الشاب قد تم التعرف عليه وألقى القبض عليه بعد ذلك بعدة أشهر. وعلى الرغم من أن أسباب هذه الأعمال لا تزال غير معروفة، فإنه من غير المحتمل إلى حد بعيد أنها كانت أعمالاً ذات طابع سياسي.

ولو أن ذلك الهجوم كان قد حدث عقب أحداث 11 سبتمبر، فلربما كان سيصنف فوراً كإرهاب سيبراني.

وفي غياب معلومات محددة، كمذكرة من المهاجمين بشأن هويتهم يكون من الصعب عَزو الهجوم للإرهاب السيبراني.

إن مصطلح الإرهاب السيبراني يغطي قائمة غامضة جداً من التهديدات الجديدة، كما أن من الصعب التكهن بالدوافع أو الأهداف المحتملة للمهاجم المجهول أو مجموعة المهاجمين. فعندما يكون الشيء الوحيد المعروف هو هدف الهجوم، فإنه يكون من المشكوك فيه أن نقدر استقرائياً التفكير الذي ربما يكون وراء المتسلل أو الإرهابي أو المُرتزق، أو النَشط، أو المجرم العادي أو مُدَبرْ المقالب (المزوح) إلى اقتراف مثل هذا العمل.

إن الهجوم من النوع المتصل بالحاسوب لا يمكن استخدامه لبيان دوافع أو أهداف المهاجمين بأي قدر من اليقين. وهذه هي إحدى الصعاب في النضال ضد الجريمة المتصلة بالحاسوب، حيث إن الحاجة تدعو إلى الحصول على المزيد من المعلومات لتحديد القصد الإجرامي.

وسواء كان الإرهاب السيبراني يتم عن طريق عملية زعزعة للأوضاع الاقتصادية، أو تهديد البنى التحتية الحرجة، أو لنشر إيديولوجية أو للتلاعب بالمعلومات، فإنه ينطوي على تهديد جديد يجب أن يؤخذ بمنتهى الجدية. ذلك أنه فضلاً عن تهديده للأنظمة المعلوماتية والعالم السيبراني الذي ترمز إليه الإنترنت، فإنه يمكن أن يعرض للخطر حياة الإنسان بخلقه تهديداً غير مباشر لحياة الناس وسلامتهم.

7.1.II المتسللون

إن فهم دوافع المتسلل ومستوى مهارته التقنية يمكن أن يساعد على تقييم مدى خطورة هجوم ما، كما يساعد على وضع استراتيجية مضادة. ولتأمين نظام معلومات، يحتاج المرء لأن يعرف من مَنْ يحتاج إلى حماية. وهناك في الوقت الحاضر مجموعتان رئيسيتان من المتسللين: المهنيون الذين يتكسبون من عملهم، والهواة الذين يميلون لأن يكونوا أشخاصاً يحتاجون بوضوح إلى الاعتراف بهم. (الشكل 4.II).

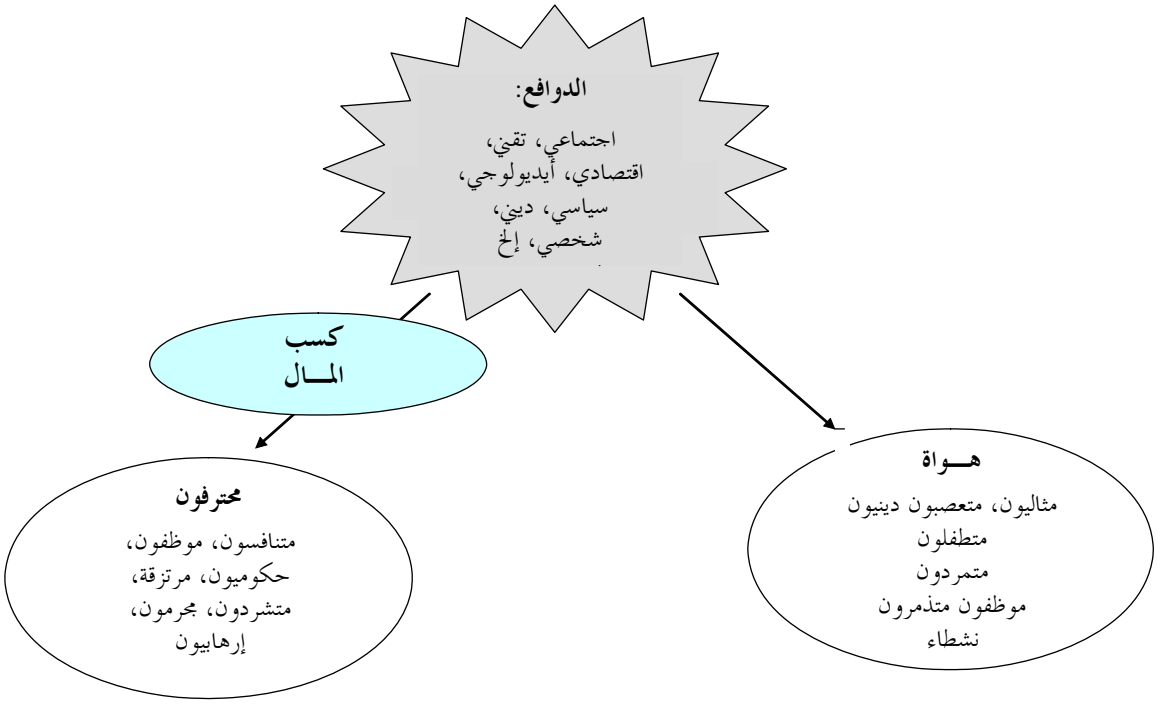
وينتمي المتسللون المحترفون إلى واحدة أو أكثر من هذه الفئات:

- المتنافسون المباشرون على المنظمة المستهدفة؛
- الموظفون المدنيون؛
- المرتزقة (المتسللون الذين يعملون لحساب منظمة في القطاع الخاص أو العام)؛
- عناصر إجرامية أخرى.

وقد يوجد بين المتسللين الهواة:

- فنيون، ينحدرون من المتسللين الأصليين، مولعون باستعراض مهاراتهم الحاسوبية والذين تحركهم أساساً رغبتهم في استعراض تمكنهم من التكنولوجيات المعنية؛
- المتطفلون؛
- المولعون بعمل المقالب – ويسمون كذلك بـــ "script-kiddies" أو "kidiots"، والذين يستمتعون غالباً بقدر كبير من الدعاية عندما يتم الإمساك بهم، فعلى الرغم من حقيقة أنهم يميلون لأن يكونوا غالباً غير مُقَنَعين، فلا يجب أن يقودنا هذا لأن نتصور أنهم الممثلون الوحيدون لفئة المتسللين؛
- الأشخاص المتهيجون نفسياً؛
- النشطاء الذين يعملون لأجل قضية إيديولوجية أو دينية (وغالباً ما يكونون أكثر احترافاً من الهواة).

الشكل 4.II – المجموعتان الرئيسيتان من المتسللين



وقد يكون الدافع الخفي لدى هؤلاء الأفراد متصلاً بعوامل اجتماعية وتقنية وسياسية ومالية أو متصلاً بالحكومة.

وعادة، ما تتمثل العوامل الاجتماعية في الحاجة إلى اعتراف القرناء، وتكون مرتبطة غالباً بعضوية عصابة أو جماعة. وهؤلاء المتسللون (hackers) يريدون أن يدللوا على أهميتهم داخل المجموعة وذلك عن طريق الارتفاع إلى مستوى القيم التي تحكم تلك الجماعة. وهذه الأفعال مماثلة للذين يلصقون البطاقات البذيئة في المدن، وهي تتأسس على نظرة مبسطة للشكل الهرمي الاجتماعي. وهذا غالباً هو الحال بين مُدَبري المقالب المزْحية الذين ينخرطون في التسلل (hacking) لأنه يعطيهم إحساساً بالعلو والهيمنة على المؤسسات التي يرون أنها تهيمن على الحياة العادية.

ونادراً ما يكون الدافع تقنياً وهدفه الأساسي الاستكشاف لحدود التكنولوجيا، ويدلل على تلك الحدود ونقاط التعرض هذه وفهم نقاط القوة.

يركز الدافع السياسي على الوقائع التي تجتذب اهتمام وسائل الإعلام بحيث تلفت الانتباه إلى مشكلة خطيرة وذلك من أجل بناء الوعي الجماهيري الذي يؤدي إلى حلها. وقد يكون الخط الفاصل بين هذا وبين الإرهاب مجرد شعرة، على الأقل من الناحية النظرية. ومن الشائع أن يستتر الشخص ذو دوافع اجتماعية وراء هدف سياسي.

يمكن للدوافع المالية أن تكون عاملاً مهماً وأن تكمن وراء عدد كبير من الإجراءات غير القانونية. وذلك أن بريق المال السهل يستهوي المجرمين ذوي الياقات البيضاء (المحتالون، والمختلسون، والمتنافسون الإجراميون، إلخ) على تسخير الإنترنت لمصالحهم.

وفي النهاية فإن المجموعة الأخيرة على قائمتنا تشمل الحكومات. ذلك أن هذا النوع من التسلل (hacking) يشمل الحرب المعلوماتية والتجسس وتقوم بهما دوائر حكومية تابعة للدولة.

وسرعان ما تأقلم الأشرار مع عصر الحاسوب، فأضافوا التسلل إلى أدوات حرفتهم، وهم يضيفون سعة الحيلة المخيفة لتسعفهم بوسائل جديدة لإساءة استعمال هذه التكنولوجيا.

8.1.II المزعجات والبرمجيات الخبيثة

1.8.1.II الرسائل الاقتحامية "Spam"

الرسائل الاقتحامية هي الإرسال بكميات كبيرة لبريد إلكتروني غير مطلوب وذلك لأغراض تجارية أو دعائية، والهدف منه هو إغراء مستخدمي الشبكة على طلب منتج أو خدمة.

وما فتئت الرسائل الاقتحامية تُشكل منغصاً قوياً على الرغم من الموارد التقنية والمالية الضخمة التي ينفقها مقدمو هذه الخدمة في البحث عن طريقة لوقفها، وعلى الرغم من النية المعلنة من جانب السلطات العامة لمكافحتها، وعلى الرغم أيضاً من تجريم مرسلي هذه الرسائل الوقحين في الماضي ففي سبتمبر 2003 استأثرت هذه الرسائل بنسبة 54 في المائة من مجموع حركة الرسائل الإلكترونية. وفي عام 2005، تجاوز عددها الرسائل الاقتحامية التي تم تداولها في الولايات المتحدة الأمريكية 12 مليار رسالة، أي 38,7 في المائة من مجموع الحركة وذلك طبقاً لما أفادت به هيئة كشف الاقتحام (IDC).

وتتشابه الرسائل الاقتحامية على أسوأ الافتراضات، مع هجوم قصفي بالبريد الإلكتروني، حيث تنوء مخدمات البريد بأحمالها، وتمتلئ صناديق بريد المستعملين وبما يرافق ذلك من مضايقات. وقد يقع مستعملو الحاسوب ضحية من خلال ممارسة تسمى بـــ"ربط القوائم" "list linking" حيث تضاف عناوينهم إلى قوائم مُشَغِلي الرسائل الاقتحامية بدون موافقتهم. ثم أن البديل الوحيد لمحاولة التملص من قوائمهم هو تغيير عنوان البريد الإلكتروني الذي يمكن أن يكون عملية شاقة. وعلى الرغم من أن هذا الإجراء فعال، فإنه مخِلْ أيضاً بدرجة كبيرة حيث إنه يحتاج من المستعمل أن يخطر جميع المراسلين المحتملين بهذا التغيير.

إن العدد الكبير من الرسائل غير المرغوب فيها وغير المحتشمة والتي تسبب الصدمة في بعض الأحيان يمكن اعتبارها اقتحاماً لخلوة المستعمل، مثل البريد الخردة (junk mail). يضاف إلى ذلك أن البريد الاقتحامي يتزايد استخدامه كمطية للبرامج الخبيثة (malware)، زيادة أُسِيةَ في مضارها.

2.8.1.II البرامج الخبيثة (Malware)

إن المتابعين الرئيسيين لأمن تكنولوجيا المعلومات (بما في ذلك فرقة الاستجابة لطوارئ الحاسوب (CERT)[12] ومكتب التحقيقات الفيدرالية في الولايات المتحدة الأمريكية (FBI) وكلوسيف (*clusif*) الفرنسية) قد لاحظت في تقاريرها السنوية بشأن الجريمة السيبرانية أن عدد البرامج الخبيثة والمزعجة التي تجري على الحواسيب بدون علم أصحابها آخذ في التزايد.

ويشمل ذلك الأنواع التالية من البرمجيات:

- آليات الإنزال، التي تستخدم في إنزال وتركيب البيانات والبرامج عن بعد؛
- keyloggers التي تتابع ضغطات المفاتيح التي يدخلها المستعمل في الحاسوب، وهناك أيضاً keyloggers لعتاد الحاسوب، غير مرئية على مستوى البرمجيات تسجل مثل هذه البيانات؛
- الزمبيات أو "البوتس" (وهي اختصار للروبوت) وهي برامج تشمل بالتحكم عن بعد في النظام بغرض بناء جيش مستتر من الحواسيب. ويكتشف كل يوم ما بين 25 إلى 50 بوتاً جديداً وهي تستخدم لأغراض إرسال الرسائل الاقتحامية، وفي هجمات "الفيشينغ" لاصطياد المعلومات الحيوية إلكترونياً احتيالياً (phishing) أو توزيع المواد الإعلانية. ففي أكتوبر 2005، ألقت الشرطة الهولندية القبض على ثلاثة رجال بتهمة الشك في تشغيل شبكة قوامها 100 000 حاسوب روبوتي لشن هجمات رفض خدمة، ولاستهداف حسابات باي بال PayPal وإي باي (eBay) الخاصة بضحاياهم.[13]
- البرمجيات الإعلانية، المستخدمة لتفصيل العمليات التجارية حسب الطلب؛
- البرامج التجسسية والتي كما يستشف من اسمها تسجل المعلومات بسرية. ويقول ويبروت ناشر البرمجيات إن هناك أكثر من 100 000 نوع من برامج التجسس على الإنترنت، وأكثر من 300 000 موقع تستضيفهم. إن أي كمبيوتر محمول PC عادي وله وصلة بالإنترنت عليه 28 برنامج تجسس في المتوسط مركبة فيه غير معروفة للمستعمل. كما أن أكثر من 80 بالمائة من حواسيب الشركات عليها برنامج تجسس أو أكثر، وهذه البرامج تشارك في 70 في المائة من جميع الهجمات.

وبالإضافة إلى أشكال البرامج الخبيثة هذه، توجد الفيروسات والمنتجات ذات الصلة (الديدان، وأحصنة طروادة، والقنابل المنطقية).

ويتكون الفيروس من شفرة خبيثة مركبة في نظام ما بدون معرفة المستخدم ولها القدرة على استنساخ نفسها تكرارياً (وفي حالة الفيروسات متعددة الأشكال، لا يكون الاستنساخ التكراري دقيقاً وإنما تحولاً إلى حد ما) وهو يهاجم البيئة المضيفة ويلوث كل ما يتلامس معه. ويمكن تمييز الفيروسات على أساس توقيعها وسلوكها وطريقة تكررها وانتشارها وأنواع الأعطال التي تحدثها، إلخ.

إن الغرض الذي يتوخاه فيروس الحاسوب، كنظيره الإحيائي، التكاثر والتزايد ذاتياً. وهو يفعل ذلك بالانتقال من حاسوب إلى حاسوب، ويلصق نسخاً من ذاته بالبرامج، وبالبريد الإلكتروني في الغالب الأعم. ويحدث ذلك عادة نتيجة لعمل ما يقوم به المستخدم. وقد تتفاوت الأضرار التي يحدثها فيروس بسلامة موارد المعلومات التي تلوثت به من المضايقات الحقيقة إلى التدمير الرئيسي، مع إحداث تأثير على توافر الأنظمة وسريتها.

---

12 www.cert.org-See statistical information for 1998-2005, at www.cert.org/stats/cert_stats.html

13 المصدر: نقرير كلوسيف (Clusif)، *panorama de la cybercriminalite, 2005* www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf

إن مصطلح "فيروس" التنوعي يستخدم لتسمية أي برنامج حاسوبي ضار (فيُحِدثْ العدوى، والتدمير، وإساءة تخصيص الموارد، إلخ) ويكون قادراً على التكاثر وإكثار نفسه.

وفي عام 2005، كان هناك ما يقدر بـــ50 000 فيروس جديد متداولاً[14] فمثلاً، أصاب الفيروس HTML_NETSKY.P، على نحو ما وصفه المركز العالمي لمتابعة الفيروسات 244 855 جهازاً حول العالم منذ أبريل 2004. وكانت التكلفة، بالنسبة للشركات التي وصلتها العدوى حوالي 42 مليوناً بدولارات الولايات المتحدة الأمريكية وذلك طبقاً لإفادة معهد أمن الحاسوب Computer Security Institute. وطبقاً لتقديرات الموقع F-secure.com فإن عدد الفيروسات المتداولة كل يوم يصل إلى أربعة آلاف.

أما الديدان فهي بايتات من شفرة حاسوبية تسافر هي الأخرى عبر النت، غالباً دون مساعدة خارجية، وبدون أي إجراء من جانب المستعمل. وهي، مصممة عادة، لربط مصادر النظام (الذاكرة وعرض النطاق) وبذلك تضر بتوافر خدمات النظام أو تساعد على التحكم في النظام المصاب بالعدوى عن بعد.

أما البرامج الخبيثة المعروفة باسم أحصنة طروادة فتكون مخبأة غالباً داخل البرامج العادية أو الملفات المساعدة ثم تتسلل إلى الأنظمة. حيث تحاول السيطرة لكي تسرق وقت الُمعَالج، أو تتلاعب بالبيانات أو البرامج أو تدمرها، وتتسبب في الانهيارات، وتقوم بالتطفل وأشكال النشاطات الخبيثة الأخرى،أو أنها ترقد – ليـــس إلا – ريثما تتاح الفرصة للهجوم مستقبلاً.

والقنابل المنطقية هي فيروسات تنشط في حادثة معينة (مثل أعياد الميلاد) لمهاجمة النظام العائل لها.

ولا ينبغي لأي من هذه الفيروسات أن تُخلَطْ "ببق" الحاسوب التي هي أخطاء برمجية، أو بصورة أكثر عمومية ثغرات في التصميم تبرز كمشاكل وظيفية.

والطريقة العادية لتكاثر الفيروسات ودخولها حيز التفعيل هي أن تنتظر التنشيط الغافل من جانب المستخدم، كبدء برنامج مصاب بالعدوى مثلاً. وكانت معظم الفيروسات تتكاثر في الماضي عبر مرفقات البريد الإلكتروني، وكانت تنشط عامة بمجرد الضغط على أيقونة "ICON" استدعاء الملف.

يتخفى الكثير من البرامج الخبيثة في صورة إضافات مُساعدة على الملاحة، وعلى الربط، وتفصيل الخدمات حسب الطلب إلخ، بينما هي في الواقع مصممة للقيام بالمراقبَة (سرقة المعلومات، سرقة كلمات المرور، ومراقبة الحركة الإلكترونية) واستخدام الموارد أو شن الهجمات. وهي تستخدم كذلك لنشر الأدوات المستخدمة في توزيع هجمات منع الخدمة والتحكم فيها. ويجري الآن تداول الآلاف من هذه البرامج والغرض منها هو الكسب المالي.

إن رفض تقديم الخدمة (DOS) وهجمات رفض تقديم الخدمة على نطاق واسع إنما ترمي إلى تعجيز موارد النظام. وهي تعمل في العادة على زيادة تحميل مُخَدم بطلبات الخدمات العادية المصمم لتأديتها عادة، مما يمنعه من تقديم الخدمة للمستخدمين العاديين (ومن هنا يأتي مصطلح رفض تقديم الخدمة). لأن هذه الطلبات تشبه الطلبات العادية بحيث يكون من الصعب للغاية الوقوف في وجه هذا الهجوم (إن حجم الطلبات في حد ذاته هو الذي يُغْرق النظام). ولزيادة فعالية هذه الهجمات يمكن شنها في آن واحد من نقاط أو أنظمة مختلفة، وهذا ما يشكل هجوم رفض تقديم الخدمات واسع النطاق distributed DOS attack.

أما سبل إكثار البرامج الخبيثة مختلفة الأنواع فتشمل البرمجيات المجانية أو برمجيات البيان العملي والمواقع أو الألعاب الجنسية الإباحية، والبريد الإلكتروني كما تشمل أيضاً الرسائل الاقتحامية ومجموعات المناقشة.

[14] المصدر IPA/ISEC تقرير حوادث فيروسات الحواسيب.

ومهما تكن الوسائل المستخدمة للتسلل داخل البرمجيات الخبيثة – فقد تشتمل حتى، على سبيل المثال في حالة البرامج الإعلانية (وليست التجسسية)، خطوة نحو الموافقة المعلنة أو المضمرة من جانب المستخدم – ذلك أنه بمجرد تركيبها فإنها تتحول إلى الاستخدام غير المشروع. وفي الغالب الأعم تنفذ هذه الأعمال بدون موافقة المستعمل. وهي تقوم بصورة سرية بجمع البيانات وإرسالها (مثلاً عن عادات رياضة ركوب زلاقة الماء، المستهدفة من الإعلان). وهي تؤدي أعمالاً كسولة للأنشطة غير القانونية مثل هجمات بالرسائل الاقتحامية واصطياد البيانات تحايلياً "فيشينغ"، وتعمل بفعالية لتحقيق الكسب المالي للتحكم في هذه العملية. إن اكتشاف مثل هذه البرمجيات وعدم تركيبها في الحاسوب ليست بالعملية الصريحة على الدوام. ففي غالب الأحيان، يفتقر المستخدمون إلى المهارات والأدوات اللازمة للتحكم في هذه المخاطر.

أما مصطلح "فيشينغ" (اصطياد استدراجي) – فهو مجاز للصيد بالسنارة، حيث يستدرج الصياد السمكة إليه بعد اجتذابها بالطعم – وهو يشير إلى هجوم يستخدم البرامج البريدية لمخادعة أو لإقناع مستخدمي الويب بإفشاء معلومات حساسة يمكن عندئذ استغلالها في أغراض إجرامية (مثل التحايل أو الاختلاس). وقد سجلت جريدة جورنال دي نت[15] الصادرة في 26 يناير 2005 أكثر من خمسة آلاف موقع "اصطياد" عاملة على الشبكة خلال شهر واحد (سبتمبر 2005) وموجهة إلى 110 أصناف مختلفة.

وتجري هجمات الاصطياد بصورة عامة باستخدام رسائل البريد الإلكتروني المزورة بحيث تبدو وكأنها صادرة عن مؤسسة حقيقية قد يكون للمستخدم تعاملات معها. (مثل مكتب البريد، أو مصرف، أو تاجر، أو موقع مزاد على الشبكة)، ولكن المهاجمين قد يستخدمون أيضاً المكالمات التلفونية، والرسائل السريعة أو الرسائل النصية على الهواتف الخلوية، أو حتى يفاتحون الضحية شخصياً.

3.8.1.II الاتجاهات

لم تعد الفيروسات اليوم تستهدف بصورة رئيسية تدمير البيانات واسع النطاق دون مبرر. بل يبدو أنها مصممة لإنجاز غرض أكثر ذكاءً بكثير هو كسب المال. وبفضل هذا الاتجاه البرمجاتي الجديد وبفضل خصائصها الذاتية، يمكن استخدامها في الغش التحيالي. وهكذا غدت الفيروسات أدوات مربحة بالنسبة للمجرمين المشتغلين بالجرائم المالية.

وبالنسبة للرسائل الاقتحامية والمنغصات ذات الصلة، أفاد النادي الفرنسي لأمن الأنظمة المعلوماتية (Clusif)[16] بأن الموقع الشبكي الرسمي AOL قد قام بتصفية 500 مليار رسالة اقتحامية في عام 2003، وأن أغزر جهة في العالم توجه الرسائل الاقتحامية، على نحو ما صرح به سبامهاوس[17] لمكافحة الرسائل الاقتحامية في ديسمبر 2003، يعتقد أنها أرسلت بـــ70 مليون رسالة بريد إلكتروني في يوم واحد!

وذكر نادي كلوسيف الفرنسي أيضاً أن ما تدعى بـــ"بافالوسبامر" حُكم عليها في مايو 2003، في الولايات المتحدة الأمريكية بتسديد مبلغ 16,4 مليون دولار بدولارات الولايات المتحدة الأمريكية إلى إيرثلينك التي تقدم خدمة الإنترنت مقابل إرسال 820 مليون رسالة غير مرغوب فيها. وصرحت "فيريس ريسيرش (Ferris Research) بأن الرسائل الاقتحامية كلفت دوائر الأعمال في العام سنة 2003، 2,5 مليار دولار أمريكي، في أوروبا و8,9 مليار دولار أمريكي في الولايات المتحدة الأمريكية. فإذا أضيفت هذه المبالغ إلى الـــ500 مليون دولار بدولارات الولايات المتحدة التي دفعها مقدمو الخدمات لسد الطريق أمام "الرسائل الاقتحامية" لاتضحت ضخامة هذه المشكلة المتمثلة في إساءة استخدام البريد الإلكتروني. ومن الواضح أننا بصدد قضية لم يعد بالإمكان تجاهلها.

15 www.journaldu net.com
16 www.clusif.asso.fr
17 www.spamhaus.org

وبالإضافة إلى التكاليف المباشرة الناتجة عن الاحتيال، يتعين على المرء أن ينظر في التكاليف ذات الصلة بانقطاع الخدمة المؤقت service interruption الذي يؤدي إلى اختلال العمليات، وفقدان المبيعات والأضرار الملازمة، وفقدان الصورة والسمعة، وتكلفة استعادة الأنظمة إلى الحالة التشغيلية. وهذه تُمثل تكلفة كبيرة للمنظمات التي هي أهداف لجرائم الحاسوب.

وتبين عمليات الرصد أن عدد الهجمات آخذ في التزايد دوماً وأن فيروسات الحاسوب قد غدت أوبئة حقيقية. فعمليات انتحال – الهوية آخذة في التزايد، وقد اكتسبت مستوى من التركيب والتعقيد يثير الخشية، مثلما حدث للتحايل ولمختلف أنواع الخداع والابتزاز التهديدي التي أصبحت حقيقة يومية في الفضاء السيبراني. فقد شاعت في كل مكان، وأضرت بكل فرد وبكل قطاعات النشاط عبر حدود الجغرافيا والزمن.

ولا يوجد أي نظام، سواء كان عتاداً حاسوبياً أو نظاماً أساسياً للبرمجيات يتمتع بالمناعة، بما في ذلك الأنظمة النقالة (الحواسيب الحضنية أو الهواتف النقالة).

9.1.II الأشكال الرئيسية لجريمة الإنترنت

1.9.1.II عمليات المخادعة، وأنشطة التجسس والتخابر، وخطط الابتزاز والابتزاز بالتهديد أو الإيذاء

إن الأشكال الشائعة المختلفة للجريمة المنظمة (خطط الابتزاز الحمائية، الاتجار بالبشر، خطط النصب والاحتيال والسرقة، إلخ) يمكنها أن تستفيد من استخدام تكنولوجيا المعلومات الجديدة، وبخاصة الشبكة. ذلك أنه عن طريق تيسير الشبكة لعمليات الاتصال فإنها تساعد المشتغلين بأي نوع من التهريب (سواء كانت المهربات أسلحة أو بشر)، وعمليات النصب (وهي هجمات على الملكية، وأنظمة الحاسوب والبنية التحتية، وسرقة البيانات، ومخالفات حقوق النشر والتأليف، إلخ).

ويستخدم المجرمون الإنترنت بطرق عدة. فبعضهم ينتحل هوية شخص آخر لكي يقوم بالشراء على حساب الضحية. ويتم هذا غالباً بواسطة الاحتيال بكارت الائتمان وذلك عن طريق خلق أرقام بطاقات سارية المفعول لا تناظر أي حساب حقيقي. وتستخدم هذه المعلومات لشراء شيء على الشبكة باستخدام عنوان يمكن التخلص منه بعد التسلم ولمرة واحدة. أما الجهة التي تتحمل التكلفة فهي النظام المصرفي أو التاجر. ويمكن لمستخدمي البطاقات الائتمانية هذه أن يقعوا ضحايا، مثلاً، إذا أبلغت أرقام بطاقاتهم الائتمانية من جانب نشال أو تاجر غير شريف إلى عصابة متخصصة.

وهناك فئة أخرى من عمليات النصب تشتمل على بيع خدمات خيالية مثل الدبلومات الجامعية، وجوازات السفر الدبلوماسية لبلدان غير موجودة، ومزادات لمنتجات غير موجودة، إلخ)

وتسهل شبكة "الويب" كذلك التجسس والتخابر حيث تُيسر الاعتراض غير المشروع للمعلومات التي يتم تناقلها على الإنترنت.

وينبغي الإشارة كذلك إلى الاستخدام النظامي لوسائل الاتصال المُؤمنة مثل التجفير على أيدي إرهابيين محترفين، حيث تساعدهم على العمل بمزيد من الأمن، عن طريق تقليل حجم المعلومات المعرضة للاعتراض من جانب سلطات إنفاذ القوانين.

والإنترنت وسط قوى يساعد على نشر طرق ارتكاب الجرائم والأفعال المنافية للقانون، وتشجيع من يفكرون في الإجرام على أن يصبحوا مجرمين.

2.9.1.II الجرائم ضد الأشخاص

تخلق الإنترنت إمكانيات نشوء مجموعات سرية خائلية حول الممارسات التي يفرض عليها القانون عقاباً. وقد يشمل ذلك المواد الداعرة، ولواط الأطفال أو ما يسمى بأفلام سَنَفْ snuff movies (وهي أفلام تعرض مشاهد للعنف

والتعذيب لضحايا حقيقيين تسفر في بعض الأحيان عن موتهم). وعادة ما يكون هذا النوع من الجريمة مرتبطاً بالاتجار في البشر، والذي يضم في معظم الأحيان النساء والأطفال. ويمكن تقاسم الأفلام والصور مع وجود قدر ضئيل جداً من رقابة الشرطة. وحيث أن المخدمات (servers) توجد غالباً في بلدان غاب عنها إنفاذ القانون أو تراخي فصار قليل الفعالية، ومع استخدام خدمات "حديث مرحل الإنترنت" (ICR) لفترات زمنية محدودة للغاية، والاتصالات التبادلية بين الأقران (P2P) exchanges فإن هذا الأمر يزيد من الأعمال الإجرامية.

وتقع جميع هذه الأنشطة غير القانونية تحت طائلة القانون العادي (المبني على العرف والعادة). ويمكن أن يثور سؤال حول ما إذا كانت ممارستها الصناعية واسعة النطاق التي غدت ممكنة بفضل وجود الإنترنت وبفضل حرية انتقال السلع والأشخاص قد حولتها إلى جرائم ضد جزء من الإنسانية.

ومن بين الجرائم ضد الأشخاص، تشمل الأمثلة الأخرى مخالفات تمس السرية، وصورة الشخص، والسرية المهنية، وحقوق سرية البيانات. أما الجرائم التي ترتكب تحديداً ضد القُصَّرْ فتشمل نشر الرسائل الداعرة التي يمكن أن يراها القُصَّرْ.

3.9.1.II القرصنة

إن السهولة التي يمكن استنساخ المعلومات الرقمية بها قد خلقت سوقاً للنسخ غير القانوني. ويستأثر هذا النسخ بعشرات كثيرة من بلايين الدولارات الأمريكية كخسائر يتحملها ناشرو البرمجيات والموسيقى وأفلام الفيديو.

وقد لوحظ أيضاً وجود زيادة كبيرة في عدد الأعمال العلمية والأكاديمية التي تلجأ إلى سرقة الأفكار فقط بمجرد نسخ وثائق موجودة من الويب.

وهناك عدد كبير من مخالفات الملكية الفكرية المحتملة: كتزييف أعمال مؤلف ما (بما في ذلك البرمجيات) والتصميم، والنموذج والعلامة التجارية، إلخ.

4.9.1.II التلاعب في المعلومات

يمكن للتلاعب أن يتخذ أشكالاً كثيرة، كتسريب وثائق داخلية مثلاً لأجل زعزعة استقرار شركة، وإرسال طلبات بالرسائل الإلكترونية للحصول على تبرعات خيرية عبر مواقع زائفة، إلخ.

والإنترنت تربة خصبة لنشر الشائعات والمعلومات المضللة. وهي تيسر كذلك ارتكاب المخالفات ضد قانون وسائل الإعلام، والتحريض الجنائي، والدفاع عن الجرائم ضد الإنسانية، ومناصرة الإرهاب والتحريض عليه، والتحريض على العداء العرقي، والتحريفية التاريخية (المذهب الرفضي) واغتيال الشخصية، والإهانات وما إلى ذلك.

والشكل 5.II يعطي أمثلة على أنواع الجرائم التي تيسر الإنترنت ارتكابها.

الشكل 5.II – أمثلة على أنواع الجرائم التي تيسر الإنترنت ارتكابها

الجرائم ضد الأشخاص – الضرر الشخصي – السرية – الصورة الشخصية – القذف – السرية – السرية المهنية – السرية الرقمية – القُصَّر
الجرائم ضد الممتلكات – عمليات النصب – الهجمات على أنظمة المعلومات – خروقات قانون الوسائط
التحريض على ارتكاب الجرائم – الدفاع عن الجرائم ضد الإنسانية – الدفاع عن الإرهاب والتحريض عليه – التحريض على العداء العرقي – إنكار الهلوكوست – القذف
المخالفات لقانون الملكية الفكرية – تقليد عمل مؤلف (بما في ذلك البرمجيات) – نسخ مزورة من تصميم أو نموذج – تزوير العلامات التجارية – المقامرة غير القانونية على الشبكة

5.9.1.II دور المؤسسات العامة

إن السلطات العامة مطالبة أكثر من أي وقت مضى بتبوء دورها التقليدي المتمثل في ملاحقة التحايل والجريمة قضائياً ومنعهما. وعليها كذلك أن تصبح نشطة في تثقيف الجمهور العام وتعميق وعيه. ومن المفيد، بوجه خاص، أن تكون هناك معلومات مرجعية بشأن حماية الأشخاص والملكية الفكرية متاحة وقت استخدام الإنترنت.

ومن الخطر السماح لسلطات إنفاذ القانون بأن تتخلف تكنولوجياً. إن تكلفة محاولة اللحاق بعد مرور عدة سنوات من الوقت الضائع تتجاوز أبعاده التكلفة المالية المباشرة في شكل حيازة بنية أساسية جديدة، إذْ إن هناك فوق ذلك كله تكلفة مرتبطة بتزايد تأثير هيئات الجريمة المنظمة على المجتمع بما يكتنف ذلك من مخاطر زعزعة الاستقرار.

إن الوجود المفرط للشرطة على الإنترنت ليس – في نفس الوقت – أمراً مرغوباً فيه بالضرورة، وربما تضارب مع الحاجة إلى حماية سرية المبادلات واحترام خصوصية الفرد.

10.1.II حوادث الأمن والجريمة السيبرانية غير المبلغ عنها

ينبغي الإشارة إلى توافر عدد ضئيل فقط من البيانات الإحصائية عن الجريمة السيبرانية. فهي نوع جديد من العمل الإجرامي. ولا يتم إبلاغ الشرطة بمعظم الحوادث. في وقوع المخالفات عبر الحدود كذلك، ومع كون التشريعات الجنائية وطنية، يكون من الصعب تجميع بيانات إحصائية عن جرائم يتم تعريفها بطرق تختلف باختلاف البلدان؛ فمثلاً، في حالة نظام حاسوبي استخدم في ارتكاب عملية تحايل مالي باستخدام هوية مستخدم منتحلة، يمكن تصنيفها إما كجريمة ذات صلة بالحاسوب أو كجريمة مالية.

ومع ذلك، فإن إنشاء فرق لا مركزية في الولايات المتحدة الأمريكية مثلاً للتحقيقات بشأن الحاسوب وتقييم التهديدات الموجهة إلى البنية التحتية (CITA) التي ينسق عملها المركز الوطني لحماية البنية التحتية (NIPC) يعطي إشارة إلى فداحة الجريمة السيبرانية.

إن عدد حوادث الأمن التي أبلغت إلى مركز التنسيق CERT[18] آخذ في الإطراد منذ بداية هذا القرن، مثلما يطرد عدد من الهجمات التي تُبلغ إلى السلطات القانونية، الأمر الذي يسهم في فهم أفضل، ويفسر جرائم الحاسوب. ففي عام

[18] مركز تنسيق CERT، جامعة كارينجي ميللون (http://www.cert.org)

2003، حدثت زيادة كبيرة في حجم الرسائل الاقتحامية الذي تجاوز انتشاره حدود الإنترنت فوصل إلى الرسائل النصية للهواتف الخلوية، وأُلقي القبض على العديد من مرسلي الرسائل الاقتحامية وإدانتهم. وتبين عمليات الشرطة واسعة النطاق التي تمت في الولايات المتحدة الأمريكية (عمليتا E-Con في مايو 2003 Cyber-Sweep في أكتوبر 2003) وفي أوروبا (إسبانيا، وإيطاليا وفرنسا والمملكة المتحدة، وغيرها) أن السلطات كانت تتعامل مع نسق إجرامي جديد وتتأقلم عليه. إن إلقاء القبض على العديد من مُخَلِّقي الفيروسات ومرسلي الرسائل الاقتحامية وتجريمهم إنما يشهد على عقد العزم على التعامل مع هذه الأنواع الجديدة من المضايقات. إلا أن عدد الإدانات لا يزال منخفضاً للغاية بالنظر إلى حجم الرسائل الاقتحامية والفيروسات المتداولة على أساس يومي.[19]

ومن الصعب تقدير معدل الجريمة السيبرانية غير المبلغ عنها. ومن المحتمل أن تكون السلطات القانونية، والشرطة والجمهور العام لا يدركون إلا ما لا يزيد على 12% من الجريمة السيبرانية[20] ومن الصعب الحصول على قائمة جرد واقعية للجريمة المتصلة بالحاسوب، وهذه عقبة خطيرة في وجه محاولات تحليل هذه الظاهرة وتحديد نطاقها.

ويرجع غياب الإحصاءات الرسمية إلى أسباب من بينها أن المنظمات:

- ترغب في تفادي الإعلان عن الهجمات؛
- قد لا تكون مدركة لأنها وقعت ضحية لجريمة سيبرانية، وبخاصة في حالات الهجمات السلبية (الاختطاف الشفاف للبيانات، والمرور، والتسمع السلبي، والاقتحام غير المكتشف، وإلى غير ذلك) كما أنها قد لا تعلم بوقوع الهجوم إلا بعد مرور وقت طويل حيث لا تكون هناك فائدة من إبداء رد فعل؛
- لا تعرف كيف تتعامل مع الوضع الخاص بالأزمة؛
- تفتقر إلى الثقة الضرورية بالسلطات القانونية وبالشرطة، وقدرتها على التعامل مع هذا النوع من المشاكل؛
- تفضل أن تتعامل مع المسألة بأنفسها.

تتحسن مهارات المتسللين، ويزداد تعقيد الهجمات وقوتها وكذلك الأدوات التي يستخدمها المهاجمون طوال الوقت، كما أن الحجم الفعلي للهجمات يواصل التزايد هو الآخر. إن التعقيد المتزايد دوماً الناتج عن هذا الاتجاه الدينامي صعب المراس. ذلك أنه في غياب الإدارة السياسية القوية والإحساس بالمسؤولية فيما بين جميع المشاركين على المستوى الدولي، وعدم قيام شراكة فعالة بين القطاعين الخاص والعام، لن تتجاوز أي تدابير أمنية سواء كانت ذات طبيعة تقنية أو تشريعية حدود النهج القاصر والقطاعي لتحقيق الأمن، ومن ثم تظل غير فعالة في التعامل مع الجريمة المتصلة بالحاسوب.

11.1.II التحضير لتهديدات الجريمة السيبرانية: مسؤولية للحماية

من الضروري أن يعد المرء نفسه لمواجهة تهديد الجريمة السيبرانية التي لا بد لها أن تحدث عاجلاً أو آجلاً.

وتحتاج حماية أصول المنظمة والدفاع عنها إلى تنظيم يراعي خطورة الجريمة، وذلك عند تعريف استراتيجية الأمن. وعلى الرغم من إمكانية صعوبة التعرف على هوية المجرمين السيبرانيين، حيث لا يُعرف الكثير عن الطرق التي يعملون بها أو عن بواعثهم. وقد لوحظ أن المنظمات الإجرامية تتصرف بصورة انتهازية بصفة عامة، بل وتميل إلى مهاجمة الأهداف الأكثر تعرضاً. ويمكن للمنظمات أن تتخذ الخطوات للتأكد من أنها ليست هدفاً مغرياً للجريمة السيبرانية وذلك عن طريق تأمين بنيتها التحتية الحاسوبية بصورة أفضل مما حولها. وذلك بدلاً من الرضى بأن تبقى على نفس المستوى من عدم الأمن مع منافسيها. وهكذا يصبح خطر الجريمة السيبرانية دافعاً لتأمين مستوى عالٍ من الأمن.

---

19 قام مركز أمن المعلومات التابع لوكالة تعزيز تكنولوجيا المعلومات (IPA/ISEC) في اليابان بتحديد عدد 059 85 من الفيروسات المعروفة في ديسمبر 2003، وذلك في تقريره الصادر باسم Computer Virus Incident Reports، 2004 : www.ipa.go.jp/security/english/virus/press/200401/virus200401-e.html

20 فلاديمير غوبوليف، "طوبولوجيا جريمة الحاسوب" نشر في 9 يناير من جانب مركز بحوث جرائم الحاسوب: www.crime-research.org/articles/Golubev123/

وعلى النقيض من ذلك فإن أي منظمة يعتبرها المجرمون فريسة سهلة مربحة، أو رمزاً يجب تدميره، سوف تجتذب الهجمات حتماً. ففي الحالة الثانية، يغدو التهديد بالتدمير بواسطة الأفعال الإرهابية احتمالاً حقيقياً. ويكون من الضروري في مثل هذه الحالات الاستعانة باستراتيجية حماية ودفاع مناسبة. إلا أن التأمين التقليدي وأدوات إدارة المخاطر ذات فعالية محدودة في التعامل مع الخطر الإجرامي حيث إن الطريقة الوحيدة لتفادي مخاطر معينة ستكون هي تفادي الدخول على الإنترنت.

والخطر الإجرامي ذو بعد عالمي، ويؤثر على المنظمات على جميع المستويات (أصحاب المصلحة، التنفيذيون، الموظفون، مرافق الإنتاج إلى غير ذلك). لذلك ينبغي لتلك المنظمات أن تتعلم كيف تحمي سلامتها التي يتهددها خطر الجريمة، مثلما تعلمت أن تتعامل مع الفساد مثلاً. ويجب عليها أن تظل رابحة، وأن تعوض عن تكلفة الفرصة البديلة التي نجمت عن خطر الجريمة السيبرانية، وتكلفة التدابير الموضوعة لإدارتها. ويجب تصميم نموذج لإيجاد أفضل الطرق لدعم تكلفة حماية البنية الأساسية، وتوفير الأمن للأنظمة، وللشبكات والبيانات والخدمات التي تمثل عبئاً على النمو الاقتصادي، وذلك بمساعدة من أولئك الذين لهم نصيب من الثروة التي تخلقها المنظمة.

إن إدراك هشاشة العالم الرقمي، واستحالة تحقيق سيطرة تامة ليس فقط على تكنولوجيا المعلومات وتكنولوجيات الاتصالات والبنية الأساسية، وإنما أيضاً على حلول الأمن التجاري، لا بد وأن يثير حتماً المسألة الجوهرية المتعلقة بالتكنولوجيات التي لا تخضع لسيطرتنا.

فإلى أي مدى نحن على استعداد للاعتماد على مُوردْ، أو بلد ما أو مدير ما؟

ويجب أن تكون الخطوة الأولى نحو ضمان مكافحة خطر الجريمة السيبرانية هي:

- مراجعة العلاقة مع التكنولوجيات الجديدة والموردين؛
- طلب ضمان أمني؛
- تحديد مسؤولية جميع المشاركين.

وقبل تنفيذ تدابير الأمن التقليدية التي تستند إلى نهج المنع – الوقاية – الدفاع، يجب علينا أن نسعى أولاً لحماية الموارد الحساسة والحرجة للمنظمة عن طريق مراجعة علاقتها بالتكنولوجيات الحديثة.

ويجب علينا أن نطلب:

- منتجات عالية الجودة تعطي مستوى أمن متجاوب مع الاحتياجات يمكن التحقق منه؛
- أن يكون الأمن شفافاً، وليس مستوراً، كما كان في الماضي؛
- أن يكون الأمن ليس فقط مسؤولية المستخدمين ولكن أيضاً أصحاب المصلحة (المسؤولية القانونية للمهنيين: مصممو البرمجيات ومقدمو خدمة النفاذْ. إلخ)؛
- أن يوضع حد أدنى من الأمن كجزء عضوي من حلول التكنولوجيات (المنتجات الآمنة)؛

فإذا ما نظرنا إلى ما وراء هواجس المنظمة، وفي مواجهة تنسيق النشاطات وتوحدها من جانب الجريمة المنظمة، والجريمة الاقتصادية والجريمة السيبرانية، لمسنا الحاجة إلى وجود استجابة لتعزيز ثقة الجهات الاقتصادية الفاعلة في تكنولوجيا المعلومات وتقليل فرص ارتكاب الجرائم.

ويجب أن يفي هذا الرد باحتياجات الأمن الوطني والمنظمات والأفراد. ويجب أن يبقى على الجريمة السيبرانية عند مستوى مقبول، وأن يعزز الثقة في العالم الرقمي ويُدَنِي من مخاطر الفساد والتهديد للسلطات العامة.

القسم 2.II – الهجمات السيبرانية

1.2.II أنواع الهجمات السيبرانية

هناك عدة طرق مختلفة لاستغلال الإمكانيات التي تتيحها تكنولوجيات الإنترنت. وهي تقوم في أغلب الأحيان على تخصيص معلمات أو كلمات مرور الاتصال للمستخدمين الشرعيين، وعلى الخداع واستغلال الصدوع ونقاط التعرض في التكنولوجيات.

2.2.II سرقة كلمات مرور المستخدمين للتسلل في الأنظمة

وفيما يلي الطرق الرئيسية التي تستخدم في الحصول على معلمات اتصال المستخدمين الشرعيين للنفاذ إلى الأنظمة.

- التخمين: كلمة المرور تكون واضحة جداً (اسم المستعمل، أو اسم زوجته أو طفله، تاريخ ميلاده، إلخ) بحيث يكون حسابه غير محمي أساساً؛
- الخداع (الهندسة الاجتماعية): حيث يظهر المهاجم بمظهر المسؤول ثم يطلب كلمة المرور تحت أي ذريعة تقنية. وفي عدد كبير من الحالات بصورة تدعو إلى الدهشة؛
- الاستماع إلى حركة المرور: حيث يعترض المهاجم أو يستمع إلى بيانات غير محفرة مرسلة إلى الشبكة عبر بروتوكولات الاتصال (التلصص، الترصد)؛
- البرمجيات: حيث يتم تسريب "حصان طروادة" إلى محطة عمل المستعمل، حيث يقوم سراً بتسجيل المَعْلَماتْ المستخدمة للارتباط بالأنظمة البعيدة؛
- النفاذ إلى ملف تخزين كلمة المرور؛
- السطو على كلمات المرور المرسلة بشكل مجفر؛
- التجسس على المستخدمين عن طريق تنشيط طرفياتهم متعددة الوسائط لتسجيل مَعْلَمات اتصالهم.

وبمجرد الحصول على مفتاح النفاذ الضروري لدخول الأنظمة (أي تركيبة اسم المستعمل وكلمة مروره) يصبح من السهل التسلل إلى الأنظمة وإجراء جميع أنواع عمليات القراءة والكتابة. والمهمة الصعبة التي تواجه المتسلل هو تفادي افتضاح أمره وعدم ترك أي أثر له داخل الأنظمة التي نفذ إليها.

3.2.II هجمات رفض أداء الخدمة

ينفذ هجوم رفض الخدمة عادة عن طريق تحميل النظام بما يفوق طاقته، ذلك أن الأنظمة المستهدفة التي يتم غمرها بطلبات تزيد كثيراً عما تسمح طاقتها بمعاملته تنهار وتصبح غير متوافرة الخدمة. ويمكن ارتكاب هذه الهجمات عن طريق استغلال تصدعات موجودة في النظام الجاري تشغيله، وباستغلال جوانب معينة في النظام مثل إدارة الدرائ buffer management (هجوم فيض الذاكرة) مما يتسبب في تعطل التشغيل الأمر الذي يمكن أن يؤدي إلى إقفال النظام.

القصف بالبريد الإلكتروني وهو يشتمل على غمر صندوق الرسائل الواردة لدى المستخدم بفيض من الرسائل بشكل من أشكال هجوم رفض أداء الخدمة.

4.2.II الهجمات الطَمسْية

ويُشن هجوم الطمس باستبدال صفحة الويب الخاصة بالضحية بصفحة أخرى بحيث تعتمد محتويات الصفحة الجديدة (داعرة أو سياسية مثلاً) ببواعث المتسلِلْ. وتنطوي إحدى تنويعات هذا النوع من الهجوم على إعادة توجيه المستعملين

نحو "موقع شبكي شَرَكْ" يبدو مطابقاً تماماً للموقع الذي كان يستخدمه المستخدمون من قبل، وحيث يطلب إليهم إفشاء معلومات بطاقات الائتمان الخاصة بهم، مثلاً. ويتم ذلك بهجمات اصطياد استدراجية على سبيل المثال.

ويمكن كذلك طَمسْ محتوي المواقع الشبكية لأغراض التضليل (للتأثير في الوقائع وبث عدم اليقين، والتلاعب بالرأي العام، إلخ) وهذه هجمات دلالية (سيمانطيقية) تقلب معنى المحتوى المعلوماتي وتقع ضمن فئة الحرب المعلوماتية.

5.2.II الهجمات الخداعية

يمكن إفساد جميع البروتوكولات (بروتوكول التحكم في الإرسال/بروتوكول الإنترنت ICP/IP) واستخدامها في خرق أمن النظام. فجميع البروتوكولات والآليات التي تنقل البيانات عبر الشبكة معرضة للمخاطر بدرجة متساوية. ومن ثم يكون في المستطاع اختطاف دورة بروتوكول التحكم في الإرسال (TCP session) أثناء دورة عمل العميل – المخدم.

ويؤدي بروتوكول التحكم في الإرسال (TCP) وظائفه عن طريق إنشاء وصلة منطقية بين متراسليْن، ومساندة تبادل بيانات التطبيق بين الاثنين. وللربط بين التطبيقات واسعة النطاق يستخدم هذا البروتوكول أرقام المنافذ، ومحددات الهوية المنطقية للاستخدامات. فبعضها يكون ثابتاً ومحتجزاً لبرامج بعينها، ومعروفاً جيداً للمستعملين، بينما يخصص غيرها أثناء حركة الربط، طبقاً لخوارزمية محددة. وينطوي أي هجوم على رقم منفذ بروتوكول التحكم على التخمين أو التنبؤ بأرقام المنافذ التالية التي تخصص لمبادلة البيانات لاستخدامها في مكان المستخدم القانوني، مختطفاً إياها فعلياً، الأمر الذي يمكن من المرور عبر حوائط النيران وإقامة وصلة "آمنة" بين الكيانات (المتسلل والهدف). وفي نفس الوقت، يكون نفاذ المستعمل القانوني البعيد للمرفق مسدوداً، ولكن بسيطاً بدرجة تمكنه من إرسال رسالة تقول إن النظام المطلوب راكد.

إن بروتوكول المستعملين (UDP) هو بروتوكول عدم توصيل (نقل) من المستوى 4. وهو بديل لاستخدام بروتوكول TCP للنقل السريع لبيانات الحجم الصغير. ولا تخضع اتصالات UDP لأي آليات رقابة، ومن ثم فليس هناك تدقيق على تحديد الهوية، التدفق أو الأخطاء. ومن نتيجة ذلك أن أي فرد يمكنه استخدام عنوان IP لأي نظام مرخص له لأجل التسلل إليه. إن سرقة دورة بروتوكول مستعملي ديتا غرام (UDP) يمكن أن تتم بدون تنبيه مخدمي التطبيق.

وحيث إن أداء مختلف البروتوكولات يعد من معلومات عامة، فإن من السهل نسبياً إساءة استخدامه، لتوليد رزم زائفة مثلاً بغرض إرباك شبكة في هجوم رفض تقديم الخدمة. وهذا يوضح الحاجة إلى الأمن من حيث علاقة ذلك بتوافر الشبكات والخدمات.

ويستغل المتسللون البروتوكولات وأوجه القصور فيها:

- لشل الشبكات؛
- لإعادة توجيه الرزم نحو مقصد زائف (نحو ذواتها مثلاً)؛
- لتحميل الأنظمة فوق طاقتها بغمرها برسائل غثة؛
- لمنع مرسل من إرسال بيانات؛
- للتحكم في تدفق إرسال رزمة، وإعاقة تداول الحركة في الشبكة والتقليل من أدائها (الدقة، والموثوقية، إلخ)

إن هجمات التسيير تشمل عادة خطوط تسيير مُرْبِكَة وبوابات تشغيل وعناوين وذلك عن طريق تزويدها ببيانات عناوين زائفة بحيث توجه البيانات وجهة خاطئة.

ويمكن للمهاجمين أن يعيدوا توجيه الرزم بسهولة نحو المقصد الذي يريدونه وذلك عن طريق استخدام خاصيات بروتوكول الإنترنت (IP) الاختيارية التي تعمل على تعريف المسار، أي بعبارة أخرى، بتحديد عناوين الأنظمة الوسيطة التي لا بد للرزمة أن تمر خلالها، ثم بتزييف هذه العناوين.

ويعرف المهاجمون كيف يستغلون، ليس فقط لخاصيات التشغيلية لبروتوكولات الاتصالات، وإنما أيضاً خصائص مختلف أنظمة التشغيل والطرق التي تعمل بها. ومن ثم يصبح من الممكن، عن طريق تحميل دارئات معينة بما لا تطيق (هجوم فيض الذاكرة) والتسبب في عطل خطير في النظام أو انهياره، وأهداف هذا النوع من الهجوم هي بالطبع تلك الأنظمة التي تؤدي خدمات مهمة إما في نقل البيانات (طرق التسيير مثلاً) أو في إدارة الأسماء والعناوين كمخدمات الأسماء مثلاً. وترمي معظم الهجمات على المواقع الشبكية إلى إغلاقها عن طريق استغلال أخطاء في نظام التشغيل.

6.2.II الهجمات على البنية التحتية الحرجة

إن مدى تعرض البنى التحتية الأساسية لمجتمع ما (إمدادات الكهرباء، المياه، النقل، لوجستيات الأغذية، والاتصالات، الصرافة والمالية، الخدمات الطبية، والمهام الحكومية، إلخ) يزداد بازدياد تجذر تكنولوجيات الإنترنت، وتصبح تلك البنى نفاذة عن طريق "شبكة الشبكات".

وثمة حاجة إلى التشديد على تعرض توليد الطاقة الكهربية وأنظمة التوزيع الضرورية لتشغيل الجزء الأكبر من البنية التحتية القومية، ومن ثم ذات الأهمية الحيوية. إن تعقد واتساع نطاق العلاقات بين مختلف البنى التحتية الحرجة جزء من قوتها، وفي نفس الوقت مصدر من مصادر تعرضها للأخطار.

ومن الضروري تأمين بوابات التشغيل بين الشبكات المستخَدَمةَ لتشغيل هذه البنى التحتية وتأمين الإنترنت. وإنشاء هيئات إقليمية أو وطنية للإشراف على حماية البنى التحتية الحرجة. ويجب أن تكون مهمتها الأولى هي تنسيق وتصميم وصيانة الخطط لحماية كل واحدة من هذه البنى التحتية. وإن الخطط والحلول الأمنية والمنسقة والمتماسكة ضرورية في حالة الطوارئ التي تضرب العديد من البنى الأساسية في نفس الوقت.

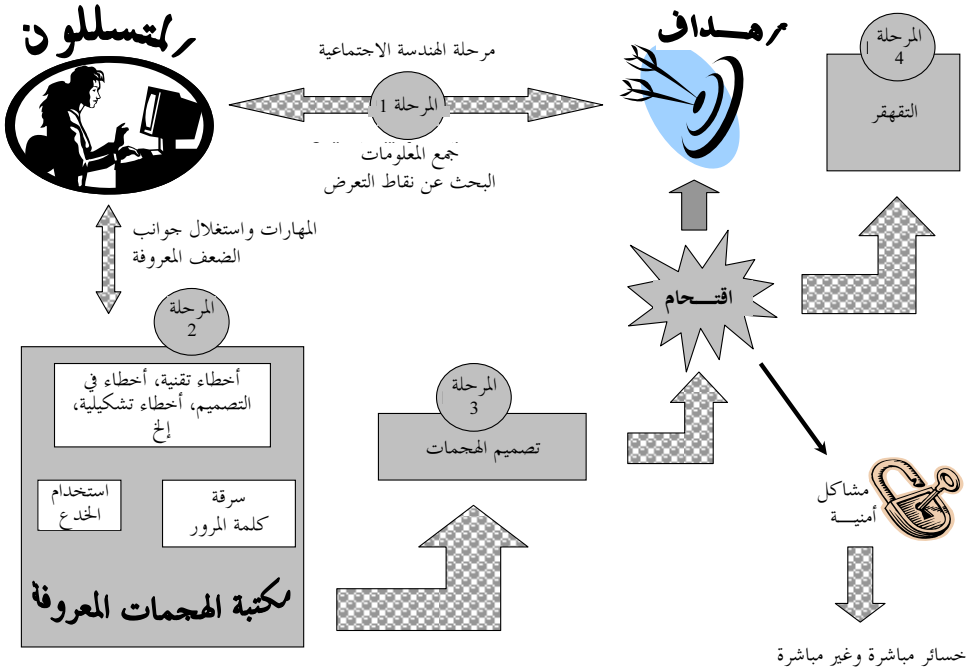
7.2.II مراحل الهجوم السيبراني

يوضح الشكل 6.II المراحل المختلفة لهجوم سيبراني[21].

إن الهدف من المرحلة الأولى هو تجميع المعلومات واستكشاف جوانب التعرض المحتملة في النظام المستهدف وذلك بغية الحصول على القدر الأكبر من المعلومات لاستغلاله مستقبلاً. وينطوي ذلك على دراسة آليات ومستويات الأمن المستخدمة في التحديد، والاستيقان، والتحكم في النفاذ، والتجفير والمراقبة، وتشخيص كوامن الضعف التقنية والتنظيمية والبشرية في البيئة. ويحاول المهاجم غالباً أن يقنع المستخدمين السُذَجْ سريعي التصديق بالكشف عن معلومات يمكن استخدامها لتصميم هجوم (ويسمى هذا هندسة اجتماعية).

[21] توضيح مأخوذ من "Sécurité informatique et télécoms: cours et exercices corrigés"، س. غرناؤطي–هيلي، دنود 2006.

الشكل 6.II – المراحل النموذجية في هجوم سيبراني



يمكن للمتسللين أن يبحثوا وأن يستغلوا – نقاط التعرض الأمني المعروفة – التي لم يتم علاجها (ترقيعها) بعد وذلك، باستخدام الوسائل المتاحة (مكتبات الهجمات، صناديق أدوات الهجمات) للتسلل إلى النظام. والغرض من مرحلة التقهقر هو التغطية على آثار الهجوم، وضمان ألا تسمح الآثار المتروكة بالكشف عن هوية المهاجم. ويزيد المتسللون من تخفيهم باستخدام الألقاب، واغتصاب هويات مستخدمين قانونيين، أو بتغطية آثارهم بواسطة أنظمة (ترحيل) وسيطة متعددة.

الجـــزء III

النهـــج التكنولوجـــي

القسم 1.III البنى التحتية للاتصالات

1.1.III الخصائص

إن شبكة الهاتف بفضل تغطيتها الجغرافية الشاسعة قد غدت الشبكة الأولى التي تخدم عدداً كبيراً من المستعملين. ويمكن اليوم لشبكة الهاتف أن تُستَعمل ليس فقط في حمل الكلام وإنما البيانات أيضاً. وهكذا أصبح من الممكن، عن طريق الوصلات البينية اللازمة، الربط بين الحواسيب على شبكة الهاتف. وفي السنوات الأخيرة، تكاثرت نقاط النفاذ إلى الإنترنت أيضاً، ولا تزال المقاهي السيبرانية آخذة في التزايد ويجري تزويد المزيد والمزيد من البلدان ببنية تحتية لنقل أيسر استعمالاً وأقدر. وفي بعض الأماكن يجري نشر شبكات بالكبل لدعم نقل القنوات التلفزيونية.

وبالإضافة إلى البنى التحتية الثابتة للاتصالات توجد أيضاً ما يعرف بالبنى التحتية "اللاسلكية" التي تسمح للمستخدم بالحركة. وتدعمه البنى التحتية ساتلية وفضائية والأنظمة الراديوية الأرضية التكنولوجيات اللاسلكية. ولقد غدا التهاتف المتنقل في السنوات الأخيرة وسيلة لتقديم الخدمات في الكثير من البلدان النامية.

ولقد وطد معيار "GSM" أي (نظام الاتصالات المتنقلة) نفسه لدى العديد من القارات لنقل الصوت وكميات صغيرة من البيانات في بعض الأحيان. ومع ذلك فإنه يمثل الرعيل الجديد من شبكات المحمول القائمة على معيار أنظمة الاتصالات (MTS) الذي يوفر قدرات نقل أفضل ويمهد الطريق أمام الاستخدام الأوسع للأجهزة النقالة متعددة الوسائط. أما وقد قلنا ذلك، فإن شبكات GSM آخذة في التطور، لإدماج GPRS (الخدمة الراديوية العامة بالرزم) التي تسمح بسرعات إرسال أكبر للوفاء باحتياجات استخدامات البيانات في شبكات الهواتف النقالة.

إن الوصول المفاجئ للتكنولوجيات مثل GSM لا يعكس تغيراً تكنولوجياً فحسب وإنما تغيراً سلوكياً واقتصادياً أيضاً. والاتصالات النقالة صناعة مزدهرة داخل سياق تنافسي عالمي شرس. فقد سمحت بتقديم خدمة جديدة هي التهاتف الراديوي بالدخول إلى سوق الاتصالات الذي كان قد ظل حتى ذلك الحين قاصراً على المشغلين الاختصاصيين، بينما تُشَيِد بنية تحتية يمكن إعادة استخدامها في جميع أنواع نقل البيانات.

وبغض النظر عن التكنولوجيا المستخدمة في نشر الخدمات الإلكترونية، ينبغي للبنى التحتية للاتصالات لدى البلدان النامية أن تسمح بـــ:

- الوصل الشبكي البيني الرقمي الموحد (الصوت، البيانات، الصورة) لمجموعة مُعَرفة من الخدمات الأساسية التي يسهل إقامتها وصيانتها وتعطي التغطية الجغرافية المطلوبة (الوطنية والدولية)، داخل إطار نهج كلي-النوعية (مستدام، مستقر يعطي أدق التفاصيل ويمكن تغييره بتكلفة تقنية واقتصادية زهيدة) وبالقدر الأكبر من الأمن؛
- التنسيق التقني والتجاري: الوقاية من تكوين الكارتلات المحتمل بأمل تطوير متناغم للبنى الأساسية والخدمات، مع ضمان التنظيم النشط لحالات إساءة استخدام المواقع المسيطرة؛

2.1.III المبادئ الجوهرية

تتكون شبكة الاتصالات من مجموعة معلومات وموارد إرسال تعمل معاً وتقدم خدمات الاتصال. وتسمح هذه الخدمات بالنفاذ عن بعد والتشارك في موارد المعلومات المتصلة بينياً، وبالربط البيني للاستخدامات والأشخاص، والتنفيذ عن بعد للبرامج ونقل المعلومات.

وترتهن جميع الأنشطة الاقتصادية حالياً بصورة حرجة بتوافر بنية تحتية للاتصال تتسم بالكفاءة وتربط بين جميع أنواع المعدات، والاستخدامات والأشخاص، وتمكنهم من العمل معاً بغض النظر عن المسافة أو المكان أو نوع تدفقات المعلومات المراد نقلها.

يتم التمييز بين الشبكات بالدرجة الأولى على أساس عدد من المعايير مثل الشمول الجغرافي، والطوبولوجيا[22]، والتكنولوجيا المستخدمة، والتطبيقات المدعومة، وطريقة التشغيل، ونوع وسط الإرسال (خط سلكي/لاسلكي) وطبيعتها الخاصة والعامة، إلى غير ذلك.

ومن الناحية التاريخية، كانت أولى الشبكات شبكات ذات مساحة واسعة[23] (هاتف، تلكس، ترانسباك، إنترنت، إلخ). وقد ظهرت شبكات المناطق المحلية مع أولى طلائع الحواسيب الشخصية (في بداية الثمانيات)[24].

وقد غدت هذه الفروق—مؤخراً—أقل ظهوراً حيث إن الشبكات المعنية مترابطة بينياً. وقد تكون شبكة المنطقة المحلية مرتبطة بشبكات المناطق المحلية الأخرى، ومن ثم تصبح شبكة أكبر. ولم تعد الشبكات – فضلاً عن ذلك – مخصصة لتعزيز نوع واحد من التطبيق. وإنما يمكن إرسال الصوت، البيانات وصور الفيديو (الشبكة متعددة الوسائط). ويمكن للشبكة أن تكون خاصة، تنتمي لمنظمة لديها حقوق استخدام حصرية، أو عامة. ففي الشبكات العامة، يتم توفير خدمات الاتصالات لمختلف الأفراد والمؤسسات على أساس ترتيبات اشتراك خاصة.

إن بروتوكول التحكم في الإرسال/بروتوكول الإنترنت هما التكنولوجيتان الرئيسيتان في الإرسال المستخدمين في الشبكات المحلية الواسعة، وفي الترحيل الإطاري (Frame relay) (أسلوب النقل اللاتزامني). وفي سوق شبكات الأعمال المحلية، فإن شبكة الإثرنت (ethernet) هي التكنولوجيا الرئيسية وتنويعاتها عالية السرعة (إثرنت السريعة – إثرنت المُبَدلة (switched ethernet)).

وفي ميدان الاتصالات، تمثل تكنولوجيات النقل البصري، وأسلوب النقل اللاتزامني خطوة كبرى على طريق تطوير البنى الأساسية وشرايين الإرسال، حيث تساعد الإرسال عالي السرعة وعالي النوعية، وتخصيص عرض النطاق دينامياً، ومعدلات البنى المتنوعة والاستخدام المتعدد الأطراف.

3.1.III مكونات الشبكة

1.3.1.III وسائط الربط البيني

ولربط الحواسيب معاً وداخل الشبكة، يلزم وجود وسائط إرسال. وقد تكون هذه الوسائط مادية (أزواج من الكبلات المبرومة، كبلات متحدة المحور، وليف بصري) أو وسائط غير ملموسة (الراديو، أمواج الأشعة دون الحمراء). وهذه الوسائط المختلفة لكل منها خصائص نوعية تحدد مدى إمكانية الاعتماد عليها والقدرة على حمل المقادير المتفاوتة من المعلومات بسرعات مختلفة.

ويقدر الإرسال أو قدرة وسط الربط البيني بكمية المعلومات المنقولة خلال فترة زمنية محددة. ويعبر عن هذه القدرة بالكيلو، أو الميغا أو حتى بمليون مليون بتة في الثانية الواحدة (مثل 100 Mbit/s). ويكون ذلك متناسباً مع عرض النطاق لوسط الإرسال، وهو ما يناظر مجال ترددات إشارة يمكنها أن تمر عبر هذا الوسط بدون أي تعديل.

---

22 طوبولوجيا شبكة ما هي نسق الوصلات التي تربط بين مختلف العناصر أو العُقَدْ.

23 شبكة المساحة الواسعة هي شبكة تربط تمديد الحواسيب فوق إقليم جغرافي واسع نسبياً (أكثر من 100 كم).

24 تسمى الشبكة "شبكة محلية" (LAN) عندما تصل بين حواسيب في منطقة صغيرة جغرافياً لا تزيد مساحتها عن بضعة كيلومترات (~10 كيلومترات). أما الشبكة الحضرية فهي تصل شبكات محلية قد تنتمي إلى كيانات مختلفة وتصل مساحتها الجغرافية إلى نحو 100 كيلومتر. وتوضع مصطلحات جديدة لتصف أنواعاً مختلفة من موارد الشبكات أو لتصف مجال تطبيق محدداً. وعلى سبيل المثال ترد مختصرات مصطلحات مثل HAN (شبكة منـــزلية) وهي شبكة تصل بين أجهزة في المنازل قابلة للتحكم فيها عن بعد، (فرن، فيديو، أجهزة تدفئة وإضاءة، إلخ)، CAN (شبكة سيارات)، SAN (شبكة تخزين)، إلخ.

2.3.1.III مكونات الربط

إن نوع الربط أو مكون الربط الذي يتم إدخاله بين وسط مُرْسِل وحاسوب لربط الاثنين، إنما يعتمد على نوع الوسط، وأسلوب الإرسال المستَخدَم. كما أن صندوق الربط أو السطح البيني للشبكة يحل مشاكل التوصيلية ويعدل الإشارة المرسلة أو الواردة إلى حاسوب إلى إشارة يمكن إرسالها عبر هذا الوسط. فمثلاً، يوفر المودِمْ (المشكل – المزيل) سطحاً بينياً بين الحاسوب الذي هو آلة رقمية تقوم بمعالجة الإشارات الرقمية، ووسط إرسال كخط هاتفي تماثلي يقوم بإرسال إشارات بشكل متواصل[25]. ومن الناحية النظرية، يمكن ربط مكون إلكتروني بالشبكة ما دام كان مزوداً بسطح بيني مناسب يربط عتاد الكمبيوتر والبرمجيات.

3.3.1.III الآلات المتخصصة ومخدمات البيانات

وبغض النظر عن الأنظمة المُستَخدِمة التي تخدم النفاذ إلى الشبكة والحواسيب المخصصة لإدارة ومعالجة التطبيقات (حواسيب البيانات الرئيسية والمخدمات) فإن معالجات الاتصالات تشكل البنية التحتية للنقل في الشبكة. فهذه حواسيب تقوم بوظيفة أو أكثر من الوظائف اللازمة لإدارة وإقامة الاتصالات (تعظيم استخدام الموارد، والتقاسم، وتسيير البيانات، وإدارة العناوين، والأسماء، والربط البيني، إلخ). وهي تضم، مثلاً، أدوات تسيير، ومعدات الإرسال، وممركزات، ومبدلات (switches) أو بوابات تشغيل للربط البيني.

ولإجراء الاتصالات، يجب أن يتم إرسال المعلومات بطريقة يُعَوَّل عليها طبقاً لترتيبات التبادل المُرضِية للمتراسلين. والنقطة المهمة هي أن الأنظمة الموصلة بينياً على شبكات الاتصالات تكون من باب أولى مختلفة. ومن أجل التمكن من إجراء حوار، ينبغي لها أن تستخدم نفس الإطار المرجعي للاتصالات، أو بعبارة أخرى تتحدث نفس اللغة وتتبع قواعد تبادل مشتركة.

وهذا شبيه بشخصين يتحدثان لغتي أم مختلفتين ويرغبان في تبادل معلومات، وعلى استعداد للاتفاق على اللغة التي سيستخدمانها. فقد يبذل أحدهما الجهد للتحدث بلغة الآخر، أو قد يستخدما لغتهما الثالثة المشتركة.

فإذا انضم عندئذ شخص ثالث أو رابع أو خامس إلى آخره إلى هذه المحادثة الأولى، وكان هؤلاء الأشخاص يتحدثون لغات أخرى، فمن المحتمل أن يصبح من الصعب عليهم تبادل المعلومات إذا كانت إحدى اللغات سوف تترجم إلى لغة أخرى لكل زوج من المتحاورين. وفي هذه الحالة، يكون من المفضل التحدث بلغة مشتركة تستخدمها جميع الأطراف الضالعة.

وبالمثل، ينبغي للحواسيب الموصلة شبكياً أن تحترم نفس بروتوكولات الاتصال وأن تتبع نفس قواعد الحوار حتى تتمكن من التواصل. وهذه البروتوكولات مدمجة في برمجيات الاتصال. وهي تخدم أغراضاً من بينها التأكد من سلامة تسيير البيانات وضمان التشغيل المشترك للتطبيقات والأنظمة البعيدة.

إن المعايير الدولية أو المعايير الواقعية يتم تعريفها بواسطة هيئات معترف بها من جانب الدوائر الصناعية كلها. فإن المنظمة الدولية للتوحيد القياسي (ISO) والاتحاد الدولي للاتصالات هما منظمتان دوليتان للتوحيد القياسي توصيان بالمعايير الدولية (مثل سلسلة X.400).

إن المعيار الواقعي هو معيار وإن كان غير معتمد من جانب هيئة من هاتين الهيئتين فإنه يستخدم على نطاق واسع في السوق، وهو يصبح عندئذ مرجعاً، أيْ معياراً واقعياً. وكل البروتوكولات النابعة من مجتمع الإنترنت مثلاً هي معايير واقعية.

[25] كي يكون بالإمكان نقل المعلومات الخارجة من الحاسوب عبر هذا الوسط، لا بد من تشكيل هذه المعلومات. والمعلومات المنقولة بشكل تماثلي ينبغي إزالة تشكيلها عند الاستقبال وعرضها في شكل رقمي إلى الحاسوب المقصود. ويقوم جهاز واحد هو المودم بتشكيل وإزالة تشكيل المعلومات التي يرسلها أو يستلمها الحاسوب.

وتعرف المعايير عدة أشياء من بينها نوع الخدمات التي ينبغي أن تقدمها بروتوكولات الاتصال وأن تحدد كيفية إنشائها. وهذا يجعل بالإمكان تصميم حلول بياناتية يمكنها التواصل فيما بينها. ولذا، فإنه باستخدام نفس أنواع البروتوكولات في ماكينات مختلفة (غير متجانسة) يمكنها أن تتواصل. إن الطبيعة الشاملة للإنترنت تتوقف على إدماج بروتوكولات أسرة الإنترنت في جميع الماكينات المُوَصَلَة.

4.1.III البنية الأساسية للاتصالات والطريق السريع للمعلومات

نحن نعني بالبنية التحتية للاتصالات، جميع وسائط الإرسال التي يمكن إنشاء خدمات الاتصال عليها. ويمكن وضع خط فاصل بين قنوات الإرسال وتكنولوجيات تحديد المسار من ناحية، وبين حلول وخدمات الاتصالات التي تقدم للزبائن من ناحية أخرى. وهكذا يكون من الممكن، دون امتلاك البنية الأساسية القائمة استغلالها كمرفق نقل لتقديم استخدامات بعينها.

ومع توافر المعدات متعددة الوسائط والبنى التحتية للاتصالات عالية الأداء، وكذلك تلاقي عالم تكنولوجيا المعلومات المسموعة المرئية مع عالم تكنولوجيا الاتصالات، يبرز مفهوم سلسلة المعلومات الرقمية الكاملة: فالاستمرارية الرقمية بين جميع مصادر المستخدمين والمستعملين، سواء داخل البنية التحتية للنقل وعلى مستوى المحتوى.

إن مفهوم الطريق السريع للمعلومات يشمل الإمداد واسع النطاق، عبر البنى التحتية للاتصالات عالية الأداء، بطائفة من الخدمات العامة والتجارية التي تساعد على تحسين مستويات الناس المعيشية، في ميدان الصحة مثلاً والتعليم والثقافة وتخطيط الأراضي وإدارة وسائل الإعلام. وبفضل طبيعة بعض الخدمات المقدمة على الإنترنت، يمكن اعتبار الأخيرة طريقاً سريعة للمعلومات.

1.5.III الإنترنت

1.5.1.III الخصائص العامة

بدأت الإنترنت في الولايات المتحدة الأمريكية وانتشرت انتشاراً حثيثاً عن طريق ربط أنظمة المعلومات المتجاورة وشبكات الحاسوب. ولا يزال هذا النمو الشبكي مستمراً. وهو يحدد هيكل الشبكة التي هي شبكة الشبكات. ولا يمكن أن تتحقق سيطرة شاملة على جميع البنى الأساسية المتراصة الواحدة تلو الأخرى ما دامت مستقلة وتنتمي إلى منظمات مختلفة.

فمن حيث العَتاد، تتألف الإنترنت، مثلها مثل أي شبكة اتصالات من أنظمة معلومات، ومن عناصر ربط ووسائل إرسال. وتشمل أنظمة المعلومات تلك الأنظمة التي تستخدم للنفاذ إلى الشبكة والسماح بالحوار مع المستعمل النهائي (الحاسوب الشخصي، الهاتف النقال، وجهاز الاستدعاء، والقوس المحدد مسبقاً PDA، إلخ) وتلك التي تساند التطبيقات (مخدم الويب، ومخدم قاعدة البيانات، إلخ) وتلك المخصصة للمعالجة داخل الشبكة (محددات التسيير، وبوابات التشغيل للوصل البيني، إلخ).

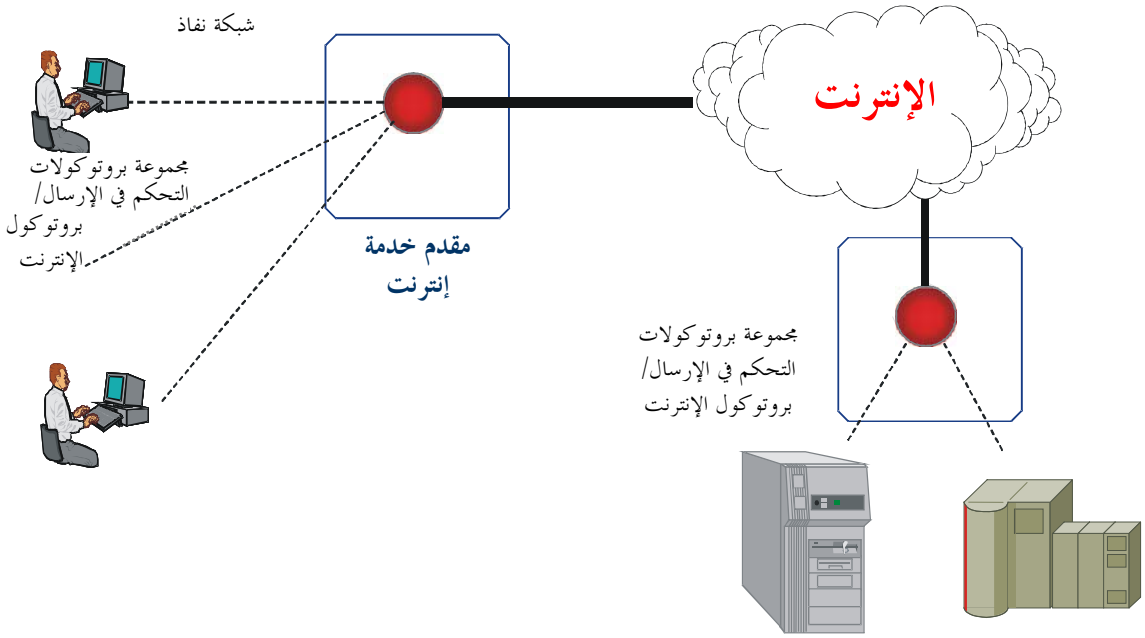
يتم تبادل البيانات بين الحواسيب عبر وسائط الإرسال التي تربط بينها مادياً. فعندما تكون نقطة النفاذ إلى البنية الأساسية للإنترنت تمر عبر نظام يسمح بحركية المستخدم من قبيل الهاتف النقال مثلاً، نكون عندئذ بصدد الحديث عن إنترنت نقالة.

تحقق بروتوكولات الاتصال من أسرة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت TCP/IP[26] نقل البيانات، وتسيير الاتصالات بين عمليات المعلومات الموزعة والمستخدمين البشريين. وهذه المبادلات للبرمجيات، الموحدة قياسياً في عالم الإنترنت، تمثل السطح البيني للاتصال الذي يساعد على مختلف أنواع أنظمة التشغيل المتبادل. وللاتصال في

[26] TCP/IP بروتوكول التحكم في الإرسال/بروتوكول الإنترنت.

بيئة الإنترنت، يجب تزويد حاسوب ما ببروتوكولات الاتصال هذه، وأن يكون هناك عنوان بروتوكول الإنترنت يتيح لذلك الحاسوب هوية فريدة (الشكل 1.III).

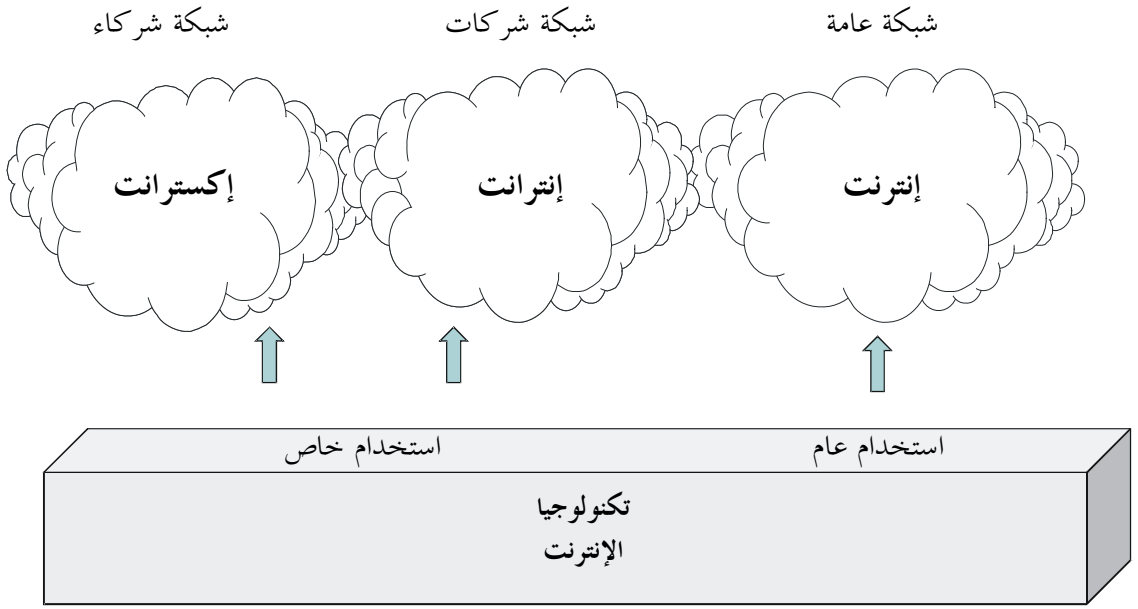
الشكل 1.III – النفاذ إلى الإنترنت عبر نقطة التشوير الدولية، وهي جناح من بروتوكولات وعنوان فيما بين الأشخاص



تقوم الإنترنت بتعيين كامل البنية الأساسية للاتصالات التي يتم توفيرها للجمهور بهدف الاتصال. وعندما ترغب منظمة في استخدام هذا البناء التحتي، وعندما ترغب منظمة في استخدام هذه البنية التحتية بصورة سرية وتقيدية فإنها تنشئ شبكة افتراضية خاصة (VPN). وقد تستخدم أيضاً، للاحتياجات الداخلية، تكنولوجيات الإنترنت لإنشاء شبكة خاصة أو إنترنت. وحينما تكون الإنترنت مفتوحة أيضاً أمام عدد من الشركاء (العملاء، الموردون، إلى آخره) فإنه يطلق عليها اسم إكسترانت (الشكل 2.III).

إن الشبكة القائمة باتساع العالم (أو "الويب" من باب الاختصار) جنباً إلى جنب مع البريد الإلكتروني، هي أهم تطبيق للإنترنت. فعلى أساس الملاحة في أنحاء الويب أمكن تطوير مجموعة حاشدة من الخدمات. فمن الممكن الإبحار في أرجاء الويب وذلك بفضل برمجيات العملاء، وبرنامج التصفح الذي يُركَبْ في محطة عمل المستخدم، ويسمح بالنفاذ عن بعد إلى مخدمات الويب. ويمكن استخدامه في البحث، أو الاستشارة أو إرسال المعلومات أو حتى أن يدير برامج. إن فكرة تصفح أو الانزلاق على الويب تنبع من حقيقة أن الوثائق التي يمكن النفاذ إليها عبر استخدام الويب هي وثائق فائقة (hyperdocuments) ومعنى هذا أنها صممت، ونظمت وشُكلت بصورة يمكن قراءتها بطريقة غير تتابعية وذلك بإدخال الوَسْمَات أو الوصلات عندما أنشئت. إن تنشيط وصلة إما تأخذ القارئ إلى جزء آخر من الوثيقة أو إلى وثيقة أخرى، ربما كانت موجودة على حاسوب بعيد. وهكذا يتزلج المرء من موقع إلى موقع عن طريق تنشيط هذه الوصلات الفائضة.

الشكل 2.III – الإنترنت – الإنترانت – الإكسترانت



2.5.1.III عنوان في بروتوكول الإنترنت واسم الميدان

يتم النفاذ إلى شبكة الإنترنت عبر نقاط نفاذ يديرها ويسيطر عليها مشاريع متخصصة تسمى مقدمي خدمة الإنترنت (ISP). وكل واحد من مقدمي خدمة الإنترنت مرتبط هو نفسه بالإنترنت عبر خطوط الاتصال دائمة تتقاسمها مع عملائها المختلفين. يضاف إلى هذه الخدمة الأساسية، أنه يقدم بصفة عامة خدمة إدارة بريد إلكتروني ويمكن أيضاً أن يستضيف المواقع الشبكية لعملائه.

وللاتصال على الإنترنت يحتاج المرء إلى عنوان على الإنترنت (عنوان بروتوكول الإنترنت). وهذه متتالية ثنائية 32 بتة معاً تحدد بوضوح كل آلة تقوم بالاتصال على الإنترنت[27].

ويعبر عن عنوان الإنترنت بشكل عشري، يتكون من أربعة أرقام عشرية تفصل بينها نقط (full stops). فمثلاً العنوان 128.10.2.30 يناظر القيمة الثنائية 10000000.00001010.00000010.00011110. حيث إن من المستحيل تذكر متتاليات هذا الرقم، حتى العشرية منها. والأسماء (وهي غالباً تذكرية) أو عناوين منطقية، وهي تستخدم لتحديد الموارد في بيئة الإنترنت. وعناوين الإنترنت هذه الأسماء المقارنة لها تخزن وتدار في أدلة إلكترونية يطلق عليها اسم مخدمات servers تعرف في الواقع بالاسم الأولى DNS (domain name server) (مخدم اسم الميدان).

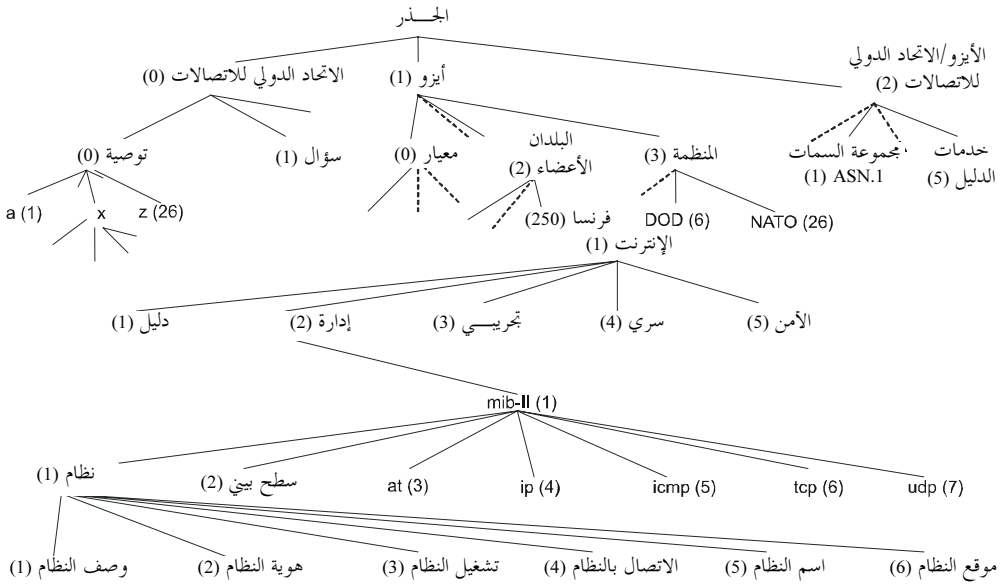
ولتنفيذ الاتصالات في بيئة مفتوحة، من الضروري أن تتوافر القدرة على تخصيص مُعَرف هوية فريد في ميدان تسمية معين. ويجب أن تكون الأطراف الضالعة في الاتصال قابلة للتعريف (العناوين، الأنظمة، عمليات التطبيق، الكيانات، أهداف الإدارة، إلخ) مثلما يجب أن تكون أدوات التنفيذ أدوات للاتصال (بروتوكولات). ولكي تتم تأكيد السلطات المختصة عبر العالم، توجد تدابير لتسجيل الأسماء ذات السلطات بواسطة سلطات مختصة يكون دورها هو تخصيص مُعَرف واضح وفريد لكل هدف يراد تعريفه.

[27] عنوان بروتوكول الإنترنت هو عنوان فريد. ويمكن تخصيصه بشكل دائم (عنوان ثابت) أو بشكل غير دائم (عنوان دينامي).

يحدد معيار المنظمة الدولية للتوحيد القياسي (الأيزو) 9834 سلطات التسجيل وتنظيمها في شكل شجرة هيرارشية. يحتوي جذر الشجرة على ثلاثة أفرع، تؤدي إلى عُقَدْ مميزة من المستوى الأول تمثل ميادين التسمية (naming domains) ولجنة ITU، ISO واسم للجنة مشتركة من الأيزو – والاتحاد الدولي للاتصالات. ويرخص المستوى الذي يأتي مباشرة تحت ISO تسجيل عدة أشياء من بينها:

- مختلف معايير الأيزو (معيار صفر)؛
- أعضاء الأيزو (عضو – هيئة 2) نجد تحتهم AFNOR (208) وANSI (310)؛
- المنظمات (المنظمة (3))، نجد تحتها مثلا وزارة الدفاع الأمريكية (DOD) (6) (الشكل III.3).

الشكل III.3 – سلطات وشجرة التسجيل



وأسماء الميادين التنوعية على الإنترنت مدونة في هذا الشكل المنطقي للتسجيل. والجزء ذو الصلة من شجرة التسجيل في هذه الحالة هو العقدة الجذرية لأسماء ميادين المستوى الأعلى (TLD). وهذه الأسماء تُعَرف بالدرجة الأولى البلدان المشار إليها بحرفين مثل (fr, it, uk, ch, nl, de, etc.)، والميادين الوظيفية مثل:

- .com المنظمات التجارية؛
- .edu المؤسسات الأكاديمية في أمريكا الشمالية؛
- .org المنظمات، مؤسسية أو غير ذلك؛
- .gov الحكومة الأمريكية؛
- .mil المنظمات العسكرية الأمريكية؛
- .net مشغلو الشبكة؛
- .int الكيانات الدولية؛
- .biz لعالم الأعمال؛
- .info لجميع الاستخدامات؛

- .name للأفراد؛
- .museum للمؤسسات التي تحفظ فيها مجموعات الأشياء وتصنف للحفظ أو للعرض على الجمهور؛
- .aero لصناعة النقل الجوي؛
- .coop للتعاونيات؛
- .pro للمهن.

ويوجد داخل تسميات الميادين الفضفاضة هذه، توجد ميادين فرعية، تناظر مؤسسات مهمة كبيرة.

إن سلطة الأرقام المخصصة التابعة للإنترنت (IANA)[28] داخل مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN)[29] هي المسؤولة عن تخصيص الأسماء والعناوين، ويجب عليها أن تتأكد من أنها كلها فريدة. ويجوز تفويض مسؤولية الأسماء إلى ميدان فرعي ينطوي هرمياً تحت سلطتها.

ويتكون تسجيل اسم الميدان من إدخال مُدْخَل في دليل الأسماء. وهذا يعادل خلق قوس جديد في شجرة التسجيل التي تتولى إدارتها منظمة مخوَّل لها ذلك. وهناك العديد من ذلك على المستوى العالمي، لا سيما للميادين (biz, .com, .info, name, .net, .org).

أما في حالة فرنسا، مثلاً، فإن سلطة التسجيل (دليل المُسَجِلْ المعتمد) والمعتمد من جانب مؤسسة الإنترنت للأسماء والأرقام المخصصة فهي أفنيك (AFNIC)[30].

وتوكل سلطة تخصيص وإدارة العناوين إلى الرابطة الأمريكية – على الأرض الأمريكية، الخاضعة للقانون الأمريكي[31]. وهكذا؛ فإن هذه الرابطة تهيمن على النفاذ إلى الإنترنت الأمر الذي يخلق مشكلة حقيقية هي اعتماد المنظمات والدول على هيئة أجنبية فوقية مهمتها أن تكون مفتوحة أمام بقية العالم ولكن التمثيل غير أمريكي داخلها ضعيف.

إن معيار الأمن من زاوية توافر (البنية التحتية، والخدمات، والبيانات)، والتي تتوقف على النفاذية إلى شبكة الإنترنت، لا يمكن مراقبته أو التحكم فيه بواسطة المنظمات. فالمنظمات تعتمد، في نفاذها إلى الإنترنت، على تخصيص عناوين الإنترنت وأسماء الميادين، ومن ثم على كيانات خارجية.

ويمكن اعتبار أدلة أسماء الميادين قواعد بيانات تدار بواسطة مخدمات اسم الميدان. وهناك نحو خمسة عشر مخدماً لاسم الميدان يجري تنسيقها بواسطة مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN)، كما أن الأغلبية الكبرى من مخدمات الجذور موجودة في أمريكا الشمالية. وهي تدير أسماء الميدان وعناوين الإنترنت ذات المستوى الأعلى. ويشمل ذلك جميع الميادين المشار إليها آنفاً (org.com إلخ) وكذلك 244 اسماً ميدانياً للبلدان المختلفة (الصين – cn، غابون – ga، سري لانكا – lk، بولينيزيا الفرنسية – pf، إلخ). ومخدمات اسم الميدان المحلية وتسمى المُبَيِنَاتْ (Resolvers) تحتفظ بنسخة من المعلومات الواردة في المخدمات الجذرية. وهذه المبينات التي توجد غالباً مرتبطة بنقاط

[28] http://www.jana.org

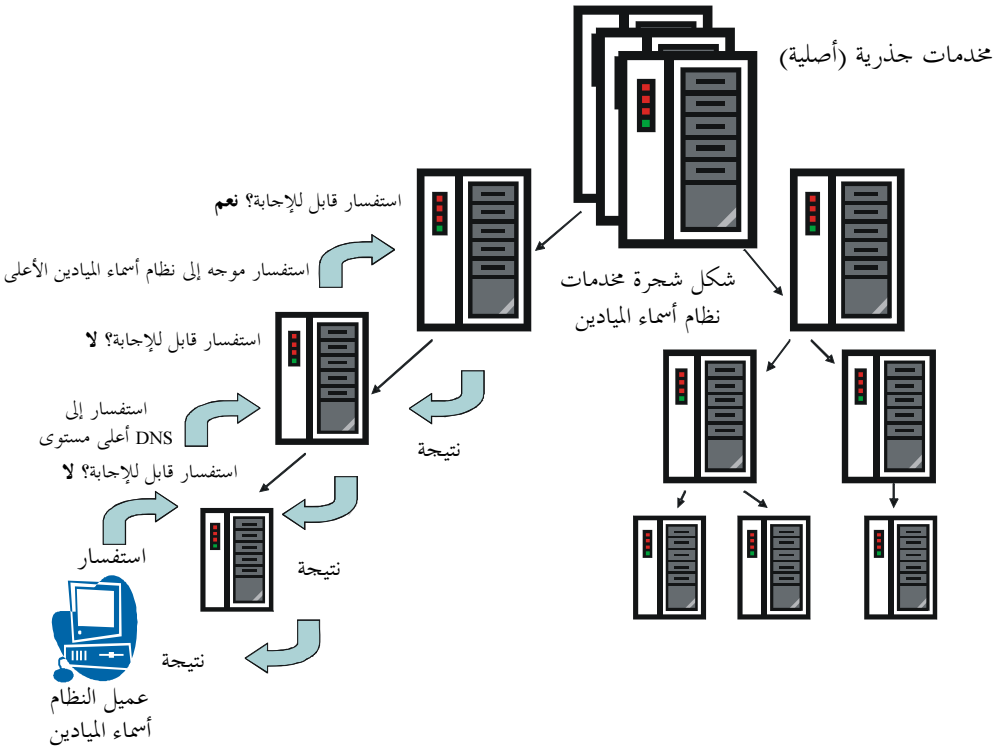
[29] http://www.icann.org/index.html

[30] http://www.afnic.fr

[31] وتبعاً لإيكان (ICANN): فإن "شركة الإنترنت للأسماء والأرقام المخصصة هي شركة منظمة دولية، غير إرباحية مسؤولة عن بروتوكول الإنترنت (IP) وتخصيص مساحات العناوين، بروتوكول تخصيص المُعرفات، تنوعة (gTLD) والشفرة الوطنية (ccTLD) الإدارة العليا لنظام اسم الميدان ووظائف إدارة نظام المخدمات الجذرية. وكانت هذه الخدمات تتم أصلاً بموجب عقد من الحكومة الأمريكية من سلطة الإنترنت للأرقام المخصصة (IANA) وكيانات أخرى. وتقوم ICANN الآن بوظائف (IANA)".

النفاذ التابعة لشبكة استراتيجية أو مرتبطة بمقدمي خدمات الإنترنت، مهمتها الرد على تساؤلات المستخدمين فيما يتعلق بترجمة اسم الميدان إلى عنوان إنترنت (الشكل 4.III)[32].

الشكل 4-III – شكل شجرة مخدمات نظام أسماء الميادين DNS



من الحيوي أن تتسم العناوين والعمليات والأنظمة الضالعة في إدارة الأسماء والعناوين وتسيير البيانات بالوفرة والاستقامة والعِوَّل والأمن. وتقع على الكيانات المسؤولة عن البنى التحتية للنقل مسؤولية حماية بيئات الاتصال لديها وإدارتها إدارة فعالة.

3.5.1.II النسخة 4 من بروتوكول الإنترنت IPv4

لا تزال النسخة 4 من بروتوكول الإنترنت[33] (IPv4) ، الموجودة منذ بدايات شبكة الإنترنت مستخدمة على نطاق واسع. ويتمثل دور هذا البروتوكول في كَبْسَلَةُ البيانات لأجل إرسالها بغرض تكوين رزم بروتوكول الإنترنت (IP packets) التي سوف يتم تسييرها على شبكة الإنترنت إلى مقصدها. وتشمل كل رزمة، إلى جانب أشياء أخرى، على العنوان المصدري لبروتوكول الإنترنت الخاص بالمرسل وعنوان IP لنظام المقصد.

ويتم التسيير عن طريق التسليم إلى كل نظام وسيط (router) يتم عبوره عند تفسير عناوين الرزمة وخوارزمية التسيير التي يقدمها النظام الوسيط.

[32] الشكل مأخوذ من "Sécurité informatique et télécoms: cours et exercices corrigés"؛ س. غرناؤطي–هيلي، دنود 2006.

[33] IPv4 and main TCP/IP protocols: IPv4: RFC 0791 –www.ietf.org/rfc/rfc0791.txt TCP: RFC 0793 – www.ietf.org/rfc/rfc0793.txt – UDP: RFC 0768 –www.ietf.org/rfc/rfc0768.txt – FTP: RFC 0959 – www.ietf.org/rfc/rfc0959.txt – HTTP version 1.1: RFC 2616 –www.ietf.org/rfc/rfc2616.txt – Telnet: RFC 0854 – www.ietf.org/rfc/rfc0854.txt

ولا تشتمل النسخة 4 من بروتوكول الإنترنت IPv4 على أي وظيفة أو آلية لضمان أمن الخدمة. وفي الحقيقة أن (IPv4) لا توفر أي طريقة للاستيقان من مصدر الرزمة أو مقصدها، ولا لتأمين سرية البيانات المنقولة أو عناوين بروتوكول مونتريال الضالعة في نقل المعلومات بين كيانين. يضاف إلى ذلك أنه طالما أن البروتوكول يعمل بأسلوب عدم التوصيل فلا يوجد ضمان لـــ:

- تسليم البيانات (احتمال فقدان البيانات)؛
- تسليم البيانات إلى المرسل إليه المقصود؛
- تسليم البيانات التسلسل السليم للبيانات.

إن بروتوكول الإنترنت (الطبقة 3 من معمار الأنظمة المفتوحة للتوصيل البيني (layer 3 of the OSI architecture)) يقدم رزمة تسليم لخدمة بروتوكول الإنترنت لا يُعَوَّل عليها. فهو يعمل بأسلوب ما يسمى بـــ"أفضل جهد". أو بعبارة أخرى أنه يبذل قصارى جهده في الظروف المحيطة ويكون تسليم الرزمة غير مضموناً. وفي الحقيقة لا يوجد أي ضمان لجودة الخدمة ولا يوجد استرداد للرزمة إذا سُلِمتَ خطأً. وهكذا يمكن للرزمة أن تفقد، أو تُغَير، أو تستنسخ، أو تزور، أو تسلم في غير تسلسلها بدون علم المرُسل أو المتُلَقي. وحيث لا توجد علاقة منطقية سابقة بين المرسل والمتلقي، فإن هذا يعني أن المُرسِل يرسل رزمة بدون إعلام المتلقي بذلك، وهكذا يمكن أن تُفْقد، أو أن تتخذ طرقاً مختلفة أو أن تصل حسب ترتيب خاطئ.

وللتغلب على رداءة الخدمة هذه، يتم تركيب بروتوكول التحكم بالإرسال/(TCP) في الأنظمة النهائية. ويوفر هذا البروتوكول TCP خدمة نقل مضمونة بأسلوب توجيه التوصيل (الطبقة 4 من معمار الأنظمة المفتوحة للتوصيل البيني (OSI). ومع ذلك، فإن بروتوكول التحكم بالإرسال TCP لا يوفر أي خدمة أمن بالمعنى الحقيقي للكلمة.

القسم 2.III – أدوات الأمن

إن تأمين سلامة المعلومات والخدمات والأنظمة والشبكات يستتبع تأمين توافر وسلامة الموارد وسريتها وكذلك عدم رفض أعمال معينة، والتيقن من الأحداث والموارد.

ويكتسب أمن البيانات معنى فقط إذا طبق على البيانات والعمليات التي نكون على ثقة من أنها دقيقة (فكرة نوعية البيانات وعملياتها) بحيث تتوافر له الاستقرار مع مرور الوقت (فكرة استقرار البيانات واستمرارية الخدمة).

وتتأسس حلول الأمن الرئيسية على استخدام التجفير أو الأساليب التقنية لعزل البيئة، وعلى احتياطي الموارد المتوافرة، وعلى التدابير المراقبة، والرقابة على الحوادث وإدارتها، وصيانة الأنظمة والتحكم في النفاذ أو الإدارة.

ويتحقق الأمن في ميدان الاتصالات بواسطة سلسلة من الحواجز (تدابير الحماية) التي ترفع مستوى الصعوبة التي يكون على المهاجمين المحتملين التغلب عليها للنفاذ إلى الموارد. وهي لا تحل مشكلة أمن وإنما تحولها فقط وتنقل المسؤولية عن الأمن إلى كيانات أخرى. وينبغي حماية الحلول الأمنية وتأمينها لكي تثمر مستوى معيناً من الأمن (الطبيعة المعاودة للأمن).

1.2.III تجفير البيانات

تُمكن تقنيات التجفير من الحفاظ على سرية البيانات، والتأكد من سلامة الكيانات والاستيقان منها.

وهناك نوعان من نظام تجفير البيانات: تجفير تناظري (بمفاتيح – خصوصية) وتجفير لا تناظري بمفاتيح عمومية.

توجد خوارزميات تجفير متنوعة. وبغض النظر عن أنها تعمل بأسلوب تناظري أو لا تناظري، فإنها تقوم على استخدام المفاتيح. وبصفة عامة، تتوقف متانتها على القدرة على إدارة مفاتيح التجفير بصورة آمنة، وعلى طول المفتاح

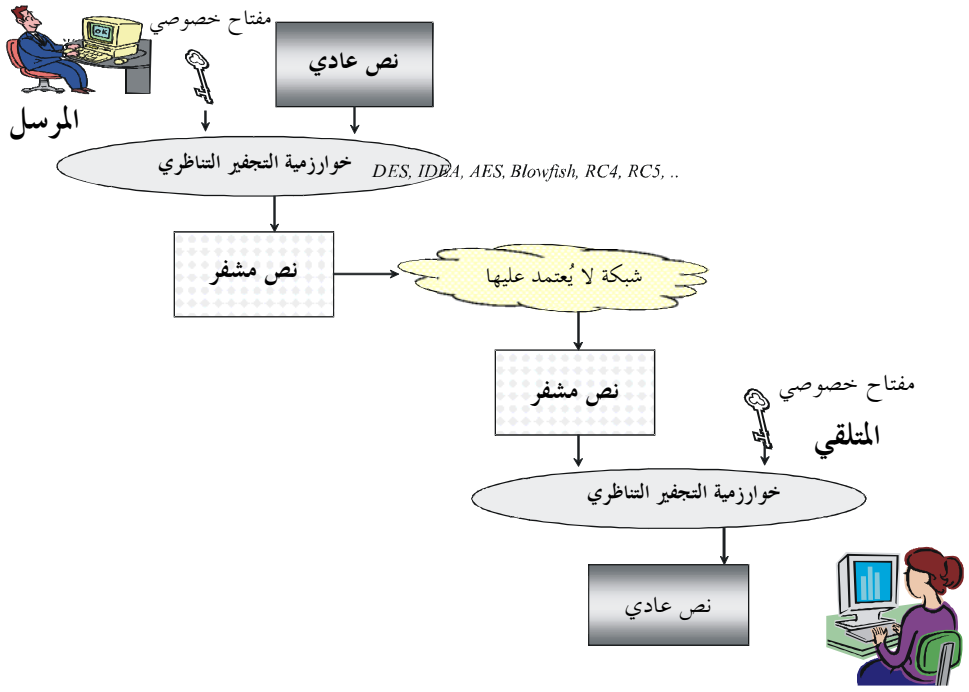
(إذْ يتحدد أدنى طول للمفتاح تبعاً لنوع الخوارزمية) وعلى أمن البرنامج المادي والمنطقي الذي ركبت فيه خوارزميات التجفير وتعمل.

1.1.2.III التجفير التناظري

ولأجل تجفير أو إزالة تجفير نص من النصوص، يحتاج المرء إلى مفتاح وإلى خوارزمية تجفير. فإذا استخدم نفس المفتاح في عمليتين (تجفير وفك التجفير) فيطلق على نطاق التجفير هذا "تناظري"، حيث يكون على المرسل والمتلقي أن يكون لديه، وأن يستخدم نفس المفتاح الخصوصي لجعل البيانات سرية، وليتمكن من فهمها. ويخلق هذا مشكلة إدارة توزيع المفاتيح الخصوصية" (الشكل 5.III).

وخوارزميات التجفير التناظري الرئيسية هي: DES، RC2، وRC5، وIDEA، وAES.

الشكل 5.III – التجفير التناظري



2.1.2.III التجفير اللاتناظري أو العمومي

ينهض نظام التجفير اللاتناظري على أساس استخدام زوج فريد من المفاتيح المتماثلة. وهذا المفتاح الزوجي يشتمل على مفتاح عمومي ومفتاح خصوصي. وتقتصر معرفة العامة على المفتاح العمومي بينما يبقى المفتاح الخصوصي سرياً ويحتَفظ به في سرية.

ويقوم المرسل بتجفير رسالة بالمفتاح العمومي للمستقبل ويفك المستقبل الرسالة بمفتاحه الخصوصي (الشكل 6.III).

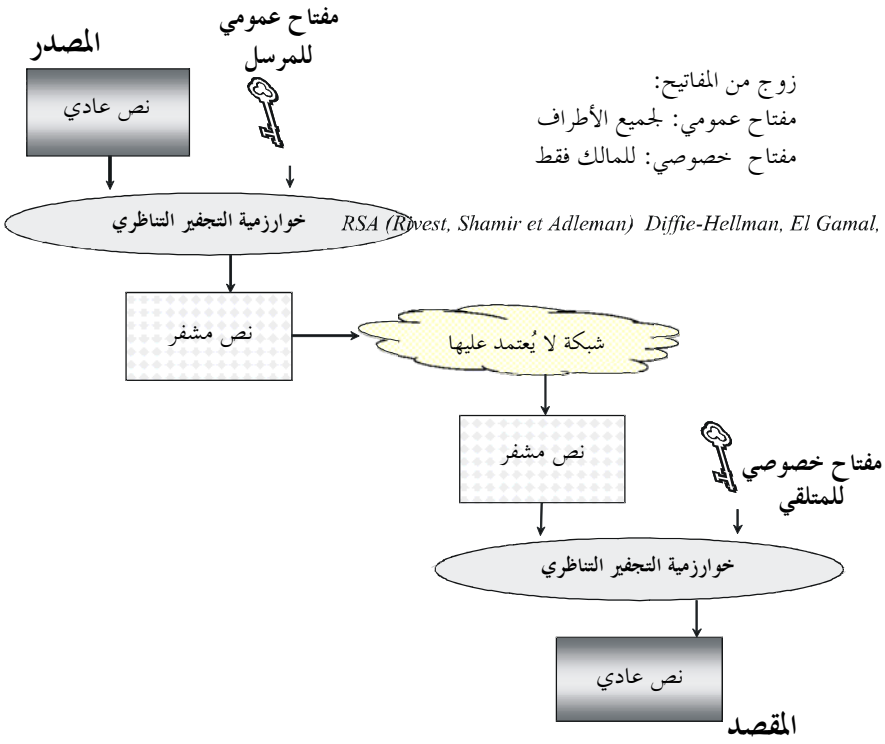
وخوارزميات التجفير بالمفاتيح العمومية الرئيسية، التي أطلق عليها اسم مخترعها، تستخدم عادة مفاتيح تتراوح أطوالها من 512 بتة إلى 1024 بتة، أو في بعض الأحيان 2048 بتة. وهي: RSA[34] (وهي تعني: R. Rivest, A. Shamir, L. Adelman)، Diffie-Hellman[35]، EL.Gamal[36].

3.1.2.III مفاتيح التجفير

يجب أن يحفظ مفتاح التجفير في سرية مضاعفة. وينبغي إدارة أنظمة التجفير بسرية.

وكما سبقت الإشارة، تعتمد سرية عملية التجفير إلى حد بعيد على السرية وعلى طول المفاتيح المستخدمة، وعلى مدى متانة الخوارزميات وأمن عتاد الحاسوب وراءها وعلى البرامج الذكية.

الشكل 6.III – التجفير اللاتناظري



4.1.2.III نظام إدارة المفاتيح

تستخدم البنية التحتية للمفاتيح العمومية PKI لتنفيذ أنظمة التجفير اللاتناظرية. والوظائف الرئيسية التي تدعمها هذه البنية هي:

- توليد زوج من المفاتيح الفريدة (مفتاح خصوصي + مفتاح عمومي)، تخصيص زوج لكيان وتخزين المعلومات الضرورية لإدارتها، حفظ المفاتيح كأضابير. من اتباع تدابير للاستعادة إذا فقد المستخدم مفتاحه أو إذا طلبت السلطات القضائية الإعلان عنه؛

34 "التجفير التطبيقي" سكاينير ب: RSA 1996، الطبقة الثانية.

35 Diffie-Hellman: www.ietf.org/rfc3631.txt

36 الجَمَال: شناير باء "التجفير المنطقي" 1996، الطبعة الثانية 1996.

- إدارة الشهادات الرقمية، إنشاء شهادات تحديد، أو التوقيع عليها أو إصدارها، أو التحقق منها أو إلغاؤها؛
- نشر المفاتيح العمومية إلى الجهات الطالبة، والمرخص لها كذلك؛
- اعتماد المفاتيح العمومية (التوقيع على الشهادات الرقمية).

5.1.2.III الشهادات الرقمية

الشهادة الرقمية هي بطاقة هوية رقمية لكيان (شخص اعتباري أو طبيعي) أو مورد معلوماتي يكون هو موضوع الشهادة. وهي تشمل، إلى جانب أشياء أخرى، هوية صاحب الشأن (حامل الشهادة)، والمفتاح العمومي المخصص لصاحب الشأن وهوية الجهة المُصدِرَة.

ويقدم المعيار X.509 (إطار استيقان الدليل) إطاراً معمارياً لإنشاء خدمة استيقان تستند إلى استخدام الشهادات الرقمية، وتحدد هيكل وقالب أي شهادة رقمية. ويعتمد هذا الهيكل الموحد في الكثير من الحلول المطروحة في السوق (الشكل 7.III).

الشكل 7.III – العناصر الرئيسية لشهادة رقمية X.509v3

النسخة
الرقم التسلسلي
خوارزمية التوقيع
اسم المصُدْر الرقم التسلسلي/زوج الإصدار يجب أن يكونا متطابقين
الصلاحية
اسم الشخص
المفتاح العمومي مع الشخص
معلومات إضافية تتعلق بالشخص أو آليات التجفير
توقيع الشهادة خوارزمية التوقيع والمَعْلمْات والتوقيع الفعلي

وللتصديق على الشهادة التي يحصل عليها العميل، عليه أن يحصل على مفتاح عمومي خاص بالمصدر للشهادة يتعلق بخوارزمية التوقيع. وعند تملك العميل لهذه المعلومات فإنه يحسب القيمة في حقل هاش ويقارنها بالقيمة في الحقل الأخير من الشهادة. فإذا تماثلت القيمتان، يكون قد تم الاستيقان من صحة الشهادة. وبعد ذلك يعمل العميل على جعل مدة الصلاحية للشهادة سليمة.

ومع كون التحكم في النفاذ مستنداً إلى الشهادات الرقمية، فيمكن توصيل عدد كبير من المستخدمين بمخدم معين. ويتم التحكم على أساس المعلومات الواردة في الشهادة الرقمية الخاصة بالعميل. وهكذا يثق المخدم بصلاحية الشهادات وبالطريقة التي صدرت بها، وهو ما يمثل ثُغْرَة في أمن النظام، حيث إن بالإمكان إفساد مخدم شهادة، أو حتى خلق شهادة رقمية مزورة. يضاف إلى ذلك أن مراقبة سلامة أي شهادة ليست أمراً سهلاً. فإلغاء الشهادات مهمة مرهقة وطويلة للغاية نظراً لأن المعلومات يجب عندئذ أن تُرسل إلى جميع الأطراف وتُسَجَل في قائمة إلغاء الشهادات (CRL). ويجب إلغاء أي شهادة بمجرد حدوث أي تغيير في محتواها (مثلاً عندما تصبح المعلومات في الشهادة متقادمة، أو يكون المفتاح الخصوصي للمستخدم قد فسد، أو غادر المستخدم الشركة، أو غير ذلك). إن

المشاورات النظامية لقاعدة البيانات النظيرة تبطئ من التحكم في النفاذ وتقلل من توافر المخدمات، بما في ذلك بالنسبة للمستخدمين المرخص لهم.

6.1.2.III الطرف الثالث الموثوق به

ومهما تكن التسمية – طرف ثالث موثوق به – سلطة تسجيل، سلطة الاعتماد، سلطة إصدار الشهادات – فإن المهمة الرئيسية للهيئة التي تنشئ البنية التحتية للمفاتيح العمومية هي إصدار شهادات تشهد على المفاتيح العمومية المخصصة لكيان ما (شهادة الهوية).

يقدم العميل طلب تسجيل (طلب اعتماد) إلى سلطة تسجيل (خدمة تسجيل قائمة على الشبكة). وقد يطلب مخدم التسجيل دليلاً على هوية العميل طبقاً لتدابير تعريف الهوية والاستيقان المتبعة من جانب تلك السلطة. وبعد إثبات صحة المعلومات، يقوم مخدم الاعتماد بتوليد مفاتيح التجفير، ويصدر شهادة رقمية باسم العميل، ويوقع على الشهادة بمفتاحه الخصوصي (اعتماد الشهادة الرقمية) ثم يرسل الشهادة إلى العميل. ويستخدم العميل مفتاح السلطة العمومي للتحقق من أن الشهادة قد صدرت حقيقة من السلطة المعنية.

وسلطة الاعتماد هي طرف ثالث موثوق به يقوم بإصدار شهادات رقمية ويعمل على التحقق من صحة معلومات معينة.

7.1.2.III عيوب البنى التحتية للمفاتيح العمومية وأوجه قصورها

الحقيقة أن هناك العديد من سلطات الاعتماد تفرض مشاكل من حيث الاعتراف المتبادل بينها، وإمكانيات تشغيلها البيني، وتواؤم الشهادات مع نطاق صحتها. ومع ذلك، فمن غير المرغوب فيه أن يكون لدينا سلطة اعتماد عالمية واحدة فقط. وذلك نظراً للصلاحيات الواسعة والزائدة عن الحد التي تسبغ عليها بحكم الواقع، وبالنظر لضخامة البنية التحتية اللازم إنشاؤها. وهناك نقص حقيقي في الثقة من جانب المستعملين تجاه سلطات الاعتماد هذه التي تكون أجنبية بصفة عامة (صلاحية الشهادات؟ ضمانات أمن؟ حماية البيانات الشخصية؟ إلخ).

أما القصور الكامن في البنى التحتية للمفاتيح العمومية فيكمن في:

- تعقيد البنية التحتية، وتكلفة نشرها وإدارتها؛
- ارتفاع مستوى الأمن اللازم لإنشاء خدمات البنية التحتية للمفاتيح العمومية (PKI)؛
- صحة الشهادات ومدة سريانها وانتهائها.

ومن بين المشاكل المحتملة في تنفيذ PKI ما يلي:

- مشاكل سياسية: فمعظم البنى التحتية للمفاتيح العمومية–سلطات الاعتماد–تنتمي إلى كيانات تابعة للولايات المتحدة الأمريكية. وهذا يثير نقطة الأداء وقضية الثقة بهذه الكيانات من حيث ما يتعلق بالخدمات التي تقدمها (خلق، خزن وتوزيع مفاتيح خصوصية ومفاتيح عمومية، وتحديد البيانات والتوثيق) عدم وجود الضمانات من حيث إمكانية إساءة استعمال البيانات، والحياد في المبادلات، وتوافر جهة للتظلم في حالة وجود نزاع مع سلطة منح الشهادة.
- مشكلة تكنولوجية: يمكن كسر أنظمة التجفير التقليدية ولا تقدم بعض الشهادات الرقمية أماناً أو ضماناً، والتحايل ممكن، ويتم توفير الأمان للبنية التحتية بوسائل أمن تقليدية يمكن التحايل عليها وتفاديها. يضاف إلى ذلك أن استخدام البنية التحتية للمفاتيح يحول مشكلة أمن حركات التبادل دون حلها في الواقع.
- مشكلة تنظيمية: إمكانية التشغيل البيني للبنية التحتية، وتوزيعها، وإدارتها، وصيانتها، وأمنها، ومدى تعقيدها، إلخ.

8.1.2.III التوقيع والاستيقان

يحفر المرسل رسالته بمفتاحه الخصوصي. ويمكن لأي كيان يعرف المفتاح العمومي للمرسل أن يفك تحفير رسالته، وهذا ما يؤكد حقيقة أن الرسالة أنشئت بواسطة المفتاح الخصوصي المُنَاظِرْ.

ويمكن التوقيع على أي وثيقة إلكترونياً (توقيع رقمي) وذلك باستخدام خوارزمية تحفير مفتاح عمومي على النحو التالي:

- خلق رسالة تُشْهِرْ هوية المرسل – التوقيع (مثل "اسمي ألفا تانغو تشارلي") التي يتم تحفيرها بواسطة المفتاح الخصوصي للمرسل وترفق بالرسالة المراد إرسالها؛
- تحفير الرسالة وتوقيعها بالمفتاح العمومي للمتلقي، ثم ترسل؛
- يقوم المتلقي بِفَكْ تحفير الرسالة بواسطة المفتاح العمومي الخاص به ويفصل التوقيع الذي يفسره بواسطة المفتاح العمومي للمرسل.

علينا التحلي بالحرص، مع ذلك، لأن شيئاً لن يمنع أحداً من إعادة استعمال التوقيع الرقمي لرسالة ما بدلاً من المرسل الحقيقي، ومن الممكن أيضاً خلق توقيع رقمي بدلاً من شريك بعد سرقة مفتاحه الخصوصي. ولأجل زيادة مستوى الأمن للتوقيع الرقمي، فإن التوقيع يؤلف من واقع محتوى الرسالة وبذلك يضمن كمال الرسالة والاستيقان من المرسل.

9.1.2.III سلامة البيانات

من الممكن التحقق من أن البيانات لم يتم تغييرها أثناء الإرسال، وذلك بإرسال موجز للرسالة في نفس الوقت الذي ترسل فيه البيانات. ويؤخذ الموجز من دالة "هاش" "hash" تطبق على البيانات. ويقوم المتلقي بإعادة حساب قيمة الـــ"هاش" من واقع البيانات التي تلقاها باستعمال نفس الوظيفة. فإذا ظهر تباين في القيمة المتحصلة، فيمكن استنتاج أن البيانات قد غُيِرتْ. ويمكن للموجز ذاته أن يُجَفَرْ قبل إرسال البيانات و/أو تخزينها.

يمكن لنظامي تجفير المفاتيح التناظري واللاتناظري أن يحددا ما إذا كانت البيانات قد غُيِرَت، لأنه يصبح عندئذ من المستحيل فك تجفيرها. وهذا يساعد على التحقق من سلامة واكتمال البيانات وإن كَان غير قادر على إثبات أن البيانات لم تدمر بالكامل.

ولتحصيل قدر من السلامة أكثر فعالية، فيتم تطبيق دالة على الرسالة الأصلية تقوم بتحويلها إلى تتابع قصير وعشوائي من البتات، مكونة بصمة رقمية ما (الموجز).

ثمة دالة "هاش" ذات اتجاه واحد تولد موجزاً للرسالة، أي، بصمتها الرقمية والتي هي أقصر من الرسالة الأصلية وغير مفهومة وبعد ذلك يتم تجفيرها بواسطة المفتاح الخصوصي للمرسل وترفق بالرسالة المراد إرسالها. وعند تسلم الرسالة وبصمتها، يقوم المتلقي بإزالة تجفير البصمة بواسطة المفتاح العمومي للمُرسل، ثم يعيد حساب البصمة من الرسالة المرسلة باستخدام نفس "دالة الهاش"، ثم يقارنها بالبصمة الواردة. فإذا كانت النتيجة واحدة، يكون المتلقي قد تحقق من صحة هوية المرسل وتأكد من سلامة الرسالة، حيث إنه، إذا كانت الرسالة قد تم تغييرها ولو بقدر ضئيل، فإن بصمتها تتعدل بدرجة كبيرة.

يمكن باستعمال مزيج من تقنيات التجفير، والتوقيع والبصمة الرقمية، وضع علامات على الرسائل لضمان سلامة البيانات. وتَستهلِكْ هذه التدابير وقتاً كبيراً من جانب المعالج processor وتبطئ كثيراً من أداء البيئة التشغيلية.

10.1.2.III منع–الرفض

خدمة منع الرفض مُصَمَمة لمنع الرفض أو الإنكار أن رسالة قد أرسلت أو وردت، أو أن عملاً أو تعاملاً قد تم. وتجعل بالإمكان البرهنة مثلاً على أن كياناً ما مرتبط بعمل معين أو حادث بعينه.

ويقوم عدم الرفض على توقيع وحيد، أو على تحديد هوية تثبت هوية من أنشأ الرسالة. ويمكن تقديم هذه الخدمة بواسطة خوارزمية تجفير للمفاتيح العمومية. ويمكن الاستعانة أيضاً بطرف ثالث محل ثقة ليقوم بعمل المُوثِّقْ السيبراني.

11.1.2..III أوجه قصور الحلول الأمنية القائمة على التجفير

يمكن للثقة بالحلول التجفيرية في السوق أن تكون نسبية فقط حيث لا توجد ضمانات أو وسائل تحقق (وجود أبواب خلفية في البرمجيات؟ استنساخ المفاتيح السرية، الإعلان عنها، إلخ؟). كذلك لا يوجد دليل على أن الخوارزميات التي يُظَنُّ حالياً أنها يعتمد عليها ستستمر كذلك في المستقبل القريب.

2.2.III بروتوكول إنترنت آمن

جاءت الحاجة إلى تلبية الاحتياجات الأمنية لصالح تنقيح النسخة 4 من بروتوكول الإنترنت. يضاف إلى ذلك أن هناك حاجة إلى النهوض بأعباء طائفة أوسع من العناوين وزيادة عدد عناوين الإنترنت المتاحة، وكذلك السماح للتخصيص الديناميي لعرض النطاق يدعم التطبيقات متعددة الوسائط. وكان من نتيجة ذلك صدور نسخة منقحة من بروتوكول الإنترنت (IP protocol) يسمى "الجيل التالي من بروتوكول الإنترنت" (IPnG) أو النسخة 6 من البروتوكول (IPv6)[37].

1.2.2.III النسخة 6 من بروتوكول الإنترنت (IPv6)

في عام 1994[38] تناول مجلس نشاط الإنترنت (IAB)[39] متطلبات أمن بروتوكول الإنترنت. وتشتمل النسخة 6 من بروتوكول الإنترنت (IPv6) على خدمات استيقان وسرية.

وتتعلق أهم التطورات في النسخة 6 من بروتوكول الإنترنت مقارنة بالنسخة 6 من نفس البروتوكول بالنقاط التالية [RFC 2460]:

- اتساع مساحة العناوين والشكل الهرمي للعناوين: فازداد حجم العنوان إلى 128 بتة (16 أثمون) ومن 32 بتة إلى (4 أثمونات)، وكانت العناوين تقدم على هيئة أرقام ستة عشرية hexadecimal[40]، تفصل علامة النقطتين فيها بين كل زوج من الأثمونات (مثال. 0123:4567:89ab:cdef: 0123:4567:89ab:cdef)، بدلاً من وضع علامات عشرية؛
- إمكانية التخصيص الديناميي لعرض النطاق لدعم التطبيقات متعددة الوسائط؛
- القدرة على خلق شبكات افتراضية بروتوكول الإنترنت؛
- دعم تدابير الاستيقان والتجفير باستخدام رأسيات الخيارات؛
- تبسيط رأسيات الرزم لتيسير التسيير وزيادة سرعته.

إن اتباع النسخة 6 من بروتوكول الإنترنت تدعو إلى أمور من بينها تعديل العنونة آلية إدارة العناوين[41]، وإقامة أنظمة داخل بيئة الإنترنت لدعم أنظمة النسخة 6 من البروتوكول التي تعمل بكلتا النسختين، ضبط تزامن هجرة النُسَخْ واسعة النطاق، إلخ.

---

37 IPv6: RFC 1883 in 1995, replaced in December 1998 by RFC 2460-www.ietf.org/rfc/rfc2460.txt

38 RFC 1636: Report of IAB Workshop on Security in the Internet Architecture, 8-10February 1994

39 www.iab.org/

40 الفبائية نظام الترقيم الست عشر (base16): 0 1 2 3 4 5 6 7 8 9 A B C D E F.

41 RFC 1886 تم تحديده في 1995، وسوف تدخل التعديلات في مخدمات اسم الميدان لدعم النسخة 6 من بروتوكول الإنترنت.

ولهذه الأسباب مجتمعة، لم يتم بعد تركيب النسخة 6 التي تم تحديدها في عام 1995، على نطاق واسع، كما يبدو أنه لا يوجد حافز حكومي أو توصية دولية قادرة على فرض الأخذ بالنسخة 6 من البروتوكول في جميع أنحاء الشبكة. وهناك عدد قليل فقط من البنى التحتية هي التي أدرجت النسخة 6 من البروتوكول IPv6.

إن تنفيذ النسخة الجديدة المُبَيَّتَة من بروتوكول الإنترنت (IPv6) بما لها من وظائف أمنية أمر غير عادي. ولهذا فإنه للوفاء باحتياجات أمن الشبكة، تم تطوير حل وسيط يسمى أمن بروتوكول الإنترنت IPSec[42]، متوائم مع كل من النسخة 6 والنسخة 4 من بروتوكول الإنترنت واتبعته جماعة الإنترنت. وقد أصدر فريق مهام هندسة الإنترنت (IETF)[43] عدة وثائق في 1995 (RFC 1825 to 1829) يحدد طرق لتأمين البنية التحتية للإنترنت.

2.2.2.III أمن بروتوكول الإنترنت IPSec

يمكن عن طريق أمن بروتوكول الإنترنت (IPSec)، جعل نقل الرزم بواسطة البروتوكول سرية. ويوفر بروتوكول IPSec سرية البيانات وخدمات الاستيقان على مستوى النقل بواسطة بروتوكولات الإنترنت وذلك عن طريق إدخال رأسية الاستيقان أو كبسلة رأسية لأمن الحمولة النافعة.

ويمكن لكل تطبيق، بغض النظر عن نوع الحركة التي يولدها، أن يستخدم خدمات الأمن هذه بدون أي تعديل. ويعمل بروتوكول IPSec بأسلوب نقطة – نقطة (وتكون البيانات مؤمَّنة بين المرسل والمتلقي عبر علاقة مأمونة بينهما).

وتوفر رأسية الاستيقان خدمات الاستيقان وخدمات السلامة لرزمة بروتوكول الإنترنت، ومن ثم تضمن ألا تكون البيانات قد تعرضت لتغيير أثناء الإرسال، وأن عنوان المَصْدَرْ هو في الحقيقة العنوان الذي يظهر على الرزمة.

وتسمح كبسلة رأسية أمن الحمولة النافعة بتنفيذ آليات التجفير (التجفير التناظري مثل DES، Triple DES، RC5 أو IDEA) كما توفر خدمات استيقان مماثله لتلك الخدمات التي توفرها رأسية الاستيقان.

تستخدم خوارزمية التجفير مفاتيح ينبغي توليدها ونشرها، وهكذا فإن إدارة مفاتيح التجفير مهمة هامة ينبغي القيام بها عند تنفيذ الحلول على بروتوكول IPSec وتشمل بروتوكولات تبادل المفاتيح، مثلاً: بروتوكول[44] تحديد مفتاح Oakley الذي يقوم على أساس خوارزمية تبادل Diffie-Hellman [RFC 2412]؛ إن رابطة أمن الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) [RFC 2408]، وتبادل مفاتيح الإنترنت (IKE) [RFC 2409].

3.2.2.III الشبكات الخاصة الافتراضية

وبتركيب بروتوكول IPSec عند نقاط النفاذ لشبكة الإنترنت، يكون من الممكن إنشاء قناة اتصال بين تلك النقاط يتم الاستيقان من نهاياتها (الشكل 8.III).

تقع هذه النهايات داخل أنظمة المنظمة، ومن ثم فهي محمية من الناحية المادية. وطبقاً للخيار المتبع، يجوز تجفير البيانات التي يتم نقلها على هذه الوصلة. وبعبارة أخرى، يمكن إنشاء طريق آمن بين نقطتين تابعتين لبنية تحتية غير مضمونة (وهذا هو مفهوم الشبكة الخاصة الافتراضية). ويجب ملاحظة أن مصطلح "شبكة" في التعبير "شبكة خاصة افتراضية" هي تسمية خاطئة إلى حد ما حيث إن ما يتم إنشاؤه هو اتصال افتراضي منطقي فقط.

3.2.III أمن التطبيقات

لمعظم التطبيقات نسخة آمنة، تسمح عامة بالاستيقان من المراسلين وتجفير البيانات المرسلة.

---

42 RFC 2401 - www.ietf.org/rfc/rfc2401.txt

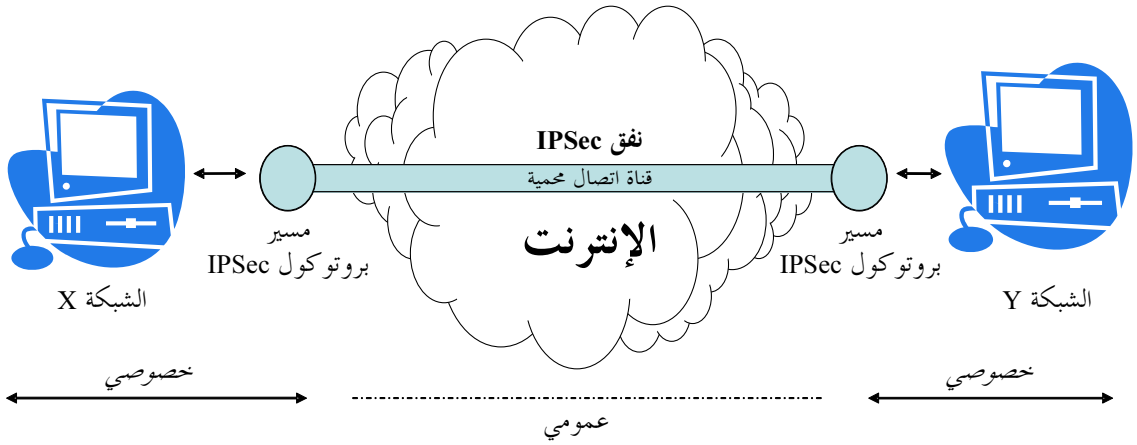
43 www.ietf.org

44 بروتوكول تحديد مفاتيح أوكلي: RFC 2412-www.ietf.org/rfc/rfc2412.txt

والبديل لتركيب نسخات جديدة آمنة من بروتوكولات التطبيق هو إنشاء آلية أمن مشتركة توفر خدمات أمن تنوعية لجميع التطبيقات. وتستخدم برمجيات طبقة المقابس الآمنة (SSL) على نطاق واسع، وبخاصة في العمليات التجارية على الإنترنت.

إن استخدام وثائق النص الفوقي نطاق واسع وكذلك تنـــزيل المحتوى، سواء كان إيجابياً أو سلبياً، يشكل العديد من مشاكل الأمن المتعلقة بأمور من بينها: المصدر، المؤلف، اليقين، الضرر، إلخ. وبدأت تظهر بعض الاستجابات لهذا البعد الجديد من أبعاد أمن نظام المعلومات: تقنيات للتوقيع على وثائق XML، وطبع الرسوم، وإدارة الحقوق الإلكترونية لاستحداث الاستقرار من الناحية الأمنية. ويجب أن يكون في الإمكان المحافظة على مستوى معين من الأمن حتى ولو وقع الهدف المراد تأمينه خارج الحدود المادية للبيئة التي يتم فيها الأمن عادة.

الشكل 8.III – إنشاء شبكة افتراضية خاصة (VPN) استخدام قناة اتصال IPSce



4.2.III طبقة المقابس الآمنة SSL وبروتوكولات نقل النص الفوقي HTTP (S-HTTP)

طبقة المقابس الآمنة (SSL) هي إحدى البرمجيات التي تضمن أمن مبادلات التطبيق. وهي تلقى الدعم من جانب معظم برامج تصفح الويب في السوق.

ويتم الاستيقان من الكيانَيْن المتواصلَيْن في وصلة SSL عن طريق الاعتماد وطرف ثالث محل ثقة. ثم تقوم هذه الجهات بالتفاوض على مستوى الأمن الذي ينبغي تطبيقه على نقل البيانات. ويتم تجفير البيانات المرسلة لأجل إتمام الاتصال بـــ SSL (الشكل 9.III).

وتركيب SSL له تأثير المخدم (server) وذلك بسبب الاعتماد المطلوب الذي يحتم إجراء حوار مع سلطة معترف بها للشهادات، كما يحتاج إلى أن يؤدي تطبيق حائط النيران (firewall) إلى دعم أسلوب تشغيل SSL. ويعتبر الاعتماد في بعض الأحيان عقبة في طريق نشر هذا الحل.

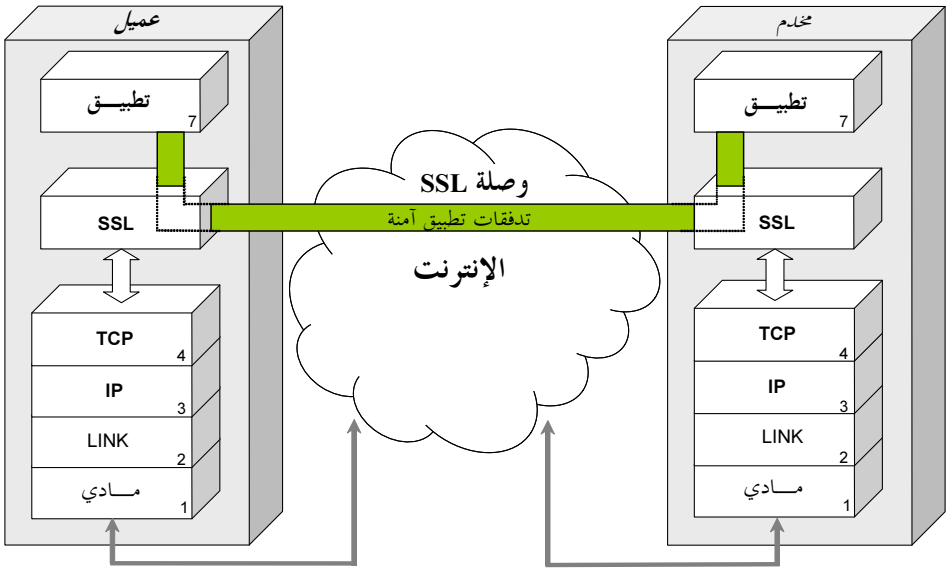
إن التمديد لبروتوكول نقل النص الفوقي الآمن HTTP (S-HTTP، HTTP) هو الحل البديل الذي طورته رابطة شركة التجارة (Commerce Net association) والذي تنطبق عليه نفس قيود الاعتماد، وعلى الرغم من أنه يدعم فقط تدفقات بيانات HTTP. وهذا الحل ليس مقبولاً ومعتمداً على نطاق واسع.

5.2.III البريد الإلكتروني وأمن مخدم الاسم

وتتعلق مخاطر الأمن التي تظهر في استخدام نظام البريد الإلكتروني بـــ:

- فقدان الرسائل، أو اعتراض طريقها، أو تبديلها أو تدميرها؛
- إصابة الأنظمة بالعدوى عن طريق رسائل تحمل فيروسات، ديدان أو أحصنة طروادة؛
- الإزعاج: القصف بالرسائل، والبريد الغث، والرسائل الاقتحامية، التي تصيب الأفراد الذين يُستَعمَل بريدهم الإلكتروني بدون موافقة مسبقة منهم، والذين لم يسبق لمرسل الرسائل الاقتحامية أن كان على اتصال بهم. إن إرسال الرسائل الاقتحامية الذي ينطوي على التوزيع واسع النطاق لرسائل حاملة للعدوى قد يُسهم في التكاثر السريع للفيروسات (رسائل اقتحامية + فيروس)، حيث تكون محركات البريد الإلكتروني محفورة في شفرة الفيروس بحيث تحدث تكاثراً ذاتياً؛
- سرقة الهوية (حيث يتظاهر المقتحم بأنه شخص آخر، بينما يقوم مُكَوِنْ من النظام بالإرسال، والاستماع إلى، أو اعتراض رسائل ليست موجهة إليه، إلخ)؛
- قد يتم دَسْ الرسائل، أو مزجها أو شطبها أو تأخيرها؛
- قد ترفض الخدمة بسبب أحد المكونات الفاسدة في سلسلة نظام الرسالة؛
- إفشاء معلومات سرية؛
- التنصل (حيث ينكر طرف في النظام أنه أرسل أو تلقى رسالة ما).

الشكل 9.III – معمار الطبقة SSL *(طبقة المقابس الآمنة)*



ويجب أن يضاف إلى ذلك أيضاً جميع التهديدات المرتبطة بالشبكات وبتشغيلها (هجمات على مستوى التسيير، مخدمات الأسماء، إلخ).

وللتعويض عن أوجه القصور الأمني هذه الكامنة في الطريقة التي يعمل بها البريد الإلكتروني، فإن النُسَخْ الجديدة من البرمجيات تضم قدرات التجفير لأجل ضمان السرية، والسلامة وموثوقية المعلومات المتبادلة والمراسلين.

وتتعلق متطلبات الأمن لأنظمة البريد الإلكتروني بـــ:

- سرية وسلامة (رسالة أو سلسلة من الرسائل)؛
- عدم التنصل (برهان على الإرسال، برهان على التلقي، التوقيع، اعتماد الرسالة)؛
- الاستيقان من هويات جميع الأطراف في نظام البريد الإلكتروني (المستخدمون العناصر الوسيطة، ذاكرة الرسائل، عملاء نقل الرسائل، إلخ).

وربما كان أعظم المخاطر هو إقحام فيروس أو دودة أو حصان طروادة من خلال رسالة. ومن بين طرق المنع تركيب برنامجية مكافحة الفيروسات في كل نظام وذلك من أجل اكتشاف الفيروسات، بل القضاء على عدواها إن أمكن. ويقوم برنامج مكافحة الفيروس باستكشاف تلك الفيروسات لأنه صُمِمَ من أجل اكتشافها فقط، ولكنه لا يوفر حماية من أشكال الإصابة الجديدة، أو ما يستلحقه ذلك من عمليات تحديث متواصلة فيتطلب جهداً إدارياً لا يستهان به.

وثمة إمكانية أخرى هي إنشاء مخدم حَجْرْ يقوم بالفحص الصارم لكل رسالة واردة مع جميع مرفقاتها. وباستخدام العديد من برامج مكافحة الفيروسات التي تعمل بالتوازي، تزداد فرص الإمساك برسالة مصابة بالعدوى.

تم تنقيح البروتوكول الأصلي المستخدم في البريد الإلكتروني على الإنترنت الذي يعرف باسم "بروتوكول نقل البريد البسيط" (SMTP) مع مرور الوقت ليس فقط من أجل تدعيم محتوى الرسالة متعددة الأغراض، ولكن أيضاً تدعيم آليات الآمن. ومن بين الأمثلة على هذه البروتوكولات تمديدات البريد متعدد الأغراض الآمن على الإنترنت (S/MIME) والبريد مُعَزَز السرية، والخصوصية الممتازة).

وتعتمد تطبيقات الإنترنت كافة، مباشرة أو بطريقة غير مباشرة، على عمل جهات مخدم اسم الميدان (DNS) حيث تقوم مخدمات أسماء الميادين بالربط بين الأسماء المنطقية وبينها وبين الإنترنت النظيرة. وتنهض مخدمات أسماء الميادين بدور رئيسي في تأمين تسيير المعلومات بصورة صحيحة. ولهذا السبب كانت من بين المكونات الحساسة بصفة خاصة في معمار الاتصال، وتتطلب وقاية إضافية. وتقام آليات الأمن (التحكم بالنفاذ، الاستيقان، التسجيل، التضاعف، المطابقة، تجفير الطلب والرد، إلخ) لمنع التلاعب بالمعلومات المخزنة على المخدمات بنية الانحراف بالمعلومات إلى مُتَلقِين غير مقصودين، وشن هجمات إنكار الخدمة، والتسبب في التحميل الزائد للمخدم أو انهيار الشبكة نتيجة لإغراقها بفيضان من الطلبات الزائفة، ومخدمات الأسماء غير الحقيقية التي تُسَجَل للحصول على ردود غير صحيحة مما يُحْدِثْ أخطاء في الإرسال، أو يؤدي إلى الاقتحام.

6.2.III كشف الاقتحام

يجب الكشف عن حوادث الاقتحام، والحوادث، والشذوذ عن القاعدة، في أسرع وقت ممكن عقب حدوثها والتعامل معها بصرامة وذلك لضمان استمرار تأدية الأنظمة المعينة لوظائفها دون ارتباك مع بقائها محمية.

والحادث هو واقعة تقع على غير توقع. ومع أن الحوادث، في الجانب الأكبر منها، ليست خطيرة في حد ذاتها إلا أنها يمكن أن تترتب عليها نتائج قاسية. أما الشذوذ عن القاعدة فهو حدث استثنائي يمكن أن يُسفْر عن أداء غير قياسي لنظام المعلومات، وإلى خرق سياسة الأمن العامة المعمول بها. وقد تكون أسبابه عَرَضِيَة (كخطأ في التشكيل مثلاً) أو متُعَمَدة (هجوم موجه إلى نظام المعلومات). والاقتحام من سمات الهجوم ويجوز اعتباره حادثة أو شذوذاً عن المألوف.

ويشير كشف الاقتحام إلى مجموعة الممارسات والآليات التي تستخدم لكشف الأخطاء التي قد تؤدي إلى خرق سياسات الأمن العامة، وإلى تشخيص حالات الاقتحام والهجمات (وتشمل كشف الشذوذ عن القاعدة وإساءة الاستخدام)[45].

يتألف نظام كشف الاقتحام من ثلاث كتلات وظيفية ألا وهي جمع البيانات، تحليل البيانات وكشف الاقتحام والرد.

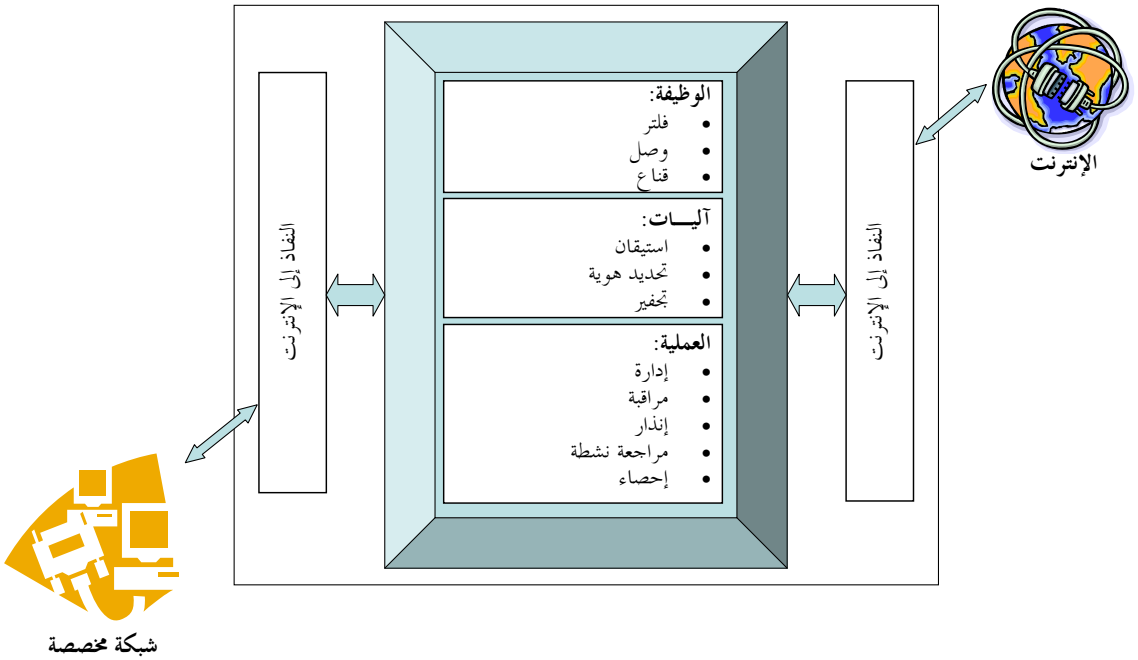
[45] اليساندري، د. وغيره "نحو تصنيف للهجمات ونظم لكشف الاقتحام" العملية
www.domino.watson.ibm.com/library/cyberdig.nsf/papers/5FA980EB952E09D085256AC600535997/$File/rz3366.pdf

7.2.III تجزئة البيئة

وإن فصل وتقنيع البيئة الخصوصية تجاه الإنترنت العمومية عن طريق تركيب نظام أو أكثر من أنظمة الحوائط النارية.

وجدار النار هذا هو جهاز للفلترة، وهو كما تَستَدعي الحالة، يقوم بسد الطريق أمام تدفقات البيانات. فهو يحلل الدفقة، فيجيز لها المرور إذا استوفت شروطاً معينة، وإلا، رفضها. وبتقسيم الشبكة يمكن للمرء أن يفصل بين بيئات بروتوكول مونتريال وذلك بجعل نقاط النفاذ في الشبكات التي من المرغوب فصلها مستقلة عن بعضها البعض. الأمر الذي يسمح بالتوصيل البيني لشبكتين لديهما مستويان أمن مختلفان. (الشكل 10.III) [46].

الشكل 10.III – التنظيم الوظيفي لحائط نيران



هناك أنواع مختلفة من حوائط النيران وذلك طبقاً لطبيعة التحليل والمعالجة التي ستتم. وهي توضع في فئات تبعاً لمستوى فلترة البيانات المقدمة: الطبقة 3 (IP) الطبقة 4 (TCP، UDP) أو الطبقة 7 (FTP، HTTP، إلخ) لنموذج معمار التوصيل البيني (OSI).

ويعمل حائط النيران التطبيقي، الذي يُعَرف أيضاً بالوكيل (مخدم بالوكالة، حائط نيران بالوكالة)، كترحيل للتطبيق. فهو من خلال عمله نيابة عن المستخدم يقدم الخدمة المطلوبة. والغرض من نظام الوكالة المشروط هو توفير التقنيع للعنوان بواسطة مُرَحِل التطبيق، وأن يعطي شفافية للبيئة الداخلية للمنظمة. والمقصود منه أن يكون بمثابة نقطة عبور إلزامية لجميع التطبيقات المحتاجة إلى نفاذ إلى الإنترنت، كما يدعو إلى تطبيق ترحيلي على محطة عمل المستخدم وعلى حائط النيران.

إن تركيب وتشكيل حائط نيران يعتمدان على معمار الشبكة المختار للوفاء باحتياجات الأمن والتحكم عند الربط بين أنظمة مختلفة.

[46] هذا الشكل مأخوذ من "أمن المعلومات والاتصالات: مقرر وتدريبات مصوبة" (*Sécurité informatique et télécoms: cours et exercices corrigés*) غرناؤطي–هيلي، دنود 2006.

يمثل حائط النيران إحدى الأدوات المستخدمة في تنفيذ السياسة العامة للأمن وإحدى مكونات عتاد الكمبيوتر والبرمجيات المستخدمة في هذا الغرض، حيث إن حائط النيران في حد ذاته لا يكفي لتوفير حماية كافية لشبكة منظمة ولأنظمتها. بل يجب أن تسانده أدوات وإجراءات وتدابير متمشية مع أهداف الأمن المُعَرَّفة طبقاً للسياسة العامة للأمن. وتعتمد فعالية أي حائط نيران أساساً على اختيار موقعه من الأنظمة التي سيقوم بحمايتها، وعلى تشكيله وإدارته.

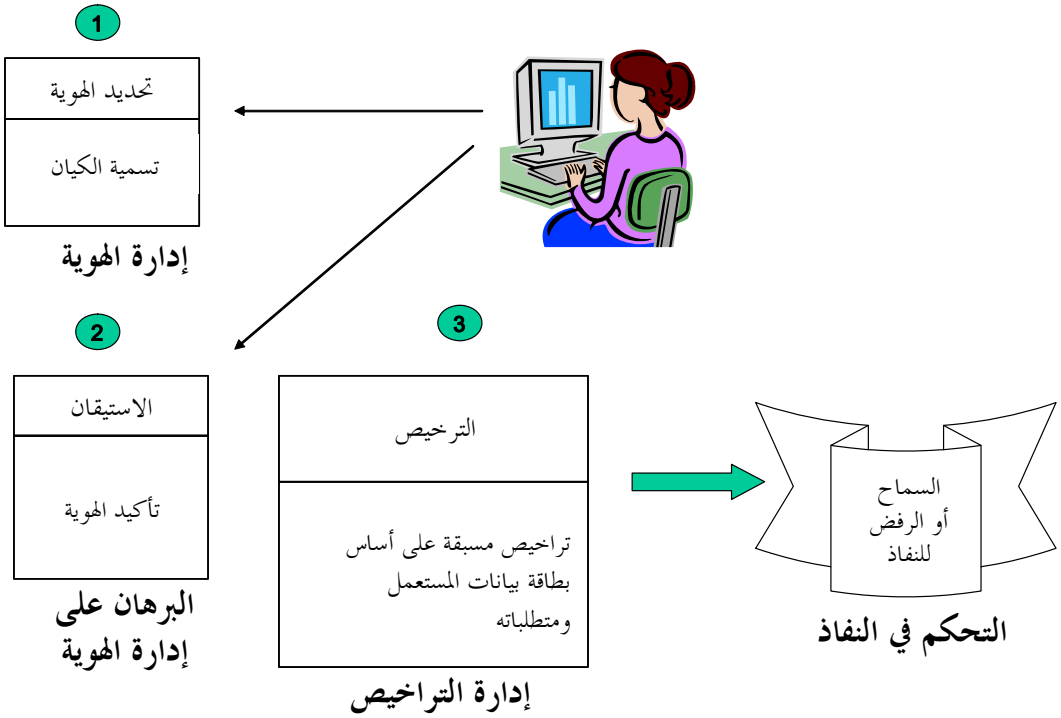
وعلى الرغم من أن حائط النيران وأنظمة كشف الاقتحام قادرة على أداء خدمات أمنية معينة، فإنها في حد ذاتها كافية لضمان حماية كاملة لموارد المعلومات.

8.2.III التحكم في النفاذ

1.8.2.III مبادئ عامة

تقوم آلية التحكم في النفاذ المنطقي، المستندة إلى تحديد هوية الأفراد والاستيقان منهم، وإلى التصاريح أو حقوق النفاذ الممنوحة لهم، بالحد من النفاذ إلى موارد المعلومات (الشكل 11.III).

الشكل 11.III – المكونات الأساسية للتحكم المنطقي في النفاذ



وعلى أساس تحديد الهوية مستيقن منه، تسمح آلية التحكم في النفاذ، طبقاً لبطاقة بيانات المستخدم، بالنفاذ إلى الموارد المطلوبة. وهذا يفترض مستقبلاً أن إدارة الهوية، وإدارة الأدلة على الهوية، وإدارة الترخيص قد تمت على أساس سليم تجاه المستخدم.

وتحتوي بطاقة بيانات المستخدم (user profile) على جميع البيانات التي استندت إليها قرارات الترخيص بالنفاذ. وينبغي تعريفها بعناية طبقاً للسياسات العامة لإدارة النفاذ.

والغرض من الاستيقان هو الربط بين فكرة الهوية وبين شخص معين. والترخيص بالنفاذ يستتبع فلترة انتقائية لطلبات النفاذ إلى الموارد والخدمات التي توفرها الشبكة بحيث يمنح هذا النفاذ فقط إلى الكيانات المخول لها ذلك.

والغرض من خدمة الاستيقان هو التأكد من أن الهوية الحقيقية (دليل الهوية). ويعتمد ذلك بصفة عامة على واحد أو أكثر من العوامل التالية:

- سِرْ معروف للكيان المعني، أي كلمة المرور أو رقم شخصي لتحديد الهوية (PIN)؛
- بند موجود في حوزة الكيان (كبطاقة أو رمز، إلخ)؛
- خاصية فريدة للكيان (كبصمة إصبع، بصمة صوت، بصمة شبكية عين، إلخ)؛

تسير عملية التحقق من الهوية وفقاً لسيناريو يقضي بأن يذكر طالب النفاذ هويته ويقدم بنداً من دليل من المفترض أنه هو وحده الذي يعرفه (مثل كلمة مرور مفتاح سري، أو بصمة أصبع). ثم تقوم خدمة الاستيقان عندئذ بمقارنة تلك المعلومات بالبيانات المخزونة في مخدم الاستيقان الخاص بها.

يجب أن يكون مخدم الاستيقان محمياً جيداً إلى أبعد حد ومُؤَمَنْ بآليات مخصصة توفر التحكم في النفاذ وإدارة الأنظمة الآمنة، وذلك بواسطة تجفير البيانات التي تشتمل عليها. ويجب ألا يكون مخدم الاستيقان معرضاً، أو عرضة للأخطاء، نظراً لأن الأمن العام للبنية التحتية للمعلومات والاتصالات تعتمد على متانته.

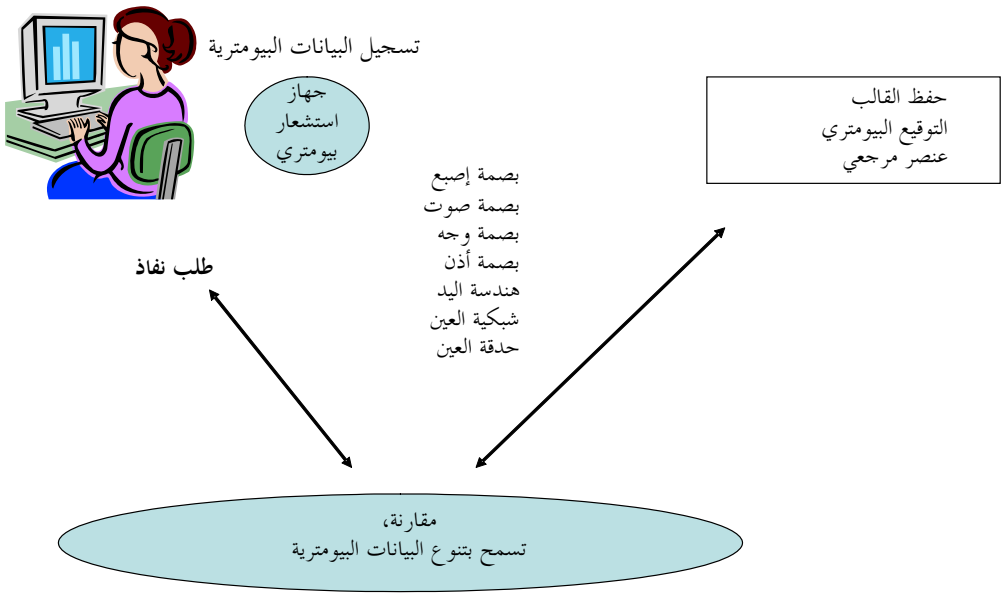
2.8.2.III مساهمات وأوجه قصور التقييس الحيوي (البيومتري)

يتكون التخصيص الإفرادي من استخدام بيانات التقييس الحيوي للتأكد من هويات الأفراد عند نقطة النفاذ إلى نطاق أو داخل إطار الإشراف القضائي (بواسطة الشرطة، إلخ).

من الممكن باستخدام التقييس الحيوي للتحكم في النفاذ إلى موارد المعلومات الاستغناء عن كلمة المرور، واستبدالها بخاصية مادية يمكن استخلاص قيمة بيانات اثنينية (binary data) منها بسهولة.

ولكي يمكن استخدام الخصائص المادية للأفراد لأجل تحديد هويتهم والتحقق من صحة هوياتهم، يكون من الضروري أولاً استخلاص وتسجيل خصائصهم التقييسية الحيوية في شكل "قالب تقييس حيوي". ويجب لمثل هذه السجلات أن تكون عالية الاعتمادية ومخزونة بأمان. (الشكل 12.III).

الشكل 12.III – مراقبة النفاذ البيومتري



إن الوقت اللازم لإتمام عملية الاستيقان قد يكون طويلاً، حيث إن مرحلة المقارنة يجب أن تراعي التنوعات الكامنة في الطبيعة الحية للبيانات محل المقارنة. فمثلاً لن تكون عينة الصوت متماثلة تماماً. فالمقارنة تقوم على المعالجة الإحصائية

والاحتمالية للبيانات البيومترية. فالضبابية الموجودة في نظام الاستيقان تعني عدم إمكانية اليقين الكامل من نتيجة الاستيقان، أي أن هذا النظام غير قادر على التحديد بيقين نسبته مائة في المائة أن الشخص "X" هو الشخص – ذكراً أو أنثى – الذي يدعي أنه هو فلا يزال معدل الخطأ في مثل هذه الأنظمة عالياً، مما يجعل من المستحيل ضمان مستوى عالٍ من الأمن. فعند إضافة آليات الاستيقان "التقليدية" التي تعتمد على كلمات المرور (التحقق الثنائي) فإن الجانب البيومتري يعمل على زيادة مستوى الأمن المقدم.

إن التوسع في استخدام التكنولوجيا البيومترية يثير العديد من القضايا ذات الطابع الأخلاقي والمتعلقة بكفاءة الأشخاص في بيئة العمل، ergonomic، ناهيك عن الطابع الاقتصادي والقانوني والتكنولوجي. وتشمل مثل هذه القضايا:

- سرية البيانات البيومترية (الإحصائية الحيوية) التي قد تعتبر خصوصية؛
- الحالات التي قد لا تكون البيانات البيومترية فريدة (التوائم المتطابقة)؛
- حقيقة أن أجهزة استشعار البيانات البيومترية يُنظَر إليها غالباً على إنها اقتحامية، ومرفوضة من جانب أغلبية المستخدمين في الحالات الاختيارية. وهي تمثل أيضاً تهديداً لحرية الفرد، مثل عدد كبير من أجهزة الاستشعار مثل كاميرات الفيديو التي تُنْصَب في أماكن عامة وتعمل بدون علم الناس؛
- حالات سرقة الهوية أو الاستخدام غير اللائق أو التحايلي للبيانات البيومترية.

ونظراً لعدم الدقة والتكاليف المستمرة للشراء والتوزيع والتشغيل، فإن حلول التحكم المستندة إلى البيانات الإحصائية الحيوية (البيومترية) لا تلقى إقبالاً كبيراً.

موجز العقبات التي ظهرت أثناء استخدام البيانات الإحصائية الحيوية (البيومترية) للتحكم في النفاذ.

1 إن البيانات البيومترية المستخدمة في تحديد هوية فرد ما تتفاوت مع مرور الوقت.

2 إن البيانات البيومترية يجب الإمساك بها وتحويلها إلى عينة مرجعية للتخزين في قاعدة بيانات. وأثناء رقمنة البيانات تصبح هشة (ومن ثم قابلة للتعديل) فيجب إيلاؤها أفضل حماية ممكنة. وبالنسبة لكل طلب نفاذ يجب الإمساك بالبيانات البيومترية للمستخدم، وهذا يثير مشكلة قبول طريقة الإمساك بالبيانات والإحساس المصاحب بالاقتحام الذي لا يلقى ترحيباً في الكثير من الحالات.

3 إن التحكم في النفاذ بالاستناد إلى البيانات البيومترية ليس مضموناً مائة بالمائة وذلك بسبب تنوع العينة البشرية المقرر تحليلها أثناء عملية الاستيقان. وطبقاً للنظام المستخدم، يكون احتمال تحديد الهوية بصورة زائفة إيجابياً أو سلبياً مرتفعة نسبياً ويعتمد على التكنولوجيا المستخدمة في تسجيل البيانات الإحصائية الحيوية (البيومترية) ونوعية التشغيل.

9.2.III حماية وإدارة البنى التحتية للاتصالات

1.9.2.III الحماية

يمكن للطبقة المادية (الطبقة 1) أن تسهم في أمن عمليات الإرسال وذلك بإصدارها التخليط على الخط، أي إرسال معلومات غير مهمة لكي تُقنِّعْ تدفق المعلومات المهمة داخل تدفق غير منقطع من البيانات الغثة. غير أنه في الحالات التي يلزم فيها حماية عمليات الإرسال من التنصت السلبي عبر الإمساك بالإشعاع الكهرمغنطيسي المستحث بواسطة إشارة محمولة عبر وسائط الإرسال، فإن الأخيرة هذه ينبغي عزلها بصورة كاملة داخل أقفاص فاراداى "Faraday cages". وواضح أن تدبير الحماية هذا ينفذ في حالة الضرورة القصوى.

وينبغي إنشاء وصيانة الأمن المادي لوسائط الإرسال، وصناديق الجدالات (splice boxes) ومعدات الاتصال.

وينبغي حماية البنية التحتية للإرسال من أي شكل من أشكال الإشعاع الذي قد يضر بعملية إرسال البيانات، ومن الهجمات السلبية (التطفل على البيانات) والإيجابية (تعديل البيانات أو تدميرها أو اختلاقها).

إن معرفة كيفية حماية وصلات المستعملين أمر في غاية الأهمية. ولهذا الغرض، يجب التعرف على هوياتهم (من هم المستعملون؟) (أين مكانهم) وتحديد متطلباتهم (ما هي تدفقات التطبيق الجاري؟). وعن طريق الرد على السؤال العام "من يعمل ماذا وأين؟" يمكن للمرء أن يُعرِّفْ مختلف المتطلبات الأمنية ذات الصلة بشبكة النقل.

وقصارى نقل البيانات هو إدماج عملية الأمن في صلب البنية التحتية للاتصال التي يجب، من ثم، أن تكون قادرة على استيعاب تلك العملية برمتها. وهذا يتطلب، في غالب الأحيان، تحديث جميع (الروترز) المُسَيِراتْ—وهو موقف يمكن أن يؤدي في بعض الأحيان إلى مشاكل تتعلق بالتشغيل البيني للمُسَيِرات وإدارة التغيير.

يضاف إلى ذلك، أن تجفير البيانات على مستوى "الشبكة" يولد رزماً من البيانات أكبر حجماً من الرزم غير المجفرة، وتكون النتيجة أن نقلها يحتل قدراً أكبر من عرض النطاق، ومن موارد الاتصال. فإلى جانب حقيقة أن عملية التجفير تزيد من وقت معالجة الرزمة، فإن تنفيذ الأمن على هذا المستوى يمكن، من ثَمَ، أن يحدث أثراً لا يستهان به على أداء الشبكة.

وتكمن الميزة الرئيسية للتجفير على مستوى البنية التحتية للشبكة في استقلالية التطبيق، ولآليات التجفير المتعلقة بالنقل، والتي يجب أن تكون شفافة بالكامل للمستعمل.

وعلى النقيض من ذلك، يقوم أمن المعاملات على مستوى التطبيق (تجفير البيانات قريباً بقدر الإمكان من تطبيق مناولة البيانات) بتعديل التطبيق ذاته، والبيانات التي يجري تجفيرها، في مكان غير مكان تسليمها إلى بروتوكول الشبكة الذي يقوم بتسييرها إلى مقصدها حيث يتم تجفيرها وذلك بواسطة مخدم التطبيق المستقبل. ويحدث أثناء الحوار الذي يجري أثناء مرحلة الإنشاء بين كيانات التطبيق (عميل ومخدم مثلاً) أن يتم الاستيقان من مفتاح الدورة، والتفاوض بشأنه. ويمكن أن يتفاوت تعقيد هذه المرحلة، ومن ثم فإن الوقت اللازم للإنشاء يتفاوت بالمثل وبمجرد أن يُستكمل ذلك، فإن التجفير يتم بسرعة كبيرة. فهو يعتمد على تنفيذ البرنامج والبنية التحتية للاتصال.

لم تعد الحماية على مستوى نطاق العمل لمستعمل ينفذ تطبيقاً واسع النطاق تعتمد على الشبكة الحاملة للبيانات، وإنما على البيئة الملامسة مباشرة للمستعمل. وتكمن صعوبة حماية التطبيقات في حقيقة أن الحماية المُقَدمة يجب أن تحتضن التطبيق برمته، ومحطة عمل المستعمل (إذْ لم تعد تقتصر على التطبيق نفسه وحسب) وبنفس المنطق، تحتضن البيئة المادية للمستخدم (النفاذ إلى المقار، إلخ).

وتتمحور تطبيقات الحماية حول مسألة حقوق المستعمل الفرد بالنسبة لمحطات العمل، والتطبيقات، والمساحة المادية التي يعمل منها.

والوظائف الأساسية لنظام التشغيل الذي يتم تركيبه في محطة عمل المستخدم تلعب دوراً بارزاً في هذه الحماية (في حين أن الأطراف الآخرين يكونون غير قادرين على التحكم أثناء دورة ما، ويحدث انفصال أوتوماتيكي بعد فترة معينة من الوقت، إلخ). ويشمل هذا حماية بطاقة الشبكة والدعم الأكيد لبروتوكولات التطبيق (إرسال الملفات المحمية، وإرسال الرسائل بصورة آمنة، إلخ) وعمليات البيانات المتماثلة (mirroring) والمزدوجة (duplexing) (حماية البيانات بتسجيل نسختين منها على أقراص، وعمليات—الكتابة والاحتفاظ باحتياطي من المعدات).

إن تأمين البنية التحتية للنقل وتأمين التطبيق يتمحوران حول نفس القضية على مستويات مختلفة:

- يجب الاستيقان من عمليات المعالجة والمستخدمين؛
- المرسل والمتلقي يستخدمان خوارزمية/تجفير خوارزمية فك التجفير متطابقتين؛
- يجب أن يمتلك كل كيان مفاتيح اتصال خوارزمية ومفاتيح تجفير/فك تجفير؛

- يجب أن تخضع مفاتيح التجفير/فك التجفير للإدارة والتنظيم؛
- ينبغي تشكيل نسق البيانات قبل نقلها.

2.9.2.III الإدارة

إذا ما حسن التنفيذ، أمكن لأنشطة النظام والشبكة أن تؤمن مستويات التوافر والأداء الضرورية لتحقيق الأمن. وهي تشمل مراقبة الشبكة، أو الشذوذ عن القاعدة، أو الحوادث (مثل الاقتحام) والكشف – وهي مهام تساهم مساهمة كبيرة في الأمن الشامل للشبكة ولنظام المعلومات الذي تخدمه.

إن الإدارة الجيدة لشبكة ما تساعد على إبقاء البنى التحتية والخدمات والبيانات متوافرة وبدرجة عالية من الكفاءة. فمن خلال إدارة الشبكة وبخاصة التشكيل، وإدارة الحوادث، يصبح من الممكن تحقيق أهداف الأمن المتمثلة في التوافر والسلامة.

يضاف إلى ذلك، أن ذلك الجانب من إدارة الشبكة المعروف بإدارة المحاسبة يوفر جميع المعلومات الضرورية ليس فقط لإرسال الفواتير للمستعملين وإنما أيضاً للقيام بوظائف المراقبة والمراجعة ذات الأهمية الكبيرة فيما يتعلق بالأمن. ويمكن أن يخدم ذلك عملية التحقق من صحة الإجراءات في إطار البرهنة أو عدم التنصل (الرفض).

وتسهم إدارة الشبكة أيضاً في تحقيق هدف السرية من حيث عدم حدوث التطفل على البيانات أو النفاذ غير المرخص به إليها. فوظيفة التحكم في النفاذ، وهي من مكونات إدارة الشبكة، ضرورية للتنفيذ التشغيلي للأمن.

يعتمد أداء ونوعية خدمة أي شبكة وتوافرها وإمكانيات الاعتماد عليها إلى حد بعيد، على نوعية إدارة طرق تسييرها (router) والمرافق التي تسمح بتمويل طريق التسيير تبعاً لحالة الشبكة وطلبات تسيير الحركة. ويمثل تحديث جداول التسيير لدى الشبكات الكبرى صداعاً تشغيلياً حقيقياً لمسؤولي الشبكات، من حيث إن أي تغييرات في القيم الموجودة في الجداول ينبغي توفيقها زمنياً وذلك لتفادي سوء الأداء أو فقدان البيانات أثناء المرور. وقد صممت بروتوكولات إدارة الشبكة، لعدة أمور من بينها، التمكين من تحديث جداول التسيير. ويمكن لإدارة الشبكة أن تسهم في أمن طرق التسيير بإنشاء نقاط نفاذ أمن أثناء تشكيلها، وتخلق إنذارات في حالة محاولات الاقتحام، وتأمين إدارة طرق التسيير ومراكز التتبع.

وهكذا فإن من المهم للغاية التمكن من توفير الحماية الضرورية بصد أو كشف الأعمال التالية إلى جانب أعمال أخرى لمنع الأفراد غير المرخص لهم من إدخال تغييرات:

- تعديل العناوين الواردة في جداول طرق التسيير، رزم بروتوكول الإنترنت، إلخ؛
- تعديل طرق التسيير، والاستنساخ غير المشروع للبيانات المنقولة؛
- رصد التدفق؛
- التحويل، تعديل وتدمير رزم البيانات؛
- رفض تأدية الخدمة، الهجوم على خطوط التسيير، إغراق الشبكة، إلخ.

ومن المهم أن يتمكن المرء من تأمين العمليات التي يتم بها تسيير البيانات عبر شبكات الاتصالات. فينبغي على مقدمي خدمات "الشبكة" حماية جميع الكيانات الضالعة في هذه العملية، وبخاصة طرق التسيير ومخدمات الأسماء، بحيث تفي نوعية خدمة التسيير بمعايير أمن التوافر (كون الخدمة تشغيلية)، والسرية (بحيث تسلم البيانات إلى المستقبلين الصحيحين)، والسلامة (بحيث لا يعتري البيانات أي تعديل أثناء النقل).

لا يكون تسليم البيانات إلى الأطراف المخولّة مضموناً من جانب خدمة أي شبكة طالما أن خدمة التوصيل لا تتأكد من صحة العنوان السليم، وبأن الخدمة تسلم فعلياً للأطراف المرخص لهم بتسلمها. ولأجل هذا، وجب القيام بمراجعة

إضافية لنوع "التحكم في النفاذ". وعلاوة على ذلك، أرسلت البيانات بدون تجفير، وسرق منها أثناء السير، فتصبح غير مفهومة للأطراف الثالثة. وحيثما كانت البيانات ذات طبيعة حساسة، فيجب تجفرها لجعلها غير مفهومة.

إن رصد شبكة للمعلومات يستتبع مراقبة دائمة لأدائها. والغرض من مثل هذا الرصد هو ضمان، ليس فقط أن نوعية الخدمة مقبولة. وإنما أيضاً، كشف المشاكل، والحوادث، والأخطاء والشذوذ عن المألوف التي تدني من أداء الشبكة، وتعرض للخطر أمن الموارد، وذلك بهدف الاستجابة الفورية والمناسبة. ويسمح رصد الشبكة بتعقب الأعمال والحوادث بحيث يمكن تسجيلها وتحليلها لاحقاً (ويرد ذلك تحت عنوان المراجعة). كما يساعد على ضمان توافر الموارد عن طريق التحقق من أن الشبكة تؤدي وظائفها بصورة سليمة. ولذلك فإن الرصد من الوظائف المهمة للغاية داخل إطار إدارة الشبكة حيث إنه يلعب دوراً في الأداء والحوادث، والتشكيل وإدارة المستخدمين والأمن.

الجـــزء IV

نهـــج شـــامل

القسم 1.IV – الجوانب المتعددة للقانون المنظم للتكنولوجيات الجديدة

1.1.IV حماية البيانات الشخصية والتجارة الإلكترونية[47]

يناقش هذا القسم حماية البيانات الشخصية من حيث انتمائها إلى التجارة الإلكترونية بصفة خاصة، ويحدد، على أساس الوضع في فرنسا وسويسرا، النصوص الرئيسية للقانون التي يجب أن يلم بها مسؤولو الأنظمة ومدراء الأمن لدى المنظمات التي تقدم الخدمات التجارية على الشبكة. وهكذا يمكن استقراء المبادئ العامة التي تحكم إجراء الأعمال في الفضاء السيبراني وتكييفها لتناسب البلدان النامية.

1.1.1.IV التجارة الإلكترونية: ما هو غير مشروع خارج الشبكة غير مشروع كذلك على الشبكة

يمكن مناقشة التجارة الإلكترونية من وجهة نظر الأعمال التجارية الإلكترونية التي تتم إما مع مستهلكين (أعمال تجارية إلى المستهلكين) (B2C) وفيما بين الشركات (أعمال تجارية إلى أعمال تجارية)، ويمكن للإدارة الإلكترونية أن توصَّف بنفس الطريقة، أي كأعمال تجارية إلكترونية إما مع المواطنين أو مع المؤسسات الخاصة أو العامة. وهذا تمييز قانوني مهم لأن القانون التجاري ينحو نحو التفريق بين المعاملات التي تتم بين الشركات والمعاملات التي تتم مع المستهلكين.

وفي أي من الوضعين، يكون الأمن، مع تكتيكات التسويق والمبيعات الملائمة على الإنترنت التي تجري بالامتثال لإطار قانوني مناسب هو الركن الأساسي للتجارة الإلكترونية. فعن طريق غرس الثقة المستندة إلى أدوات الأمن واحترام القانون، ومن ثم خلق سياق مؤدٍ إلى تبادل البيانات، يمكن للبلدان أن تشجع الجمهور العام على اتباع تكنولوجيا معلومات وخدمات اتصال وأن يطور في نفس الوقت اقتصاد خدمات حقيقي.

إن الحاجة إلى تعريف إطار قانوني مناسب لاستخدام التكنولوجيات الجديدة قد شهدت ظهور قوانين جديدة صيغت لإكمال التشريعات القائمة، والتي ينطبق معظمها على الفضاء السيبراني. ومع ذلك، ومهما يكن الأمر، فإن ما هو غير شرعي "خارج الشبكة" هو غير شرعي كذلك على "الشبكة"! فالفضاء السيبراني هو فضاء دولي عابر للحدود، ومن ثم يصعب للغاية تحديد من له الولاية القضائية لحل القضايا القانونية الناشئة عن التجارة الإلكترونية. وهذا هو السبب في أن معاملات الإنترنت يجب أن تحدد حدود العرض وأن تقدم معلومات دقيقة عن أي المحاكم هي المختصة قانوناً في حالة حدوث نزاع.

2.1.1.IV واجب الحماية

إن حماية البيانات الشخصية جانب رئيسي من جوانب التجارة الإلكترونية. إذْ يجب تنوير المستهلكين بشأن البيانات المجموعة، والمستخدمة والداخلة في الاتصالات بواسطة معلنين أو دوائر أعمال على الشبكة. وعليهم أن يعرفوا مسبقاً الكيفية التي سيتم بها استخدام البيانات المتعلقة بهم ومن سيتمكن من النفاذ إليها. ويجب إبلاغهم كذلك بشأن الخطوات المتخذة لحماية تلك البيانات. ويجب الإعراب بوضوح عن سياسة فعالة متعلقة بالخصوصية، يكون من السهل الإطلاع عليها واستشارتها، وتكون ظاهرة للعيان ومفهومة عندما تتم المعاملات التجارية. ويجب أن توضع على الموقع الشبكي للشركة المعنية.

ويجب على الشركة كذلك أن تتخذ تدابير أمن كافية لحماية بيانات العميل التي جُمِعَتْ وعولجت. وعليها أن تحرص على أن تفي الأطراف الثالثة الضالعة في المعاملات بمتطلبات الأمن.

[47] كتب هذا القسم بالتعاون والتضافر مع إغلي تاسكي، مساعد الدراسات العليا بجامعة لوزان.

3.1.1.IV احترام الحقوق الأساسية

إن سرية البيانات الشخصية والسرية الرقمية من حقوق الإنسان الأساسية.

نموذج التوجيه الأوروبي

يوجد التوجيه الأوروبي المعني بهذا الموضوع منذ 1995، ومنذ أوائل السبعينات سُنَ عدد من البلدان تشريعات وطنية بشأن حماية البيانات الشخصية، ومراقبة استخدام السجلات العامة المحتوية على معلومات اسمية وذلك تفاديا لمخاطر اختزان البيانات الشخصية دون ضرورة أو بصورة غير لائقة.

الوضع في فرنسا

ومن الأمثلة قانون تكنولوجيا المعلومات والحريات المدنية، الذي نشر في يناير 1978 ونقح في أغسطس 2004. وسرعان ما دخلت النسخة المنقحة حيز التطبيق، وأدخلت مفاهيم قانونية متكيفة مع الأشكال الجديدة للمعالجة التي ظهرت في مجتمع المعلومات والاقتصاد الرقمي. وهي تغير محل التوجيه 95/46/EC الصادر في أكتوبر 1995. وهدفها تعزيز الحقوق والحماية الممنوحة للأشخاص الماديين وتعزيز الالتزامات الواقعة على كاهل أولئك الذين يعالجون البيانات.

وتشمل التشريعات التي من هذا القبيل عادة مواداً تتعلق بـــ: تعريف البيانات الاسمية أو الشخصية، وحقوق النفاذ، والاعتراض والتصويب، وغرض المعالجة، وجمع المعلومات ولتخزين والتحديث، وأمن السجلات الاسمية، وبيع البيانات ورصد تدفقات البيانات العابرة للحدود.

وهي غالباً ما تُستَكْمَل بواسطة صكوك قانونية مثل، كما هو في حالة فرنسا، قانون الأمن اليومي الصادر في 15 نوفمبر 2001، الذي ينص على أن البيانات المتعلقة بالاتصالات الإلكترونية، باستثناء المعلومات الإعلانية، ينبغي شطبها أو جعلها مجهولة الصاحب. وما يعرف ببيانات "غير مباشرة" (كزيارة مواقع الموارد الموحدة URL أو عناوين بروتوكول مونتريال IP للمخدمات التي استشيرت، وسطور موضوع الرسالة) يجب إزالتها هي الأخرى.

الوضع في سويسرا

اعتمدت سويسرا القانون الفيدرالي بشأن حماية البيانات يوم 19 يونيو 1992 (ألمانيا مشروع قانون 21 يناير 1977، بلجيكا: قانون 8 ديسمبر 1992؛ كندا: قانون المعلومات الشخصية وحماية الوثائق الإلكترونية 1982؛ الولايات المتحدة الأمريكية: قانون الخصوصية 1974؛ القواعد بشأن قواعد البيانات والخصوصية 1988).

وحماية البيانات في سويسرا يضمنها أولاً وقبل كل شيء الدستور الاتحادي المنقح الذي دخل حيز السريان يوم 1 يناير 2000، المادة 13/2 ونصها: "*إن لجميع الأشخاص الحق في الحماية من إساءة استخدام البيانات الشخصية*"[48].

إن أهم النصوص الفيدرالية هو قانون حماية البيانات لعام 1992، والقواعد المنفذة بتاريخ 14 يونيو 1993. وينطبق قانون حماية البيانات بغض النظر عن الوسط والتكنولوجيا المستخدمين لجمع البيانات ومعالجتها. وهو ينطبق على كل من الأفراد الخصوصية وعلى السلطات الفيدرالية. وعلى الأشخاص الطبيعيين والكيانات الاعتبارية، بغض النظر عن الكيفية التي تعالج بها البيانات. وتعرف المادة 3 البيانات الشخصية بأنها "*جميع المعلومات المتعلقة بشخص محدد أو قابل للتحديد*". ويعرف القانون كذلك القواعد المتصلة بصفة محددة بالبيانات الشخصية الحساسة وببطاقات البيانات الشخصية.

[48] باستثناء الإشارة إلى عكس ذلك، ترجمت مقتطفات من النصوص القانونية الفرنسية والسويسرية من الأصل الفرنسي بواسطة خدمات الترجمة لدى الاتحاد الدولي للاتصالات.

وتُعَرَّفْ المعالجة، بصورة فضفاضة، بأنها تشمل *" أي عمليات تتعلق بالبيانات الشخصية، بغض النظر عن المعدات والتدابير المستخدمة، وبخاصة الجمع، والتخزين والاستخدام، والتعديل، والوصل، والحفظ في الأضابير للبيانات أو تدميرها"* ومع ذلك فإن المادة 2/2 تدرج عدداً من المجالات التي لا ينطبق عليها القانون مثل الإجراءات القانونية المعلقة و" *البيانات الشخصية التي عالجها شخص طبيعي قصرياً للاستخدام، والتي لم يتم إفشاؤها لطرف ثالث*" (الفقرة الفرعية أ). وفي مقرر صادر في 5 أبريل 2000، حكمت المحكمة الفيدرالية بأن سرية الاتصالات تمتد إلى الرسائل الإلكترونية. وتشمل المادة 43 من القانون الاتحادي السويسري للاتصالات التزاماً بالحفاظ على السرية وتنص: "*يحظر على أي شخص كان مسؤولاً عن تقديم خدمة الاتصال أن يقدم إلى أي شخص ثالث معلومات عن حركة المستعمل، ويحظر على مثل هذا الشخص أيضاً تمكين أي أحد آخر من نقل مثل هذه المعلومات إلى أطراف ثالثة*". المادة 44 من القانون المستكملة بالمواد 6 إلى 11 من القانون الوضعي لمجلس الاتحادي بشأن الاتصالات البريدية ومراقبة الاتصالات الصادر في 1 ديسمبر 1997.

وتتشابه القواعد السويسرية لحماية البيانات الخاصة على الإنترنت من عدة أوجه مع قواعد التوجيه الأوروبي بشأن نفس الموضوع.

4.1.1.IV القيمة الاقتصادية للتشريع

يشجع التشريع المعني بمناولة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية المنظمات على إدارة تقنية المعلومات وأمن الشبكات لديها جيداً (بما في ذلك بيانات المستعملين، ومراقبة الاتصالات والموظفين، وإدارة الحفظ، والمعالجة الأوتوماتية للبيانات الشخصية أو غير ذلك). ويجب على المنظمات أن تتزود بالوسائل الملائمة للأمن والضبط.

وتتراوح القيمة الاقتصادية للاستثمارات المطلوبة لكفالة المستوى الأدنى من الأمن (الحماية المادية والقانونية) حسب ما قد يلحق بالمنظمة من خسائر مادية محتملة ومخاطرة بسمعتها وصورتها، وهكذا فإن التشريع هو عامل داخلي للأمن.

2.1.IV التجارة الإلكترونية وإبرام العقود في الفضاء السيبراني[49]

يناقش هذا القسم مختلف جوانب العقود من حيث اتصالها بالمعاملات التجارية التي يتم إجراؤها في الفضاء السيبراني، كما يحدد النصوص التشريعية السويسرية والأوروبية الرئيسية التي تنظم مثل هذه المعاملات. وتتضمن اللوائح التنظيمية السويسرية والتوجيهات الأوروبية الرئيسية المشار إليها عدداً من المبادئ الأساسية التي يمكن تعديلها لتتلائم مع بلدان وقوانين وطنية أخرى.

1.2.1.IV مسألة اختيار القانون

المشكلة القانونية الأولى التي تطرحها التجارة الإلكترونية هي تعريف المنطقة الجغرافية التي تتم فيها المعاملة الإلكترونية. ولا تتوافق خواص الإنترنت (التغطية الدولية والتكنولوجيا الرقمية وأسلوب التشغيل) مع مفهوم الحدود الجغرافية للدول، كما لا تتوقف تدفقات المعلومات عند الحدود الدولية.

ويمكن النفاذ إلى البيانات والخدمات وتقديمها عن بعد، وذلك بغض النظر عن مكان مستعملي الإنترنت أو المخدّمات، وغالباً ما يتعامل كل من البائع والزبون من بلدان مختلفة، ولذلك فإن معرفة أي القوانين تسري عند نشوب نزاع هو أمر في غاية الأهمية، بل ويشكل نقطة أساسية في أي عرض. وفي هذا الخصوص، يجب على المعاملات التي يتم إجراؤها عبر الإنترنت أن تشير إلى حدود العرض، وتوفير معلومات محددة بشأن أي المحاكم لها الولاية القضائية للفصل في حالة نشوب نزاع[50].

---

[49] كتب هذا القسم بالتعاون والتضافر مع إغلي تاسكي، مساعد الدراسات العليا بجامعة لوزان.

[50] يشير مصطلح Lex Fori إلى مبدأ خاص في القانون الدولي يعنى به قانون البلد التي تتم فيه إجراءات التقاضي.

يجوز أن تتفق أطراف العقد على اختيار القانون والمحكمة التي لها الولاية القضائية، وفي حالة عدم وجود البند الذي ينص على اختيار القانون، فيجب عندئذ تحديد ما إذا كان العقد يدخل في نطاق معاهدة دولية مثل مبادئ المعهد الدولي لتوحيد القوانين الخاصة UNIDROIT بشأن العقود التجارية الدولية (1994)، وهذا نوع من إتيكيت الإنترنت، أو اتفاقية لاهاي المؤرخة في 15 يونيو 1955. إلا أن الاتفاقيات الدولية ليست ملزمة، إلا إذا تم إدراجها في العَقدْ بشكل صريح.

وإذا لم يكن بالإمكان استخدام أي من هذه الحلول، انطبقت قواعد قانون العَقْد.

ففي القانون السويسري على سبيل المثال، ترد هذه القواعد في القانون الاتحادي بشأن القانون الدولي الخاص لعام 1987، الذي تنص المادة 1 منه على[51]:

"1 أن القانون ينظم الأمور التالية في سياق دولي:

أ- الولاية القضائية للمحاكم السويسرية أو السلطات الإدارية؛

ب- القانون الحاكم؛

ج- متطلبات الاعتراف بالقرارات الأجنبية وإنفاذها؛

د- إشهار الإفلاس والتسوية مع الدائنين؛

هـ- لتحكيم.

2 عدم المساس بالمعاهدات الدولية."

المبدأ الأساسي هو كما يلي: يخضع العقد لقانون الدولة التي يرتبط بها أوثق ارتباط (المادة 117/1 من القانون)، ويشير ذلك بصفة عامة إلى من يقدم السلع أو الخدمات إذا تم إدراج ذلك بشكل صريح في الشروط العامة، وذلك باستثناء واحد: المادة 120 من هذا القانون التي تنظم العقود مع المستهلكين وتنص على:

"تخضع العقود الخاصة بأداء يتعلق بالاستهلاك العادي الموجه للاستخدام الشخصي للمستهلك أو لأسرته وليس متصلاً بأنشطة مهنية أو تجارية لقانون الدولة محل الإقامة العادية للمستهلك، وذلك إذا:

أ- كان صاحب العرض قد تلقى الطلب داخل تلك الدولة؛

ب- إن في تلك الدولة قد سبق إبرام العقد عرضٌ أو إعلانٌ وأن يكون المستهلك قد اتخذ الإجراءات القانونية الضرورية لإبرام العقد، أو

ج- إن صاحب العرض قد حث المستهلك على الذهاب إلى خارج البلاد ثم يقوم بتسليم الطلب هناك.

2 يكون اختيار القانون مستبعداً."

قد يكون محتوى الموقع، على سبيل المثال اللغة المستخدمة أو العملة المدرجة مؤشراً على السوق المستهدفة لصاحب العرض وبالتالي على القانون الساري.

وفي الحالات التي لا يتحدد اختيار القانون فيها بموجب اتفاق بين الأطراف، يكون من المحتمل رفع دعوى قضائية في محل إقامة المدعى عليه أو المقر الرئيسي.

[51] مصدر النسخة الإنكليزية في القانون الاتحادي بشأن القانون الدولي الخاص: Jerome H. Farnum, B.A., J.D., *Swiss Federal Act on International Private Law, English Translation of Official Tex*t, Swiss-American Chamber of Commerce/Schulthess, Zurich, 2004 (revised edition).

2.2.1.IV العقود التي يتم إبرامها إلكترونياً

إن القواعد التي تسري على العقود المبرمة إلكترونياً هي بصفة العموم نفس القواعد التي تنطبق على ما يسمى بالعقود التقليدية، ويعتبر العقد قد أبرم عندما يكون أحد الأطراف قد تقدم بعرض ويكون الطرف الآخر قد قبل ذلك العرض.

التوجيه الأوروبي

يعنى التوجيه 97/7/EC للبرلمان الأوروبي والمجلس الأوروبي المؤرخ في 20 مايو 1997 بمسائل المبيعات والتجارة الإلكترونية عن بعد. وهو ينص على وجوب توفير المعلومات التالية للمستهلك قبل إبرام العقد بفترة مناسبة، وذلك لأي عقد عن بعد:

- هوية المورِدْ، وفي حالة العقود التي تتطلب الدفع مسبقاً، عنوانه أيضاً؛
- الخصائص الرئيسية للسلع أو الخدمات؛
- أسعار السلع أو الخدمات شاملاً كل الضرائب؛
- تكاليف التسليم، حيثما يتناسب؛
- ترتيبات الدفع أو التسليم أو الأداء؛
- وجود حق الانسحاب، إلا في الحالات المشار لها في المادة 6 (3) من التوجيه؛
- تكلفة استخدام طرق الاتصال عن بعد، عندما يتم حسابها على أساس سعر مختلف عن السعر الأساسي؛
- الفترة التي يظل فيها السعر أو العرض سارياً؛
- أقل فترة للعقد، حيثما يتناسب، وذلك في حالة عقود الإمداد بالمنتجات أو الخدمات بشكل دائم أو متكرر.

والنقطة الأكثر أهمية فيما يتصل بإبرام العقد هي ما يتعلق بتعريف ما يشكل "عرضاً" وما يشكل "قبولاً للعرض". فلا تشكل السلع (المعروضة) على أي من مواقع الإنترنت بإشارة إلى السعر والمعلومات الإعلانية المتصلة بذلك عرضاً، ولكن بالأحرى دعوة إلى تقديم العروض، وذلك بما لا يتعارض مع المدونة السويسرية للالتزامات التي تنص المادة 7 منها على إنه " [2] *لا يشكل إرسال التعريفة الجمركية أو قوائم الأسعار أو ما شابه عرضاً في حد ذاته [...]*".[52]

وإرسال رسالة إلكترونية أو استمارة طلب يعتبران دعوة إلى تقديم العروض.

وعندما يقبل المشتري ويضغط على زر (شراء)، يكون عرضاً أكيداً قد تم التقدم به، وتم الدخول في العَقدْ، فهو لا يعبر عن أية نية للشراء بمجرد زيارته للموقع الشبكي بأي درجة أكبر من مجرد زيارة المحل التجاري. ومن ناحية أخرى يمكن أن يشكل عرض السلع على الموقع الشبكي عرضاً فقط إذا أوضح البائع المخزون المتاح من السلع حالياً، وأنه آخذ في التناقص نتيجة لورود طلبات، أو إذا كانت هذه السلع بطبيعتها تمكن البائع من تلبية الطلب.

ويتم العقد عندما يتسلم متلقي الخدمة أي المستهلك الراغب في شراء السلع المعروضة تأكيداً إلكترونياً من البائع، ولكن بشرط إذا تم إرسال الوثيقتين خلال فترة قصيرة تفصل بينهما، وفي هذا الصدد هناك تمييز ما بين العقد الذي يكون معلوماً للطرفين كليهما في نفس الوقت، والعقد الذي لا يكون كذلك.

---

[52] مصدر النسخة الإنكليزية هو مدونة الالتزامات: Rebecca Brunner-Peters, J.D., et al, *Swiss Code of Obligations*, Volume I, Contract Law, Articles 1-551, English Translation of the Official Text, Swiss-American Chamber of Commerce/Schulthess, Zurich, 2005 (revised).

هل يمكن أن يقع العقد مبرماً وأطرافه غائبون؟ نعم، ولكن...

أي عقد يبرم على الإنترنت يعتبر عقداً بين أطراف غائبة، الأمر الذي يعني ضمناً أن العقد ينبغي أن يُقبل خلال فترة زمنية معقولة، كما نصت على ذلك المادة 5 من المدونة السويسرية للالتزامات:

"المادة 5:

ب- فيما بين أشخاص غير حاضرين...

[1] إذا تم تقديم العرض لشخص غير حاضر دون تحديد حد زمني، يظل صاحب العرض ملزماً حتى الوقت الذي يكون من حقه فيه منطقياً تلقي رد مرسل إليه بطريقة صحيحة وفي التوقيت السليم.

[2] وهكذا يجوز لصاحب العرض عندئذ أن يفترض أن عرضه قد وصل في التوقيت السليم.

[3] إذا كان إعلان القبول قد أرسل في الوقت المناسب ولكنه وصل إلى صاحب العرض فقط بعد ذلك الوقت، يكون صاحب العرض ملزماً ما لم يقدم إخطاراً دون تأخير بنيته بعدم الاعتداد بالعقد."

ولكن إذا تم تبادل معلومات العقد خلال منتدى للمناقشة أو حجرة محادثة أو برنامج فوري للرسائل أو المهاتفة من خلال الإنترنت، فيعتبر العقد معلوماً للطرفين كليهما في نفس الوقت، ويجب أن يكون القبول فورياً. وتنص المادة 4/1 من المدونة السويسرية للالتزامات على أنه: *"إذا تم تقديم عرض لشخص حاضر بدون تحديد حد زمني، فلا يعتبر صاحب العرض ملزماً بعد ذلك إذا لم يُقبل العرض فوراً."*

3.2.1.IV التوقيع الإلكتروني

يمكن للقارئ اختبار سلامة الرسالة وبالتالي ضمان أنها لم تُعدل أثناء الإرسال والتأكد ممن هو المرسل، وذلك بفضل نظام التجفير اللاتناظري، وهكذا فلا يمكن للمرسل أن ينكر أنه أرسل الرسالة (مفهوم عدم الرفض). ويتم القيام بهذه الخدمات لأمن المعلومات باستخدام شهادة رقمية (للتوقيع) على وثيقة رقمية، وبالتناظر مع التوقيع المكتوب باليد، فإن التوقيع الإلكتروني هو توقيع رقمي للبيانات.

وهناك مفاهيم متصلة بذلك وهي مفاتيح التجفير (الخصوصية والعمومية) (المعروفة أيضاً باسم الطرف الثالث الموثوق به TTP).

ولكي يتم اعتبار التوقيع الإلكتروني مناظراً للتوقيع المكتوب باليد على وثيقة ورقية في العالم الرقمي، فلا بد أن يكون مرتبطاً بشكل متفرد بالموقّع، ولا بد أن يكون لديه القدرة على تحديد الموقع، ولا بد أن يتم عمله من خلال وسائل يكون الموقّع قادراً على إبقائها تحت تحكمه منفرداً.

ويعتبر القانون السويسري أن التوقيع الإلكتروني لديه نفس التأثير الذي للتوقيعات المكتوبة، وطبقاً للمادة 14 من مدونة الالتزامات:

"[1] يجب أن يكون التوقيع مكتوباً باليد.

[...]

[2مكرراً] ويكون التوقيع الإلكتروني المؤهل القائم على شهادة مؤهلة يصدرها مقدّم خدمات التصديق المعترف بها في إطار المعنى الذي يرمي إليه القانون الاتحادي بشأن التوقيعات الإلكترونية تاريخ 19 ديسمبر 2003 مكافئاً للتوقيع المكتوب باليد. وتبقى الأحكام القانونية أو التعاقدية المخالفة لذلك محفوظة".

ينظم التوقيعات الإلكترونية القانون الاتحادي بشأن التوقيعات الإلكترونية بتاريخ 19 ديسمبر 2003 الذي يحدد التوقيع الإلكتروني ويصف الصور العديدة التي يمكن أن يكون عليها، ويدرج قائمة بالجهات الضالعة في تنفيذ آلية التوقيع وإصدار الشهادات الرقمية.

"مادة 2- تعريفات

ولأغراض هذا القانون

أ- يعني التوقيع الإلكتروني البيانات الموجودة في صورة إلكترونية المرفقة أو المرتبطة منطقياً ببيانات إلكترونية أخرى والتي تعمل كطريقة للاستيقان؛

ب- يعني التوقيع الإلكتروني المتطور توقيعاً إلكترونياً يفي بالمتطلبات التالية:

1. *أن يكون متصلاً بشكل متفرد بالموقع،*
2. *أن يكون بإمكانه تحديد هوية الموقع،*
3. *أن يكون قد تم عمله باستخدام وسائل يمكن للموقع الإبقاء عليها تحت تحكمه منفرداً،*
4. *أن يكون مرتبطاً بالبيانات التي يتصل بها بطريقة تجعل من الممكن اكتشاف أي تغيير لاحق للبيانات.*

ج- يعني التوقع الإلكتروني المؤهل توقيعاً إلكترونياً متطوراً بناء على ترتيب آمن لإنشاء التوقيع، وذلك في إطار ما تعنيه المواد 6/1 و 6/2 وعلى شهادة مؤهلة كانت صالحة أثناء إنشائه؛

د- يعني مفتاح التوقيع بيانات متفردة مثل الرموز أو مفاتيح التجفير التي يستخدمها الموّقع لإنشاء توقيع إلكتروني؛

هـ- يعني مفتاح التحقق من التوقيع بيانات مثل الرموز ومفاتيح التجفير العامة التي يتم استخدامها لغرض التحقق من التوقيع الإلكتروني؛

و- تعني الشهادة المؤهلة شهادة تفي بالمتطلبات الموضحة في المادة 7؛

ز- يعني مقدمو خدمات التصديق إحدى الجهات التي تقوم بالتصديق على البيانات في البيئة الإلكترونية وتصدر شهادات رقمية من أجل ذلك الغرض؛

ح- تعني هيئة الاعتراف الجهة المخولة بالاعتراف بمقدمي الخدمات والإشراف عليهم، وذلك طبقاً لقواعد الاعتماد؛

[...]".

التوقيع الإلكتروني والتوجيه الأوروبي

يقوم التوجيه 1999/93/EC بتاريخ 13 ديسمبر 1999 بشأن إطار العمل الأوروبي بالتمييز ما بين الأنواع الثلاثة للتوقيعات الإلكترونية وذلك تبعاً لدرجة إدماج آليات التجفير وعلى مستوى الأمن الذي يمكن تحمل تكلفته.

وهناك أنواع عديدة من التوقيع الإلكتروني. الأول هو ببساطة التوقيع على الرسالة بدون ربط التوقيع بمحتويات الرسالة (وهو المبدأ الأساسي في التوقيع الإلكتروني). وفي هذه الحالة يمكن لأي أحد أن يقوم بفصل التوقيع من الرسالة واستخدام هذا التوقيع، ويحل محل صاحب الحق المشروع في التوقيع، وللتغلب على هذا النقص يمكن استخدام وظيفة تجفيرية لربط التوقيع بمضمون الرسالة، وللتحقق من صحة هوية المرسل، ومن سلامة الرسالة عند التلقي (مفهوم التوقيع الإلكتروني المتطور).

وختاماً يناقش هذا التوجيه التوقيعات الإلكترونية الآمنة القائمة على أحكام أمنية تبعاً للملحق الثاني بشأن متطلبات مقدمي خدمات التصديق الذين يقومون بإصدار شهادات مُؤَهَلة[53].

4.2.1.IV حق الإبطال

قد تدفع السهولة التي يمكن من خلالها شراء الأشياء على الإنترنت بعض المستهلكين إلى التصرف بتعجل، ولحق الإبطال أهمية خاصة في هذا السياق.

ففي سويسرا، يتم تنظيم حق الإبطال بالمادة 9 من مدونة الالتزامات في الفقرة 1 التي توضح المبدأ التالي: *"إذا قام صاحب العرض بإبطال عرضه، ووصل هذا الإبطال إلى الطرف الآخر قبل (...) العرض، فسوف يعتبر (...) العرض كأنه لم يكن"*، وينطبق نفس المبدأ على إبطال القبول.

حق الإبطال والتوجيه الأوروبي

في الاتحاد الأوروبي يتم تنظيم حق الإبطال من خلال التوجيه 1997/7/EC بتاريخ 20 مايو 1997 الذي ينص على أنه بالنسبة لأي عقد يبرم عن بعد، يمكن للمستهلك الانسحاب من العقد بدون توقيع عقوبة، وبدون إبداء أية أسباب، وذلك خلال فترة لا تقل عن سبعة أيام عمل. إذا لم يتمكن المورد من الوفاء بالالتزامات الموضحة في المادة 5، وخاصة فيما يتعلق بالشروط والإجراءات من أجل ممارسة حق الإبطال، وتكون الفترة عندئذ ثلاثة أشهر.

5.2.1.IV إدارة النـــزاعات

سوف يكون على الضالعين في نزاع ينشأ عن عقد تم إبرامه بشكل مثبت أن يقدموا البرهان بشأن ما إذا كان العقد قد تم إبرامه إلكترونياً أم لا. ولهذا فإنه مما ينصح به دائماً هو الحفاظ على سجلات المعاملة، مثل نسخة من الرسالة الإلكترونية أو طباعة من على الشاشة.

الموقف في فرنسا

في فرنسا، لا تحدد المادة 109 من مدونة المستهلك الشكل الذي لا بد أن يكون البرهان عليه وذلك فيما يتصل بالمعاملات بين الشركات، ولهذا فإن رسائل البريد الإلكتروني معترف بها مثلها مثل الوثائق الورقية. ولكن فيما يتعلق بالمعاملات بين الشركات والزبائن، فلا بد أن يكون هناك إثبات مكتوب للمعاملات التي تتجاوز قيمتها مبلغاً معيناً من المال. والغاية من ذلك هي حماية المستهلك المتوسط، الذي ليس لديه لا القدرة ولا الموارد القانونية لرفع قضيته في حالة نشوب النـــزاع مع شركة تجارية.

ولكن يمكن أن تكون رسائل البريد الإلكتروني معترفاً بها كبرهان، وذلك في إطار النصوص القانونية التي تحكم التوقيع الإلكتروني، ويعني هذا أن أي رسالة بريد إلكتروني موقعة إلكترونياً سوف تكون بمثابة إثبات صحيح إذا روعي احترام الأحكام المذكورة أعلاه بشأن التوقيعات الإلكترونية.

شروط عامة

تتضمن العقود عن بعد في غالب الأحيان شروطاً عامة تكون جزءاً لا يتجزأ من العقد، ولكي تكون هذه الشروط العامة صالحة في حالة النـــزاع، فلا بد أن يكون من السهل النفاذ إليها والتماس المشورة بشأنها على الخط، ويجب إحاطة المستهلك علماً بشكل واضح بأن تلك الشروط جزء من العقد.

[53] http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

فض النـــزاعات على الخط

نظراً للطبيعة الدولية للتجارة الإلكترونية، تم بلورة وسائل لتسوية النـــزاعات بحيث تتخطى المحاكم التقليدية. وقد ولد مفهوم فض النـــزاعات على الخط (ODR) انطلاقاً من الرغبة في العثور على حلول فورية لعدم أداء العقود التي يتم إبرامها عبر الإنترنت. ويقوم هذا النوع من فض النـــزاعات على تحقيق التوافق، مما يتضمن التفاوض والوساطة والتحكيم[54]، وهذا أسرع وأقل تكلفة وأكثر راحة للمستعملين، ولكن نقطة الضعف هي أن ذلك قائم على مدونات سلوك وتوصيات، تعرف أيضاً بالقانون اللين مثل (السياسة العامة لمؤسسة الإنترنت للأسماء والأرقام المخصصة ICANN بشأن تسوية النـــزاعات حول أسماء الميادين)، مما يجعل من الصعب إنفاذ المقررات.

3.1.IV الفضاء السيبراني والملكية الفكرية[55]

1.3.1.IV فروع القانون التي تحمي الملكية الفكرية

تتم حماية حقوق الملكية الفكرية من خلال العديد من فروع القانون، وهي أساساً:

- قانون العلامة التجارية؛
- قانون حقوق المؤلف؛
- قانون براءات الاختراع؛
- قانون التصميم والنموذج؛
- القانون الذي يحمي الأصناف النباتية؛
- القانون بشأن طوبوغرافيات أشباه الموصلات؛
- قانون شعارات النبالة العامة والشارات العمومية الأخرى؛

قانون المنافسة غير العادلة والذي يؤثر أيضاً في حقوق الملكية الفكرية.

2.3.1.IV حقوق المؤلف والحقوق المجاورة لها

هذا هو فرع من القانون يقوم بحماية:

- مؤلفي الأعمال الأدبية والفنية؛
- المؤدين، ومنتجي الصوتيات والمرئيات ومشروعات الاتصال الصوتي المرئي.

والعمل هو إبداع روح أدبية أو فنية، وهذا أمر فردي بطبيعته، مهما كانت قيمته أو غرضه المقصود، ويتضمن إبداع الروح ما يلي:

- الأعمال التي تستخدم اللغة، سواء كانت علمية أم أدبية أم غير ذلك؛
- الأعمال الموسيقية والصوتية الأخرى؛
- أعمال الفنون الجميلة، وخاصة أعمال النحت والأعمال الجرافيكية/المرئية؛

[54] هذه الآلية لتسوية النـــزاعات هي موضوع نموذج قانون قامت بوضعه لجنة منظمة الأمم المتحدة بشأن قانون التجارة الدولية (UNICITRAL).

[55] كُتب هذا القسم بالتعاون مع الأستاذة سارة بن لغا من جامعة تونس التقنية، وهي محاضرة في جامعة لوزان.

- الأعمال ذات المحتوى العلمي أو التقني، مثل التصميمات والخطط والخرائط أو الأعمال المنحوتة أو المنمذجة؛
- الأعمال المعمارية؛
- أعمال الفن التطبيقي؛
- الأعمال الصوتية والسينمائية وغيرها من الأعمال السمعية-البصرية؛
- الأعمال الرمزية المتعلقة بالرقص والمسرح؛
- برمجيات الكمبيوتر؛
- المشروعات والعناوين وأجزاء العمل التي هي فردية بطبيعتها.

تُخَوِلْ حقوق المؤلف له (وهو الشخص الحقيقي الذي قام بإبداع هذا العمل) أو للمؤلف المفُتْرض (وهو الشخص الذَي أتى بالعمل حتى يتم إثبات هوية المؤلف) التمتع بكافة الحقوق الأدبية وحقوق الملكية للعمل.

وليس من الضروري إيداع العمل لدى مكتب، أو تسجيل الحقوق، بالرغم من أن بعض البلدان لديها إيداعات لحقوق المؤلف. إذْ لا يمكن حماية الأفكار إلا إذا تم كتابتها أو عملها، لأنه لا يمكن حماية إلا العمل المحسوس أو الملموس.

يشير مصطلح (الحقوق الأدبية) أساساً إلى الاعتراف بتأليف العمل، والحق في تقرير ما إذا كان العمل سوف يتم نشره، ومتى، وبأي شكل، وتحت أي اسم، بينما يتصل مصطلح (حقوق الملكية)، وذلك باستخدام العمل (إنتاج وبيع النسخ، والتوزيع والإذاعة وغير ذلك).

لا يعني نقل ملكية العمل، سواء الصورة أو الأصل نقل حقوق المؤلف. وحقوق المؤلف قابلة للتنازل وللتوريث.

يشير مصطلح "الحقوق المجاورة" إلى حق المؤدين (الأشخاص الحقيقيين الذين يؤدون عملاً أو يشاركون فنياً في أدائه) لمنتجي الصوتيات والمرئيات ولشركات الاتصال الصوتي-المرئي.

3.3.1.IV قانون العلامة التجارية

إن الهدف من العلامة التجارية هو التمييز بين المنتجات والخدمات الخاصة بصاحب العلامة التجارية من تلك الخاصة بشركات أخرى. وتحدد العلامة التجارية شيئاً (وليس تابعاً للقانون يتم تحديده باسم أو باسم شركة).

وليس بالإمكان الحصول على حماية للعلامة التجارية لما يلي:

- العلامات الموجودة في ميدان عام؛
- أشكال تتصل بطبيعة المنتج أو هي كامنة في استخدامه؛
- العلامات المضللة؛
- العلامات المنافية للقانون السائد أو للمبادئ الأخلاقية.

يجب تسجيل العلامة من أجل الاستفادة من الحماية، ويمكن معارضة إحدى العلامات المسجلة:

- إذا كانت العلامة مطابقة لعلامة تم تسجيلها سابقاً لمنتج مطابق؛
- إذا كانت مطابقة أو مشابهة لعلامة تم تسجيلها من قبل لمنتجات أو خدمات وهناك حظر للخلط.

4.3.1.IV قانون براءات الاختراع

يتم إصدار براءات الاختراع للاختراعات الصناعية، ولا يمكن إصدارها للمنتجات الفرعية الواضحة للتطور التقني، ولا لأصناف الحيوانات أو النباتات، ولا للعمليات البيولوجية الجوهرية المستخدمة لإنتاج نباتات أو حيوانات، ويمكن إصدارها للعمليات الميكروبيولوجية والمنتجات التي يمكن الحصول عليها من خلال تلك العمليات.

تُمنح براءة الاختراع (تحت شروط محددة) إلى الشخص الذي قام بالإجراءات من أجل ذلك (وهو المخترع أو من يخلفه طبقاً للقانون أو طرف ثالث يملك الاختراع بناء على أسباب أخرى).

إذا قام العديد من الأشخاص باختراع نفس المنتج أو العملية بشكل مستقل، فيتم عندئذ منح براءة الاختراع إلى من تقدم إليها أولاً أو من له الأولوية في تقدمه.

5.3.1.IV الحماية الفكرية لموقع شبكي

وعلى الإنترنت وبخاصة ما يتعلق بالمواقع الشبكية، تتضمن حماية الملكية الفكرية للموقع الشبكي العديد من فروع القانون[56]:

- بخصوص اسم الميدان:
  - لا يمنح تسجيل اسم الميدان في حد ذاته أية حقوق حصرية للمالك؛
  - من أجل حماية اسم الميدان، يجب الرجوع إلى الأسس القانونية التي هي:
    - قانون العلامة التجارية؛
    - القانون الذي يحكم أسماء الشركات؛
    - حق التسمية؛
    - قانون المنافسة؛
- ما يتعلق بمحتوى الموقع الشبكي:
  - توزيع الأعمال عبر الإنترنت تحديداً:
    - إذا تم إنشاء المحتوى تحديداً من أجل الموقع، فهو محمي بموجب حقوق المؤلف؛
    - رقمنة عمل قائم وتوزيعه على الخط هو نوع من إعادة الإنتاج، مما يستوجب موافقة مؤلف العمل الأصلي؛
    - الصلات مع مواقع أخرى: لا يشكل استخدام صلة فوقية بسيطة اعتداءً على أية حقوق حصرية، حيث لا يتضمن ذلك إعادة للإنتاج، ولكن الروابط العميقة (التي توجه المستعمل إلى صفحة بعينها في موقع آخر، متخطياً الصفحة الرئيسية للموقع) هي أمر مختلف. فالمسألة هي ما إذا كانت الصفحة موضع النقاش عملاً أم لا، وكقاعدة، يمكن تنظيم في مسائل مثل هذه من خلال قانون المنافسة، ويكون المعيار القاطع عندئذ هو الطريقة التي يتم بها استخدام الروابط الفوقية. الاستخدام العادل هو المفهوم الأساسي هنا.

6.3.1.IV الطبيعة التكميلية للحماية التقنية والقانونية

يتم استحداث تدابير تقنية لكفالة احترام حقوق المؤلف، ويتم اعتماد تشريعات لكفالة ألا يتم التحايل على تلك التدابير، وهكذا تتمتع حقوق المؤلف بحماية قانونية، وحماية تقنية، وحماية قانونية للحماية التقنية.

[56] Philippe Gilliéron, *Propriété intellectuelle et Internet*, University of Lausanne (CEDIDAC No. 53), 2003

4.1.IV البريد الاقتحامي: بعض الاعتبارات القانونية[57]

1.4.1.IV السياق والإزعاج

بشكل عام، تشير كلمة spam[58] أو البريد الإلكتروني الاقتحامي إلى إرسال رسائل غير مطلوبة، وتتميز بما يلي:

- يتم إرسال الرسائل غير المطلوبة بأعداد كبيرة مراراً وتكراراً؛
- يكون للرسالة هدف تجاري، أو تكون ذات مقصد خبيث (الرسائل الخداعية، الاستحواذ على الكمبيوتر، واستحداث برمجيات خبيثة مثل الفيروسات وبرامج الإعلانات والتجسس وغير ذلك)؛
- عادة ما يكون قد تم الحصول على العناوين بدون معرفة أصحابها (وذلك بالمخالفة للقواعد المتعلقة بحماية البيانات الشخصية)؛
- غالباً ما يكون المضمون مخالفاً للقانون أو مضللاً أو ضاراً.

ونظراً لكون البريد الاقتحامي غير مطلوب، فإنه يعتبر أحياناً أسلوباً مقتحماً للبيع أو للإعلان. واليوم لا يأخذ هذا البريد فقط صورة رسائل للبريد الإلكتروني ولكن أيضاً رسائل خدمات الرسائل القصيرة على الهواتف المحمولة/النقالة أو على المعدات الحديثة متعددة الوسائط مثل الحاسب الشخصي للجيب.

يتسبب البريد الاقتحامي في تكبيد كل مستعملي الإنترنت تكاليف، وتتعلق هذه التكاليف عامة بالوقت الذي يستغرقه معالجة الرسائل، والحصول على أدوات لمنع البريد الاقتحامي، وهناك تكلفة اجتماعية من حيث فقدان ثقة المستعملين وانخفاض الإنتاجية وغير ذلك.

وتفيد دراسة قامت بها شركة كليرسويفت لمكافحة البريد الاقتحامي (anti-spam firm Clearswift) تم نشرها في مجلة (جورنال دو نت) Journal du Net جريدة الشبكة بتاريخ 13 سبتمبر 2005، فإن البريد الاقتحامي يقع في إحدى الفئات التالية:

أنواع البريد الاقتحامي	يونيو 2005
الصحة	%43,86
المنتجات	%37,65
الأمور المالية	%9,06
الصور والأفلام الإباحية	%5,32
الرسائل الخداعية	%1,41
المراهنة	%0,1
أمور أخرى	%2,32

[57] تمت كتابة هذا القسم بالتعاون والتضافر مع إيجلي تاشي، وهو معيد في قسم الدراسات العليا في جامعة لوزان.

[58] كانت كلمة spam أساساً علامة تجارية مسجلة لهورمل وكانت بمعنى (لحم ولحم خنـــزير متبل)، وهو نوع من لحم البقر المملح الذي كان يقدم للجنود الأمريكيين أثناء الحرب العالمية الثانية، ويشير استعماله الحالي إلى إرسال رسائل بريد إلكترونية غير مطلوبة وينبع هذا فيما يبدو من عمل مسرحي قصير لمونتي بايثون يتم فيه غناء كلمة spam مراراً وتكراراً، مما يجذب أصوات الشخصيات الأساسية الأخرى في المسرحية.

يمكن للبريد الاقتحامي أن يأخذ العديد من صور (الخُدع)، ومن أشهرها ما يطلق عليه الخطاب النيجيري[59]. الرسائل الخداعية الاستدراجية هي عبارة عن إرسال رسالة تبدو أنها قادمة من مؤسسة معروفة، على سبيل المثال أحد البنوك، وتدعو المتلقي إلى الاتصال والدخول على موقع زائف، وإدخال رموز النفاذ ومعلومات أخرى حساسة، ومن ثم يتم استخدامها بدون علمه.

ويمكن أيضاً إرسال البريد الاقتحامي لأغراض تدميرية، أو لإغلاق صندوق البريد الخاص بالمتلقي، مما يجعل من غير الممكن له استقبال رسائل ومنعه من استخدام موارد الإنترنت. ويحدث القصف البريدي بأشكال متنوعة: رسائل ضخمة تؤدي إلى مشكلات في المعالجة والحفظ المؤقت، وكميات هائلة من الرسائل، والإرسال لعدد ضخم من المتلقين لإغراق المخدّم أو الاستحواذ على عنوان المرسل عنوة.

2.4.1.IV العلاجات القانونية للبريد الاقتحامي

يتم تغطية البريد الاقتحامي من قبل العديد من مجالات القانون، وخاصة قانون حماية البيانات، وقانون المنافسة غير العادلة، ويتحمل من يقومون بإرسال البريد الاقتحامي مسؤولية جنائية.

الموقف في سويسرا

لا توجد في سويسرا أحكام قانونية تنص بشكل صريح على الحد من استخدام البريد الاقتحامي.

فمن وجهة نظر حماية البيانات، وطبقاً لمفوض الاتحاد السويسري بشأن حماية البيانات ووثيقته (مذكرة المساعدة بشأن الرسائل المنشورة غير المرغوب فيها التي تنتشر من خلال البريد الإلكتروني/ البريد الاقتحامي) *Aide-mémoire concernant les messages publicitaires indésirables diffusés par courrier électronique (spams)*[60]، فإن العناوين الإلكترونية هي بيانات شخصية يمكن استخدامها لتحديد هوية الشخص. وتبعاً للمادة 12/3 من قانون حماية البيانات، فإنه "*كقاعدة عامة، لا يمكن التعدي على حقوق الشخص إذا كان الشخص المتضرر قد قام بجعل البيانات متاحة في النطاق العام ولم يمنع بشكل صريح معالجة هذه البيانات*". ويشكل معالجة العناوين الإلكترونية بواسطة مرسل بريد اقتحامي تعدياً على الخصوصية (مادة 4/3) تم ارتكابه بنية سيئة (مادة 4/2) بدون موافقة الشخص المعني (مادة 13/1)، ولهذا فهو يشكل مخالفة لحماية البيانات.

"المادة 4 مبادئ

1 يجب القيام بأي معالجة للبيانات الشخصية بشكل مشروع.

2 يجب القيام بالمعالجة بنية حسنة ولا يجب أن يكون مفرطاً.

3 يمكن فقط معالجة البيانات الشخصية للغرض الذي إما تم جمعها من خلاله أو ما هو ظاهر من الظروف، أو ما ينص عليه القانون."

يخول قانون حماية البيانات للأشخاص المعنيين بالرجوع إلى المحاكم (المادة 15 التي تشير إلى المادة 28 وما بعدها من القانون المدني السويسري).

---

[59] يقدم المرسل نفسه على أنه وريث شخص ثري متوفي حديثاً، أحياناً في دولة نائية، ويزعم الوريث أن لديه مشاكل في المطالبة بحقه ويقترح استخدام الحساب الخاص بالضحية وذلك في مقابل مبلغ ضخم يعوض الضحية عما يلحق به، ويجب على الضحية مقدماً دفع تكاليف المعاملة، وهذه محاولات قد تختلف لخداع الناس للحصول على أموالهم.

[60] www.edsb.ch/f/doku/merkblaetter/spam.htm

التوجيه الأوروبي

وضع التوجيه 95/46/EC بتاريخ 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبالحركة الحرة لهذه البيانات المعايير الدنيا لإنشاء مثل هذه السجلات ومعالجة البيانات. وتحدد المادة 10 أن الشخص المستهدف من جمع البيانات يجب أن يعرف الغرض الذي من أجله تم تجميع البيانات وهوية من يقوم بالضبط.

الموقف في فرنسا

وفي فرنسا يشتمل قانون تكنولوجيا المعلومات والحريات المدنية على التعديات على الحق في الخصوصية الناجمة عن سجلات الكمبيوتر أو معالجتها في مدونة العقوبات الفرنسية. وقد استحدثت النسخة المعدلة للقانون لعام 2004 أربعة عشر مادة جديدة ترسي عقوبات أكثر صرامة لإساءة استخدام البيانات الشخصية.

الموقف في الولايات المتحدة الأمريكية

الولايات المتحدة هي أكبر مَصْدَر للبريد الاقتحامي، وفي 1 يناير 2005، قام الكونغرس بسن قانون CANSPAM الذي يمكن من خلاله مقاضاة من يقومون بإرسال هذا البريد. ويحظر القانون (جمع) عناوين البريد الإلكتروني من المواقع الإلكترونية، ويمنع البرامج التي تقوم بتوليد عناوين من خلال (الهجمات المعجمية) التي تقوم عشوائياً بتركيب الحروف والأرقام.

ويعد البريد الاقتحامي أيضاً مشكلة من وجهة نظر المنافسة غير العادلة عندما يتم استخدامه لأغراض إعلانية.

البريد الاقتحامي والإعلان والمنافسة غير العادلة

يتم تنظيم الإعلان على الإنترنت من خلال الأحكام القانونية العامة بشأن الإعلان، وليس من خلال أي إطار قانوني محدد. وفي نوفمبر 2001 قامت اللجنة السويسرية لإقرار العدالة بالاتصال التجاري لاستصدار رأي استشاري بشأن إرسال البريد الاقتحامي، الذي تعتبره على وجه الخصوص طريقة اقتحامية للبيع، ومن وجهة نظر إعلانية، يمكن استخدام هذه الطريقة فقط بالامتثال لمبادئ رئيسية محددة، سواء كان ذلك أثناء القيام بأعمال تجارية تقليدية أو التجارة الإلكترونية.

هذه القواعد هي:

- حماية مستعملي الإنترنت حديثي السن؛
- احترام الإنسان؛
- احترام الإعلان العادل والصادق والأمين؛
- احترام الخصوصية القانونية لمستعملي الإنترنت؛
- سهولة الإبحار.

تنص المادة 3 من القانون الاتحادي السويسري لمكافحة المنافسة غير العادلة: *المنافسة غير العادلة تحدث خاصة عندما يقوم أحد الأشخاص بالآتي:*

[...]

ب- تقديم معلومات غير دقيقة أو حافلة بالمغالطات حول نفسه واسم شركته ومنتجاته وأعماله وخدماته وأسعاره ومخزونه وطريقته في البيع أو التجارة، أو أنه من خلال تقديم مثل هذه المعلومات يقدم ميزة لطرف ثالث تفوق منافسيه؛

ج- عرض أو استخدام ألقاب أو تسميات مهنية بشكل يجعل الآخرين يعتقدون أن لديه مميزات أو قدرات معينة؛

د- اتخاذ تدابير بشكل يؤدي إلى الخلط مع سلع أو أعمال أو خدمات أو تجارة تخص شخصاً آخر."

ولكن النقطة ح من المادة 3 هي التي تصل إلى جوهر المشكلة، فهي تنص على أنه: (*تحدث المنافسة غير العادلة خاصة عندما يقوم أحد الأشخاص:*

[...]

ح- بالحد من حرية الزبون في أن يقرر، وذلك باستخدام طريقة للبيع تكون مقتحمة بشكل خاص.

وعندما يتم استخدام البريد الاقتحامي لأغراض تجارية بالكثافة المذكورة أعلاه، يمكن اعتباره عندئذ داخلاً في نطاق هذه المادة.

البريد الاقتحامي والقصد الإجرامي

عندما يقوم مرسلو البريد الاقتحامي بقصد إجرامي فإنهم يتحملون المسؤولية العقابية، وحتى لو كانت الرسالة ذات طابع تجاري، فإن محتواها قد يعرضهم للمقاضاة.

البريد الاقتحامي والمواد الإباحية

هناك أغلبية من رسائل البريد الاقتحامي تدعو القارئ إلى زيارة مواقع إباحية، ويعد هذا عملاً إجرامياً تحت إطار المادة 197 لمدونة العقوبات السويسرية، وخاصة إذا قامت الرسالة بإتاحة المحتوى لأشخاص لا يرغبون في تلقيه (مادة 197/2) أو لأشخاص أصغر من سن 16 (مادة 197/1).

البريد الاقتحامي والخداع وبيع المواد المحظورة

يعد الخداع عملاً إجرامياً تحت المادة 146 لمدونة العقوبات السويسرية. ويتم تعريفه على أنه الحصول على ميزة مالية من الضحية بهدف الإثراء الذاتي، ومن هذه الزاوية يعد (الخطاب النيجيري) بالتأكيد نوعاً من الخداع.

يمكن أن يكون البريد الاقتحامي أفضل الطرق لإصابة الأجهزة بعدوى الفيروسات. وفي القانون السويسري، إذا نجم عن إدخال فيروس إفساد البيانات (إذا تم تعديل بيانات الضحية أو إزالتها أو جعلها غير قابلة للاستخدام، يمكن ملاحقة من يقومون بإرسال البريد الاقتحامي قضائياً بموجب المادة 144 من قانون العقوبات.

يحظر القانون السويسري استخدام البريد الاقتحامي لبيع الأدوية. فتحظر المادة 32 من القانون السويسري بشأن المنتجات الدوائية والأجهزة الطبية الإعلان الذي يشجع الاستخدام المفرط أو المسيء أو غير اللائق للمنتجات الطبية أو الإعلان عن المنتجات الدوائية التي لا يمكن بيعها في السوق السويسري أو التي لا يمكن الحصول عليها إلا بتذكرة طبية.

3.4.1.IV تنظيم البريد الاقتحامي

هناك طريقتان متعارضتان لتنظيم البريد الاقتحامي هما: نهج اختيار المشاركة ونهج اختيار عدم المشاركة.

ويعد نهج المشاركة الذي يطلق عليه أيضاً تسويق التصاريح، أكثر احتراماً لمستعمل الإنترنت من حيث إنه عبارة عن إرسال الإعلانات الموجهة إليه فقط والتي وافق بشكل صريح على تلقيها، إما من خلال انتقاء أو رفض أحد صناديق الاختيار. ويمكن أيضاً استنتاج الموافقة، ولكن في هذه الحالة يجب أن يتم إخبار الزائر بوضوح بالطابع التجاري وبالنتائج التي تترتب على الاشتراك.

ويتألف نهج اختيار عدم المشاركة من إيقاف الاشتراك وإرساء حق رفض تلقي رسائل لاحقة. ويجب على كل إعلان أن يتيح للمتلقي إمكانية الانسحاب من القائمة. يمكن أن يتم عمل سجلات انسحاب بشكل قانوني (على سبيل المثال بشراء قائمة اشتراك) أو جمعها باستخدام إجراء عشوائي.

وقد وقع اختيار المشرعين السويسريين والأمريكيين على نهج عدم الاشتراك، بينما يميل الاتحاد الأوروبي إلى تفضيل نهج اختيار الاشتراك، كما أظهر ذلك التوجيه 2002/58/EC فيما يتعلق بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية (التوجيه بشأن الخصوصية والاتصالات الإلكترونية).

ونظراً لأن من يقومون بإرسال البريد الاقتحامي يميلون للعمل دون تحديد هوياتهم ومن دول أجنبية، فإن المقاضاة تكون عالية التكلفة ومعقدة وعادة ما تتضمن توكيل محام.

4.4.1.IV وسائل تقنية للتعامل مع البريد الاقتحامي

قيود تقنية

يمكن الحد من تأثير البريد الاقتحامي من خلال وسائل تقنية لتقييد، على سبيل المثال، عدد المتلقين لكل رسالة، وعدد الرسائل لكل مَصْدَر، وعدد الرسائل لكل وحدة زمنية.

القوائم السوداء

تعمل القوائم السوداء على أساس مبدأ أنه يمكن تصنيف البريد الإلكتروني تبعاً لسمعة المخدّم وذلك كمعيار.

وتتأثر سمعة مخدّم البريد الإلكتروني الذي قام مؤخراً بتسليم بريد اقتحامي سلباً من حيث إمكان افتراض أنه سوف يرسل المزيد من البريد الاقتحامي في المستقبل، ويمكن تحديد هوية المخدّم من خلال عنوان بروتوكول الإنترنت الخاص به.

الفلاتر التي تستخدم كلمات بحث أساسية

تقوم الفلاتر القائمة على كلمات بحث أساسية بمنع الرسائل التي تحتوي على كلمات بحث أساسية معينة، ولكنها غير فعالة لأن بإمكان من يقومون بإرسال البريد الاقتحامي أن يتفادوا هذه الفلاتر.

تقنية تكوين بطاقات بيانات شخصية

يتكون البريد الاقتحامي من إرسال أعداد هائلة من رسائل متطابقة، ويتم استخدام تقنية تكوين البيانات الشخصية لتحديد البيان الشخصي لمحتوى الرسالة ومقارنته بقاعدة بيانات للمحتويات التي تعتبر بريداً اقتحامياً.

السياسة العامة لمكافحة البرمجيات الخبيثة

ويجرى استخدام مجموعة متنوعة متزايدة من البرمجيات الخبيثة (الفيروسات وأحصنة طروادة واليرقات، وغير ذلك) من أجل تركيب مخدّمات للبريد على الأجهزة المصابة بالعدوى، والهدف من ذلك هو جعلها أسهل في نشر البريد الاقتحامي. ويعني مكافحة البريد الاقتحامي مطاردة البرمجيات الخبيثة.

يمكن لبرامج مكافحة البريد الاقتحامي المساعدة في فلترة ومنع البريد الاقتحامي على مستوى مخدّم البريد الإلكتروني، وهكذا يمكن الحد من انتشاره، ولكن هذه الطريقة ليست دوماً فعالة، فلا تصل الرسائل الصحيحة للمتلقين (مفهوم الإيجابيات الزائفة) بينما يصل البريد الاقتحامي الحقيقي (مفهوم السلبيات الزائفة).

إن موقف المستعمل هو أحد الجوانب الأساسية في مكافحة البريد الاقتحامي، حيث يمكن الحد من نطاق المشكلة على سبيل المثال إذا تعامل المستعملون مع الرسائل بدراية (يجب أن يكونوا واعين بمخاطرة سرقة الهوية، والتحقق من كيفية استخدام عناوين بريدهم الإلكتروني قبل إدخالها في نموذج بيانات إلكتروني، واستخدام العديد من عناوين البريد الإلكتروني، وتجنب مواقع معينة، وتعلم عدم فتح رسائل من مرسلين غير معروفين، وحذف البريد الاقتحامي بدون قراءته، وعدم الرد أو الضغط على الإطلاق على أية وصلات فوقية داخل رسالة البريد الاقتحامي وغير ذلك).

5.4.1.IV التكامل ما بين الوسائل التقنية والقانونية

نظراً لأن الوسائل القانونية ليس لها إلا تأثير ضعيف على انتشار البريد الاقتحامي، فهناك حاجة لحل تقني. ويمكن مكافحة ظاهرة البريد الاقتحامي فقط من خلال استخدام كل من الوسائل التقنية والقانونية. ويعني الفت في عضد أي ممن يرسلون البريد الاقتحامي، وذلك من خلال قواعد القانون أو منعهم من القيام بذلك من خلال حل تقني يحول دون إرسال الملايين والملايين من الرسائل.

5.1.IV موجز بالمسائل القانونية الأساسية المتصلة بالفضاء السيبراني[61]

1.5.1.IV الوضع القانوني لشبكة الإنترنت التجارية

يتم تعريف الوضع القانوني لشبكة الإنترنت التجارية من خلال الحالة القانونية لأدوات تكنولوجيا المعلومات المستخدمة.

بالنسبة للبريد الإلكتروني، فإن الجدل يدور حول محتوى الرسالة وعنوان صندوق البريد وحقيقة أن العنوان يمكن أن يستخدم لتحديد –أو لسرقة– هوية أو علامة مميزة أو اسم الشركة، ويتم تنظيم هذه النقاط من خلال القانون المدني لكل بلد.

وبالنسبة لمواقع الويب، يثير مفهوم العمل سواء كان سمعياً–بصرياً أم لا مسائل تتعلق بحقوق المؤلف، وتثير الصلة الفوقية تساؤلات حول المحتوى والمسؤولية وما إذا كانت محمية أم لا، والمشاكل المتعلقة بمحركات البحث.

2.5.1.IV العقود السيبرانية

يثير إبرام العقود في الفضاء السيبراني ليس فقط مسائل قانونية وإنما يتطلب أيضاً وجود آليات تقنية لإبرام العقود بالفعل (الأدوات والإجراءات المستخدمة: العالمية وكونها غير ملموسة وعدم كونها في مكان بعينه).

النقاط الآتية مهمة من وجهة نظر قانونية:

- العرض وحالته (عن بعد أم لا) وقبوله؛
- الإعلان والطلب والبريد الاقتحامي وغير ذلك؛
- الأداء؛
- قبول العرض على الخط، وتكنولوجيا المعلومات المستخدمة لتشير إلى القبول؛
- حق الانسحاب؛
- اختيار القانون والولاية القضائية.

[61] كُتب هذا القسم بالتعاون والتضافر مع إيجلي تاشي، وهو معيد في قسم الدراسات العليا في جامعة لوزان.

يتم تنظيم هذه النقاط من خلال العديد من التوجيهات الأوروبية ألا وهي:

- اللائحة التنظيمية للمجلس الأوروبي رقم 44/2001 بتاريخ 22 ديسمبر 2000 بشأن الولاية القضائية للسلطات القضائية والاعتراف بالأحكام وإنفاذها في الأمور المدنية والتجارية؛
- التوجيه 2000/31/EC بشأن التجارة الإلكترونية؛
- التوجيه 98/34/EC المؤرخ في 22 يونيو 1998 الذي يحدد إجراءاً لتقديم المعلومات في مجال المعايير واللوائح التنظيمية التقنية؛
- التوجيه 97/7/EC بشأن حماية المستهلكين بالنسبة للعقود عن بعد.

ويتصل بذلك أيضاً نموذج القانون لعام 1996 لهيئة الأمم المتحدة بشأن قانون التجارة الدولية حول التجارة الإلكترونية، والإعلان الوزاري لمنظمة التجارة العالمية لعام 1998 بشأن التجارة الإلكترونية والبيان المشترك بين الولايات المتحدة والاتحاد الأوروبي لعام 1997 بشأن التجارة الإلكترونية.

3.5.1.IV الوثائق والتوقيعات الإلكترونية

تثير الوثائق الإلكترونية التي يتم توقيعها إلكترونياً مسائل تتعلق بصلاحيتها. والغاية من ذلك هي القدرة على ضمان الصحة القانونية للتوقيع من أجل تحديد هوية الموقع وللتأكد من اعتزامه التوقيع على الوثيقة وبالتالي تَحمُّل مسؤولية مضمونها.

وهناك أمثلة لنصوص قانونية متعلقة بذلك وهي التوجيه 1999/93/EC بتاريخ 13 ديسمبر 1999 على إطار عمل للجماعة بشأن التوقيعات الإلكترونية (الاتحاد الأوروبي)، قانون رقم 59 بتاريخ 15 مارس 1997 في إيطاليا، وقانون التوقيعات الإلكترونية في التجارة العالمية والقطرية في 30 يونيو (في الولايات المتحدة) وقانون الاتصال الإلكتروني في 15 مايو 2000 (المملكة المتحدة).

4.5.1.IV المدفوعات الإلكترونية

يمكن اعتراض سبيل عمليات الدفع الإلكتروني التي تتضمن كروت الائتمان أو الشيكات أو النقود الإلكترونية من خلال طرف ثالث، على سبيل المثال عندما يتخاطب مقدم الخدمة مع المتلقي ويتم إساءة استخدام المعلومات المتعلقة.

انظر المقرر 2000/46/EC بتاريخ 18 سبتمبر 2000 بشأن اتخاذ والتماس إشراف قانوني لأعمال مؤسسات النقود الإلكترونية وذلك كمثال على نص قانوني.

5.5.1.IV حماية أسماء الميادين

تعتبر أسماء الميادين صورة جديدة من الأصول غير الملموسة التي يمكن أن يكون لها قيمة تجارية كبيرة، ولا بد أن يتم النظر فيها من حيث كيفية اتصالها بما يلي:

- العلامات التجارية وأسماء الميادين؛
- العلامات المُميِّزة؛
- أسماء الأعمال التجارية وأسماء الميادين؛

هذا بالإضافة إلى التشريع الوطني بشأن العلامات التجارية والأسماء وبراءات الاختراع، ومما يتعلق بهذا القانون الأمريكي لحماية المستهلكين من الاستقطان السيبراني (ACPA).

6.5.1.IV الملكية الفكرية

تثير الملكية الفكرية على الإنترنت مسائل تتعلق بحقوق المؤلف والعلامات التجارية وبراءات الاختراع. ويكفي ذكر اتفاقية WIPO لحقوق المؤلف واتفاقية WIPO لحقوق للعروض الفنية والصوتيات، وفي التشريع الأوروبي الورقة الخضراء لعام 1995 بشأن حقوق المؤلف والحقوق المتعلقة بمجتمع المعلومات والتوجيه 2001/29/EC للبرلمان الأوروبي وللمجلس المؤرخة في 22 مايو 2001 بشأن التوفيق بين جوانب معينة لحقوق المؤلف والحقوق المتعلقة في مجتمع المعلومات.

7.5.1.IV حماية الخصوصية الرقمية

يعد إرسال البريد الاقتحامي تعدياً على الحق في الخصوصية الرقمية (انظر التوجيه 97/7/EC بشأن حماية المستهلكين فيما يتعلق بالعقود عن بعد والتوجيه 97/66/EC فيما يتعلق بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات، مما يحظر التسويق المباشر باستخدام البريد الاقتحامي.

8.5.1.IV مسائل قانونية أخرى

من بين المسائل القانونية العديدة الأخرى التي يجب النظر فيها عند تحديد الإطار القانوني المناسب لاستخدام الإنترنت أسئلة مثل ما يلي:

- تشريع حماية التجارة من التكتلات (انظر الخطوط التوجيهية لحماية التجارة للتعاون بين المتنافسين في الولايات المتحدة أبريل 2000)؛
- مسؤولية الموردين والوسطاء التقنيين (إلى أي مدى يعد المورد مسؤولاً عن أنشطة مستعمل الإنترنت، والأنشطة الإجرامية، والمواد الإباحية للأطفال وغير ذلك)؛
- عدم إمكانية مخالفة السرية البريدية.

القسم 2.IV – توقعات

1.2.IV ثقِّف ودرِّب وزد الوعي لدى جميع أصحاب المصلحة في الأمن السيبراني

من المهم جعل كل أصحاب المصلحة في الإنترنت واعين بأهمية مسائل الأمن المتضمنة، وبالتدابير الأساسية التي إذا تم بيانها بوضوح وتنفيذها بفهم فإنها تعزز ثقة المستعمل في معالجة البيانات وتقنيات الاتصالات، بما في ذلك الإنترنت. ويجب أن تكون الإنترنت مِلكاً للجميع وليست حكراً لمنفعة الأنشطة الإجرامية.

ويجب اتخاذ خطوات لرعاية ثقافة ونهج متعدد التخصصات للأمن ومكافحة خطر استخدام تكنولوجيا المعلومات في أهداف إجرامية، ويجب أن تكون هناك رؤية استراتيجية لهذه المشكلات لدى الدول والمنظمات.

ويجب أن يتم توفير التعليم والمعلومات والتدريب حول معالجة البيانات وتقنيات الاتصالات، وليس فقط في الأمن والروادع. ولا يجب أن يقتصر رفع الوعي بمسائل الأمن على الترويج لثقافة الأمن، حيث لا بد أن يكون هناك أولاً ثقافة تقنية المعلومات. ولا بد أن يتم إعطاء أصحاب المصلحة الوسائل لتعلم إدارة المخاطر التقنية والتشغيلية والمعلوماتية التي يتعرضون لها خلال استخدامهم للتقنيات الجديدة.

ويمكن للطبيعة الخائلية للإنترنت وأبعادها الترفيهية أن تعمي خاصة صغار السن من المستعملين وحديثي الاستخدام بصفة خاصة عن قدرتها التي لا يستهان بها لإلحاق الضرر. ويمكن أن تكون التداعيات المخيفة سواء للمنظمات (الشركات والمنظمات الإدارية أو الاجتماعية) والأفراد الذين يقعون ضحية لها. يعني التحكم في المخاطر التقنية أكثر

من مجرد مطاردة المتسللين أو إنشاء حواجز تقنية. وأحياناً تكون أخطر التداعيات ناجمة عن مجرد الإهمال الناتج عن نقص الكفاءة أو التقنيات التي لا يتم إدراكها أو تطبيقها بشكل جيد، والصلاحية المفرطة لمديري النظام وسوء الإدارة وغير ذلك.

2.2.IV نهج جديد نحو الأمن

يجب أن يثير الوعي بتعرض العالم الرقمي، وبالصعوبات الجوهرية الكامنة في طبيعة تقنيات المعلومات والاتصالات والبنى الأساسية وكذلك في حلول الأمن التي يتم الترويج لها، أسئلة خطيرة بشأن اعتمادنا على تقنية من الصعب إدارتها. ولا يمكن تجاهل أخذ البيانات كرهينة بواسطة أنظمة تكنولوجيا المعلومات كأمر حتمي لا يمكن تجاهله.

ومن قبيل التمني الاعتقاد أن الحلول القانونية والتقنية تعوض عن الأخطاء المفاهيمية والإدارة الضعيفة لتقنية المعلومات والاتصالات، سواء كان ذلك على المستوى الاستراتيجي أو التكتيكي أو التشغيلي، والأكثر من ذلك إنه لا يمكن لتدابير الأمن التقليدية حماية الموارد الحساسة أو الرئيسية للأشخاص والمنظمات والدول إلا إذا تم تنفيذها بطرق تتسم بالشفافية وإمكانية التحقق والرقابة.

إن إرساء نهج شامل للأمن مُتضمِّناً المنع والحماية والدفاع ورد الفعل يعني تبني الوسائل البشرية والقانونية والتقنية والاقتصادية اللازمة للقيام بذلك.

3.2.IV خصائص السياسة العامة للأمن

إن السياسة العامة السليمة للأمن هي نتاج تحليل للمخاطر، وهي شاملة ومتماسكة وتقدم استجابة موجهة لاحتياجات الأمن في سياق بعينه.

ويجب أن تكون هذه السياسة العامة:

- بسيطة ويسهل فهمها؛
- يمكن تنفيذها على أيدي العاملين المدربين واليقظين؛
- يسهل تنفيذها؛
- تسهل صيانتها؛
- يمكن التحقق منها والرقابة عليها.

يجب ألا تكون سياسة الأمن استاتيكية، حيث لا بد أن يتم مراجعتها بشكل دوري والوصول بها إلى الشكل الأمثل، وتعديلها بحيث تتلاءم مع التطورات في السياق الذي تُنفَّذ فيه، ويجب أن يكون بالإمكان تشكيلها وتعديلها حسب الطلب طبقاً لبطاقات بيانات بالمستعملين، وذلك في ضوء التدفقات والسياق والمكان الجغرافي لأصحاب المصلحة، وأن تتغير سياسة الأمن حسب الوقت والمكان.

ويجوز تفكيك السياسة العامة للأمن إلى سياسات فرعية لضبط النفاذ والحماية، وإدارة الأزمات والمتابعة، والوصول إلى الوضع الأمثل والثقة.

4.2.IV تحديد الموارد الحساسة من أجل حمايتها

يمكن الحصول على صورة أوضح للبيئات واحتياجاتها للحماية من خلال عمل قائمة جرد كاملة ودقيقة لكل الموارد والناشطين في سلسلة الأمن. ويتم تحديد قيم مختلف فئات الموارد من أجل تحديد مدى حساسيتها (أو أهميتها)، وبالتالي إعطاء الأولوية لأي منها لتأمينه. وتعتمد درجة الحساسية على النتائج التي تحدث في حالة ما إذا تم فقد البيانات أو تم تغييرها أو إفشاؤها. وكلما ازدادت الخطورة على المنظمة، كلما زادت حساسية وقيمة المورد.

ويعتبر كل مورد هدفاً أمنياً، ويجب تحديد المخاطر ذات الصلة وكيف تنشأ (خلال خطأ المستعمل أو خطأ في تحديد المعلمات، أو بالصدفة، أو من خلال الاستخدام الخبيث أو التخريب أو الهجمات المنطقية أو غير ذلك) كما أن آليات الأمن الداخلية والقابلة للتنفيذ (التشكيل والمعلمات وغير ذلك)، وكذلك العقبات التقنية والتنظيمية ينبغي تعريفها من أجل تحديد الجدوى التقنية والتنظيمية للسياسة العامة للأمن لكل هدف من الأهداف.

5.2.IV الأهداف والرسالة والمبادئ الرئيسية للأمن السيبراني

أهداف الأمن السيبراني هي:

- السرية (بدون نفاذ غير مشروع): للحفاظ على سرية المعلومات وقصر النفاذ على الجهات المصرح لها؛
- السلامة والدقة (بدون معلومات زائفة وبدون أخطاء)، وذلك للحفاظ على سلامة البيانات والبرامج وعدم فساد حالتها؛
- التوافر (بدون تأخير): للحفاظ على التوافر بشكل مستمر وبدون انقطاع أو تدهور؛
- طول العمر (بدون تدمير): وذلك للحفاظ على البيانات والبرمجيات للفترة المطلوبة؛
- عدم الرفض والاستدلال على الفاعل (بدون نزاعات): لضمان الأصل والمنبع والوجهة والصدق في كل التصرفات؛
- احترام الخصوصية الرقمية؛
- الاستيقان (بدون شك يكتنف هوية المورد).

يمكن تفكيك كل رسالة إلى الأنشطة الرئيسية المكونة لها:

- بلورة خطة أمنية قائمة على تحليل سابق للمخاطر؛
- تحديد محيط التعرض الذي ينشأ عن استخدام تقنيات جديدة؛
- الحماية المستمرة على مستوى مكافئ للأخطار التي يتم التعرض لها؛
- التنفيذ والتحقق من البنية والتدابير والأدوات والإجراءات الخاصة بالأمن؛
- متابعة ومراقبة وضبط وتطوير نظام المعلومات والأمن به؛
- الوصول إلى الوضع الأمثل لأداء نظام المعلومات جنباً إلى جنب مع مستوى الأمن المطلوب؛
- التوفيق بين الاحتياجات وبين المخاطر والتكاليف.

المبادئ الأساسية المساندة لأي إجراء للترويج للأمن السيبراني هي كما يلي:

- المعجم (الحاجة إلى الاتفاق على لغة مشتركة في تعريف الأمن)؛
- التماسك (الأمن السيبراني هو ما ينتج عندما يتم إدماج الأدوات والآليات والإجراءات المطلوبة لمنع واكتشاف والحماية من الأخطاء والأشياء الضارة أو العوامل الطبيعية وإصلاح الضرر الناجم عنها بشكل متناغم؛
- الإرادة الإدارية (تقع المسؤولية على الإدارة لإتاحة الوسائل المطلوبة لتنفيذ وإدارة خطة الأمن السيبراني)؛
- النواحي المالية (لا بد من حساب تكلفة الأمن وتدابير الضبط بالمقارنة بالمخاطر)؛
- البساطة والعالمية والصدق (لا بد أن تكون تدابير الأمن بسيطة ومرنة ويسهل على المستعملين فهمها ولا يجب أن تكون مثيرة لئلا تغري المهاجمين المحتملين)؛

- التغير والاستمرارية (لا بد أن يكون الأمن دينامياً من أجل إدماج تعديلات الأنظمة مع مرور الوقت والاحتياجات والمخاطر المتغيرة، ولا بد أن تكون الأنظمة قيد التشغيل دائماً)؛
- التقييم والضبط والتكيف (من أجل كفالة أن مستوى الأمن متوافق مع الاحتياجات الحقيقية).

6.2.IV عوامل النجاح

1.6.2.IV الخطوط التوجيهية للاستراتيجية

يتطلب التنفيذ الناجح لاستراتيجية الأمن ما يلي:

- إرادة استراتيجية؛
- سياسة أمن بسيطة ودقيقة ويمكن فهمها وتنفيذها؛
- نشر سياسات الأمن العامة؛
- إدارة أمن مركزية وتحقيق درجة من الأوتوماتية في الإجراءات الأمنية؛
- الثقة والتكامل فيما بين الأشخاص والأنظمة والأدوات المستعملة؛
- إجراءات التسجيل والمراقبة والتدقيق؛
- التصميم على عدم تعريض الموارد للخطر؛
- إطار قانوني يمكن تطبيقه على المستوى الوطني والدولي؛
- احترام الموانع القانونية.

2.6.2.IV خطوط توجيهية لمستعملي الإنترنت

تمثل الخطوط التوجيهية التالية تدابير بسيطة واقتصادية وفعالة إلى حد ما يمكن لمستعملي الإنترنت تبنيها لجعل مواردهم وأنشطتهم الإلكترونية أكثر أمناً[62]:

- إغلاق الكمبيوتر في حالة عدم التشغيل؛
- عدم فتح رسائل البريد الإلكتروني الواردة من مرسلين غير معروفين؛
- استخدام برنامج لمكافحة الفيروسات يتم تحديثه بشكل منتظم لتحقيق القدر الأدنى من الحماية؛
- لا تُفش كلمة المرور الخاصة بك وداوم على تغييرها؛
- لا تفش بيانات شخصية عن نفسك أو عن الآخرين على الإنترنت؛
- لا تسمح أبداً لأي شخص آخر باستخدام حسابك لتَصفُحْ الإنترنت؛
- استخدم أنظمة التجفير لحماية البيانات؛
- لا تزر مواقع غير أخلاقية، ولا تقم بإنزال أو تعميم برامج أو ملفات غير قانونية؛
- لا تنخرط في أفعال على الإنترنت تكون محظورة ويعاقب عليها في العالم غير الخائلي (مثل الخداع والتشهير وما إلى ذلك)؛
- لا تتراخى بشأن مستوى الحماية الموجود لديك؛
- ضع في اعتبارك أنه – مثلما هو الحال في العالم الحقيقي–فإن أي عمل هو من صنع شخص ما، وأن هذا الشخص قد لا يكون أميناً.

---

62 توقعات مستمدة من "Sentiment de sécurité sur Internet" ورقة بحثية مقدمة في إطار دراسات عليا عن القانون والجريمة والأمن، من إعداد Anne-Sophie Perron، تحت إشراف غرناؤطي–هيلي، لوزان، 2005.

3.6.2.IV خطوط توجيهية لتأمين نظام بريد إلكتروني

يمكن لهذه الخطوط التوجيهية الأساسية أن تحمي نظاماً للبريد الإلكتروني.

قم بحماية المخدّم من خلال:

- استخدام برنامج لمكافحة الفيروسات؛
- فلترة الرسائل باستخدام معايير معينة قابلة للقياس (الحجم والمرفقات وغير ذلك)؛
- شكل النظام صحيح؛
- أدْرهُ بشكل فعال من أجل ضمان توافره؛
- تجنب حسابات الصيانة بالتغيب؛
- وفرة حماية مادية له.

بالنسبة للمستعمل:

- ركب، وأدره، وأفرض استخدام برنامج لمكافحة الفيروسات؛
- عرِّف قواعد استخدام نظام إدارة الرسائل (لا تقم بفتح ملفاً قابلاً للتنفيذ وغير ذلك)؛
- عمِّق الوعي بالأخطار الممكنة؛
- احصل على تعهد بالاستخدام السليم لموارد تكنولوجيا المعلومات؛
- شكِّل بطريقة سليمة كل وحدة عمل خاصة بالمستعمل وتطبيق الرسائل؛
- نفِّذ نسخاً آمنة من نظام البريد الإلكتروني؛
- استخدم تدابير التحفير للرسائل السرية والاستيقان من المصادر.

4.6.2.IV خطوط توجيهية لحماية بيئة الإنترنت والإنترانت (الشبكة الداخلية)

سوف تساعد الخطوط التوجيهية الأساسية التالية بشأن استخدام حوائط النيران في حماية بيئات الإنترنت والإنترانت:

- لا بد من حماية وتأمين حوائط النيران ضد النفاذ غير المصرح به (مفهوم النظام الموثوق به الذي به نظام تشغيلي آمن)؛
- لا بد أن تتوقف كل حركة البيانات (الصادرة والواردة) عبر حائط النيران؛
- يجب السماح فقط للمرور الذي يتم تعريفه على إنه صالح ومصرح به بعبور حائط النيران؛
- لا بد أن يتم تشكيل حائط النيران بفلترة كل شيء لم يتم التصريح له صراحة؛
- لا يمكن أن يكون حائط النيران في نفس الوقت هو المخدّم الشبكي للشركة؛
- إذا كانت البيانات الموجودة في الشبكة الداخلية على درجة عالية من الحساسية، فلا بد أن يكون النفاذ إلى الإنترنت من خلال أجهزة غير متصلة بالشبكة الداخلية؛
- لا يمكن أن يقوم حائط النيران بتأمين البيئة ضد الهجمات أو النفاذ غير المشروع الذي لا يمر من خلاله، وهو غير فعال ضد الجرائم التي يتم ارتكابها من داخل الشركة.

ليس حائط النيران مضاداً للفيروسات، لذا لا بد أن يكون محمياً ضد الفيروسات، ويجب أن يكون كل نظام يقدم توصيلية (مخدّمات البريد الإلكتروني ومخدّمات الاتصالات وما إلى ذلك) بصورة مطلقة، وكل جهاز يحتوي على بيانات (أرشيف أو مخدّم لقاعدة بيانات أو غير ذلك) وكل وحدة عمل لمستعمل مزوداً ببرمجيات مضادة للفيروسات.

الجـــزء V

الملحقات

الملحق A – مسرد مصطلحات الأمن الرئيسية[63]

مراقبة النفاذ (Access control)

آلية الغرض منها حماية مورد (خدمة، نظام، بيانات أو برنامج) من الاستخدام غير المناسب أو غير المرخص به.

حادثة (Accident)

حادث غير متوقع يسبب ضرراً لكيان ما.

هجوم فعال (Active attack)

هجوم يغير من الموارد التي يستهدفها (يضر بالسلامة، أو التوافر أو السرية).

الغُفلْية (Anonymity)

وهي تميز كياناً ما غير معروف الاسم أو لا يكشف عن اسمه، ويسمح لكيان أن يستخدم الموارد دون أن يكون معروف الهوية (غُفْلاً) وينبغي النص على احترام رغبة مستعملين معينين قد يكون لديهم سبب وجيه لعدم إماطة اللثام عن هوياتهم عند الإدلاء ببيانات على الإنترنت، وذلك لتفادي التقييد الزائد عن الحد لحريتهم في التعبير، ولتشجيع التعبير الحر عن الأفكار والمعلومات، ولضمان الحماية من المراقبة غير المرخص بها على الشبكة من جانب كيانات عامة وخاصة. ومن ناحية أخرى، ينبغي للسلطات القضائية والشرطية أن تكون قادرة على الحصول على المعلومات عن الأفراد المسؤولة عن ارتكاب أنشطة غير قانونية، وذلك داخل الحدود التي يحددها القانون الوطني، والاتفاقية الأوروبية لحقوق الإنسان والمعاهدات الدولية الأخرى مثل الاتفاقية بشأن الجريمة السيبرانية.

مضاد الفيروس (Antivirus)

برنامج الكشف عن الفيروسات.

أصول (Asset)

شيء له ثمن ويمثل شكلاً ما من أشكال رأس المال (مفهوم الأصل الحساس). ومن المهم – أمنياً – تحديد الأصول وتصنيفها تدريجياً حسب الأهمية، وذلك لتنفيذ التدابير المطلوبة للحماية وبذلك يمكن تفادي فقدانها أو على الأقل لتدنية التأثير الضار الناجم عن فقدها إلى أبعد حد.

الخوارزمية التجفيرية اللاتناظرية (Asymmetric cryptographic algorithm)

خوارزمية تستند إلى استخدام زوج من المفاتيح (أحدهما لتجفير البيانات والآخر لإزالة التجفير).

هجوم (Attack)

اعتداء، عدوان أو عمل ضدي أو يسبب ضرراً لأفراد أو موارد. وهناك أنواع مختلفة من الهجمات ذات الصلة بالحاسوب.

---

[63] مقتبس بتصرف من المسرد الوارد في "*Securité informatique et réseaux, cours et exercices corrigés*"، س. غرناؤطي–هيلي، دنود 2006.

القابلية للتدقيق (Auditability)

مدى قابلية بيئة للخضوع لتحليل لغرضي التحليل والتدقيق.

مدقق (Auditor)

شخص يجري تدقيقاً.

الاستيقان (Authentication)

عملية الاستيقان. والغرض من الاستيقان هو لتأكيد (أو لدحض) أن عملاً ما، إعلاناً ما، أو معلومة ما يقينية (أصلية، حقيقية). والعملية المستخدمة بصفة خاصة للتأكد من صحة هوية كيان ما ولضمان توافقها مع هوية سجلت سلفاً لذلك الكيان.

الوثاقة (Authenticity)

صِبْغَة ما هو وثيق. وهذه الخاصية تسمح بالإشهاد (التصديق) أو اعتماد الصحة. وغالباً ما تكون مرتبطة بحقيقة أن معلومة ما أو واقعة ما لم تخضع لتغيير أو تعديل أو تزوير، وأنها في الحقيقة من نتاج الكيان الذي يدعي أنه هو الذي أنشأها.

سُلْطَة (Authority)

جهاز مخول له ممارسة وظائف محددة. وتستخدم عامة لتشير إلى جهاز مُكَلف بإصدار شهادات رقمية.

الترخيص (Authorization)

عمل الترخيص، السماح أو التفويض. إِذْنْ بالقيام بأعمال معينة، منح حقوق، حصول على حق النفاذ إلى خدمة، معلومات، نظام ما إلخ.

التوافر (Availability)

معيار أمني تكون الموارد بمقتضاه متوافرة وقابلة للاستخدام لكي تفي بالمتطلبات (عدم رفض نفاذ مرخص به إلى أنظمة، خدمات، بيانات بنية تحتية، إلخ).

الباب الخلفي، باب المصيدة (Backdoor, trapdoor)

يشير عادة إلى جزء من شفرة مدرجة في برمجيات يسمح لكيانات غير مرخص لها بالتحكم في الأنظمة، واستنساخ معلومات، إلخ بدون علم صاحب الشيء.

خطة مساندة (Backup plan)

مجموعة الوسائل التقنية والتشغيلية المتنبأ بأنها تضمن استدامة المعلومات واستمرارية النشاطات، مهما كانت المشاكل التي تظهر.

خرق (Breach)

هو التأثير الناجم عن، أو التدهور الناتج من عمل اعتدائي أو هجوم قد يكون تأثيره: ملموساً (تغيير مادي، تعطل منطقي، تشتيت التدابير، إلخ)، منطقي (عدم التوافر، فقدان السلامة، خرق السرية)؛ استراتيجي (وبخاصة ما يتعلق بالمالية، أو بتكاليف إضافية للاستضافة، للنقل أو للاتصالات، للدراية، لبيع/استئجار عتاد أو برمجيات، موظفين، إسناد مهام لجهة خارجية، خسائر تشغيلية (هامش ربح، سيولة نقدية، خسائر زبائنية)، فقدان أموال أو سلع، إلخ).

بَقْ (Bug)

خطأ برنامجي. بالتناظر، عيب مفاهيمي أو في التنفيذ يكشف عن طريق الأعطال.

شهادة، شهادة مفاتيح عمومية (Certificate, public-key certificate)

مجموعة بيانات صادرة عن سلطة اعتماد (طرف ثالث موثوق به) وتستخدم لتقديم خدمات أمن (سرية، استيقان، سلامة). وتستخدم الشهادة الرقمية التجفير بمفاتيح عمومية. وتشتمل الشهادة على قيمة المفتاح العمومي للموضوع، الذي يشهد بصحته ذلك التوقيع على الشهادة من جانب السلطة المصدرة للشهادة.

سلطة إصدار الشهادة (CA)

طرف ثالث موثوق به لإنشاء شهادات المفاتيح العمومية والتوقيع عليها ونشرها.

كبير مسؤولي الأمن (CSO)

الشخص المنوط به أمن أنظمة تكنولوجيا المعلومات.

مُجَفرة (Cipher)

خوارزمية تجفير تستخدم لتحويل نص عادي إلى نص مجفر.

نص مجفر (Ciphertext) – انظر *Cryptogram*

الامتثال (Compliance)

التوافق، الاتفاق مع؛ الامتثال للمقاييس.

السرية (Confidentiality)

الاحتفاظ بسرية المعلومات والمعاملات. طبيعة ما هو سري. هدف أمني يرمي إلى منع إفشاء المعلومات إلى أطراف ثالثة غير مرخص لها، كما يرمي إلى حماية تلك المعلومات من مطالعتها، التصنت عليها أو استنساخها بصورة غير قانونية، سواء بالصدفة أو عمداً، وذلك أثناء تخزينها أو معالجتها أو نقلها (مفهوم سرية البيانات).

كوكيز (Cookies)

ملفات مكتوبة للملف المطبوع الخاص بمستخدم الإنترنت بدون علمه، عندما ينفذ إلى المواقع الشبكية، وتقوم هذه الملفات بجمع بيانات عن المستخدمين بغرض مبدئي هو تسخير خدمات الويب المعروضة بما يتناسب مع ما يريدون.

إجراء مضاد (Countermeasure)

دالة، أو إجراء أو تدبير أو آلية لأمن النظام ترمي إلى تقليل مستوى التعرض والتصدي لتهديد قبل أن يتجسد في الواقع.

تحليل التجفير (Cryptanalysis)

مجموعة طرائق تستخدم لتحليل معلومات مجفرة سلفاً لإزالة التجفير عنها، ويشار إلى تحليل التجفير أيضاً لـــ"فك الشفرة "decoding". وكلما كان التجفير متيناً كلما ازداد تحليل التجفير صعوبة.

نص مجفر (Cryptogram, ciphertext)

بيانات متحولة بالتجفير. بيانات، نص أو رسالة مجفرة. بيانات تحصلت بالتجفير.

خوارزمية تجفيرية (Cryptographic algorithm)

خوارزمية مستخدمة في تجفير البيانات لجعل البيانات سرية، وهي مبنية على دالة رياضية ومفتاح تجفير.

فترة تجفيرية (Cryptographic period)

فترة زمنية لا تتغير أثناءها مفاتيح نظام ما.

التجفير (Cryptography)

التطبيق الرياضي المستخدم لكتابة المعلومات بطريقة تجعلها غير مفهومة لأولئك الذين لا تتوافر لديهم سبل إزالة التجفير. أنظر *Encryption*.

إنكار شامل للخدمة (DDoS)

هجوم تشبعي (أو إنكار الخدمة) يُشنْ من عدة أنظمة في آن واحد.

دايجست (Digest)

سلسلة من الحروف تتشكل عند استخدام دالة البصمة (hash) على سلسلة من البيانات.

التوقيع الرقمي (Digital signature)

بالتناظر مع التوقيعي اليدوي، يستخدم التوقيع الرقمي الذي يتم الحصول عليه عن طريق خوارزمية تجفير لا تناظرية في التحقق من هوية وصحة مرسل رسالة، وللتأكد كذلك من سلامة الرسالة.

خسائر مباشرة (Direct losses)

خسائر يمكن تحديدها تنتج مباشرة عن عيب في الأمن.

تثبيط (Dissuasion)

وسائل تستخدم لردع مهاجمين خبثاء من تنفيذ هجوم، وذلك عن طريق إقناعهم بأن النفع الذي قد يعود عليهم لا قيمة له مقارنة بالخسائر التي ستلحق بالنظام الذي يهددون بمهاجمته.

إنكار الخدمة (DoS)

هجوم تشبعي يرمي إلى انهيار الهدف بحيث يتوقف عن أدائه المتوقع.

الكفاءة (Efficiency)

نوعية ذلك الشيء ذي الأثر المتوقع، الذي ينتج نتائج مفيدة. خاصية تدابير الأمن المناسبة والتي لديها قدرة حقيقية على حماية مورد.

خطة طارئة (Emergency plan)

مجموعة الوسائل التقنية والتنظيمية المتنبأ لها بالاستجابة المثلى إزاء حادث خطير مضر بالمنظمة ومضر بالأداء السلس للعمليات.

التجفير (Encryption, encipherment)

التحويل التجفيري للبيانات (الكتابة المجفرة) لضمان السرية. ويتألف التجفير من جعل البيانات غير مفهومة لأي شخص ليس لديه مفتاح فك التجفير. ويتم تجفير النص العادي باستخدام خوارزمية ومفتاح تجفير لإنشاء نص مجفر يمكن حل تجفيره باستخدام مفتاح مناظر خاص يفك التجفير (باستثناء الحالات التي يكون التجفير فيها نهائياً لا رجعة فيه). وتسمى العملية المعاكسة فك التجفير أو إزالة الشفرة.

أخلاقيات (Ethics)

وهي قواعد لضبط التعامل مع ما هو صالح أو طالح. مجموعة القواعد الأخلاقية التي يتبناها مجتمع ما.

عُطل (Failure)

تعطل، انهيار يجعل المورد غير متاح.

حائط نيران (Firewall)

عتاد أو برمجيات تُسْتخَدم لعزل أو لتقنيع الموارد، ولتصفية البيانات، والتحكم في الدفقات، ومن ثم حماية بيئات المعلومات أو المنظمات الخاصة المرتبطة بالإنترنت.

التوهيج (Flaming)

تقنية تتكون من إرسال عدد كبير من الرسائل البذيئة لتقويض مصداقية فريق مناقشة.

مَسْرَبْ فيضاني (Flooder)

برنامج خبيث يستخدم لإبطاء الاتصالات بين مقدم النفاذ ومستعمل الإنترنت أو لقطع الاتصال مع المستعمل.

متسلل (Hack, hacker)

عملية دخول نظام بطريقة غير قانونية. شخص يدخل – بغض النظر عن سبب الدخول – إلى نظام شخص أخر بدون ترخيص وبصورة غير قانونية. ويمكن أن يكون هذا الهجوم سلبياً أو إيجابياً.

التسلل (Hacking)

سلسلة العمليات التي تستخدم لخرق نظام لتكنولوجيا المعلومات.

دالة البصمة (Hash function)

وفي سياق التجفير، يشار إلى هذه الدالة أيضاً على أنها دالة ترتيب اختزالي (digest function). تبدأ من بيانات الرسالة ثم تعد موجزاً لها أي نوعاً من بصمة الإصبع الرقمية تكون أقصر من الرسالة الأصلية وغير مفهومة. ثم تُجفَر هذه البصمة بالمفتاح الخصوصي للمرسل، وترفق بالرسالة المراد إرسالها. ولدى تلقي الرسالة والبصمة الخاصة بها المتلقي بفك تجفير البصمة بواسطة المفتاح العمومي للمرسل، وإعادة حساب بصمة الإصبع من الرسالة الواردة باستخدام نفس دالة البصمة، ثم مقارنتها بالبصمة الواردة. فإذا كانت النتيجة واحدة، يكون المتلقي قد تحقق من صحة هوية المرسل وتأكد من سلامة الرسالة، حيث إنه لو كانت الرسالة قد غيرت ولو قليلاً تكون بصمتها قد تعدلت كثيراً.

تحديد الهوية (Identification)

العملية التي يمكن بها للفرد أن يتعرف على كيان سبق التحقق من هويته.

الهوية (Identity)

المعلومات المستخدمة للتعيين وللتمييز، إن أمكن بطريقة فريدة لا يشوبها الغموض من كيان محدد داخل نطاق ميدان التسمية.

التأثير (Impact)

التعبير عن مستوى النتائج التي أحدثها هجوم ما (**التأثير المالي**: تكلفة الهجوم، **التأثير المنطقي**: يُقَوِضْ التوافر، السلامة والسرية، **التأثير الاستراتيجي**: يعيق بقاء المنظمة، **تأثير ملموس**: تأثير حقيقي، مباشر ومُلاَحظ).

خطورة التأثير (Impact gravity)

تقييم لخطورة حادث، مُرجَحْ بتواتر حدوثه. ومن المهم تحديد حجم خطورة التأثير من أجل التحديد الدقيق للمتطلبات وترتيب أولوياتها مثلاً: لا تأثير/تأثير لا يؤبه له (صفر) تأثير ضئيل (1)، تأثير معتدل (2)، تأثير قوي (3)، تأثير كارثي (4).

الاستدلال على الفاعل (Imputability)

الصفة التي تجعل في الإمكان نسب عملية إلى مستعمل في وقت ما بكل تأكيد. حقيقة كون المرء قادراً على تحديد هوية المسؤول في حالة وقوع خرق للقواعد.

خسائر غير مباشرة (Indirect losses)

الخسائر الناجمة بصورة غير مباشرة عن عيب أمني.

السلامة (Integrity)

حالة شيء ظل سليماً دون المساس به. معيار أمني إذا تم الوفاء به يجعل من الممكن ضمان أن مورداً لم يعتره أي تغيير (أو تعديل أو تدمير) وبصورة غير مرخص بها.

الشبكة الداخلية (Intranet)

شبكة داخلية وخصوصية لمنظمة ما تستخدم تكنولوجيا الإنترنت وتكون معزولة عادة عن الإنترنت بحوائط نيران (firewalls).

نظام كشف الاقتحام (IDS)

نظام لكشف الحوادث التي يمكن أن تسفر عنها انتهاكات لسياسات الأمن العامة وتشخيص الخروقات المحتملة.

أمن بروتوكول الإنترنت (IPSec)

نسخة من بروتوكول الإنترنت تقدم خدمات الأمن. ويفتح نظام كشف الاقتحام قناة اتصال منطقي (IP tunnel) بين متراسلين على الشبكة العمومية. ويتم الاستيقان من نهايات القناة هذه أما البيانات المنقولة له عبرها فيمكن فك تجفيرها (مفهوم القناة المجفرة أو الشبكة الافتراضية).

الإصدار 6 من بروتوكول الإنترنت (IPv6)

ويشمل تحديث الإصدار 4 من بروتوكول الإنترنت التي تضم إلى جانب أمور أخرى، آليات مُبَيَنَة ذاتياً لتنفيذ خدمات الأمن (الاستيقان من كيانات المنشأ والمقصد، ومن سرية البيانات المنقولة).

مفتاح (Key)

مفتاح تجفير أو لفك التجفير، وهو عادة ما يكون قيمة رياضية لخوارزمية تجفير وما لم تكن مفاتيح التجفير عمومية، فلا ينبغي الإعلان عنها: فهي وسائل سرية لحماية سر آخر (المعلومات التي جُفرت لضمان سريتها).

إدارة المفاتيح (Key management)

إدارة مفاتيح التجفير، توليد وتوزيع وحفظ أضابير، تدمير المفاتيح المحفوظة لدى شرطة الأمن.

قنبلة منطقية (Logic bomb)

برنامج خبيث يبدأ استخدامه بحادث محدد (كتاريخ عيد ميلاد) ويقصد به إيذاء النظام الذي يوجد فيه.

فقدان خدمة ضرورية (Loss of essential service)

عدم التوافر الكلي أو الجزئي أو عطل تشغيل الموارد اللازمة لنظام المنظمة لكي تعمل بصورة سليمة.

أعمال شريرة (Malevolent)

تقال عن الأعمال العدائية التي يمكن أن تسبب ضرراً لموارد منظمة وتقترف بصورة مباشرة أو غير مباشرة بواسطة أشخاص داخل أو خارج المنظمة (سرقة عتاد، بيانات، إفشاء معلومات سرية، خروقات غير قانونية، إلخ).

برمجيات خبيثة (Malware)

مصطلح تنوعي لبرنامج مثل فيروس أو دودة أو حصان طروادة، أو أي شكل آخر غير برمجيات الهجوم وتعمل في قليل أو كثير بصورة مستقلة.

التنكر (Masquerade)

نوع من الهجوم يقوم على أشكال خادعة زائفة من النظام.

عدم – الرفض (Non-repudiation)

القدرة على منع مُرْسل من الإنكار في وقت لاحق أن يكون قد أرسل رسالة أو قام بأي عمل ما. وهو يضمن توافر الدليل الذي يمكن تقديمه لطرف ثالث، ويثبت أن حادثاً أو عملاً قد حدث، أي الدليل على أن رسالة قد أرسلت من جانب شخص محدد في وقت معين دون أن تعدل في وقت لاحق. وينبغي لمثل هذا الدليل أن يكون قابلاً للتحقق من صحته بواسطة طرف ثالث في أي وقت. فبدون عدم الرفض، يمكن لمرسلي المعلومات أو متلقيها أن ينكروا تلقيهم أو إرسالهم للمعلومات المعنية.

عدم الاختيار (No-opt)

الخدمة التي لا يستطيع فيها الزبائن اختيار الكيفية التي تستخدم بها المعلومات المتعلقة بهم (إمكانية النيل من حقهم في سرية البيانات).

التوثيق (Notarization)

تسجيل البيانات لأغراض الدليل.

دالة البصمة وحيدة الاتجاه (One-way hash function)

دالة يمكن استخدامها لحساب بيانات بصمة الإصبع، ولكن ليس لتوليد بيانات ذات بصمة محددة. ويجب على هذه الدالة تفادي خلق تصادمات، أي أن يتم توليد نفس الملف من رسائل مختلفة.

هجوم سالب (Passive attack)

هجوم لا يغير من الهدف (التسمع السلبي، إفشاء السرية).

كلمة مرور (Password)

معلومات سرية يصدرها مستعمل مرخص له لكي يثبت هويته أثناء إجراء الاستيقان لطلب النفاذ إلى مورده.

رقعة تشفير مُصَحِّحْ (Patch)

تحديث البرمجيات يهدف إلى إصلاح نقطة ضعف ظهرت بعد أن تم تركيب البرمجيات.

اختبارات تغلغل (Penetration tests)

وهي تستخدم لتحليل واختبار درجة حماية الأنظمة ومتانة آليات الأمن.

الفركنة (التلصص والتنصت الإلكترونيين) (Phreaking)

الاستخدام غير القانوني أو إساءة استخدام خدمات الاتصال – على حساب الفرد أو المُشغِلْ (على يد مُفرْكِنْ).

المنع (Prevention)

مجموعة إجراءات تتخذ لتلافي خطر أو خطورة، دون تحقق التهديدات، وإلى التقليل من وتيرة الحوادث بهدف تحقيق الحماية.

حماية الخصوصية (Privacy protection)

تدابير وقائية لضمان عدم إفشاء المعلومات عن أنشطة مستعمل الإنترنت إلى أي أطراف غير مرغوب فيها، وعدم استخدامها لأي أغراض غير الأغراض التي يكون صاحبها وافق عليها. وهذا يشير إلى حق الأفراد في التحقق من صحة المعلومات المتعلقة بهم التي يمكن جمعها إما مباشرة أو غير مباشرة عن طريق رصد سلوكهم على الإنترنت والمواقع التي يزورونها.

المفتاح الخصوصي (Private key)

المفتاح الذي يستخدم في آليات التجفير اللاتناظرية (التجفير بالمفاتيح العمومية) التي تنتمي لذي كيان والتي ينبغي إبقاؤها في طي الكتمان.

البنية التحتية لإدارة الامتيازات (PMI)

وهي بنية تحتية تدعم إدارة الامتيازات، والتراخيص والتصاريح.

الحماية (Protection)

عملية الحماية، حالة كون الشيء محمياً. تقال عن تدبير أمني يساعد على كشف وتحييد آثار هجوم والتقليل منها.

مفتاح عمومي (Public key)

هو بصفة عامة، وفي التجفير اللاتناظري، مفتاح عمومي لكيان ما تجب إتاحته للراغبين في إرسال بيانات مجفرة بحيث يمكنه فك تجفير تلك البيانات باستخدام المفتاح الخصوصي المقابل.

التجفير بالمفاتيح العمومية (Public-key cryptography)

نظام تجفير لا تناظري يستخدم جفرات ثنائية المفاتيح أو زوج مفاتيح: أحدهما مفتاح سري خصوصي، والآخر مفتاح عمومي علني. والمفتاحان تكامليان ولا يمكن الفصل بينهما. ولا يمكن استخدام العلاقة الحسابية بينهما لحساب المفتاح الخصوصي.

البنية التحتية للمفاتيح العمومية (Public-key infrastructure (PKI))

بنية تحتية تدعم تنفيذ التجفير اللاتناظري (بالمفاتيح العمومية) وتشمل أموراً من بينها إدارة وتوزيع مفاتيح التجفير والشهادات الرقمية.

الموثوقية (Reliability)

قدرة النظام على أداء وظائفه بدون وقوع حوادث لفترة معينة من الزمن.

الرفض (Repudiation)

حقيقة إنكار أن أحداً قد اشترك في مبادلة.

الإلغاء (الإبطال) (Revocation)

الإخطار بأن مفتاحاً خصوصياً قد فقد سلامته. ويجب عندئذ أن يتوقف استخدام شهادة المفتاح العمومي المناظر له. وفيما يتعلق بالعقود، فإنه يشير كذلك إلى الحق في سحب عرض أو قبوله.

المخاطر (Risk)

الاحتمالية النسبية لن يصبح تهديداً واقعاً، مقاساً من حيث الاحتمالات والتأثيرات.

تحليل المخاطر، تقييم المخاطر (Risk analysis, risk assessment)

عملية تحديد المخاطر وتقييمها (تقيم احتمالات الحدوث والأثر).

إدارة المخاطر (Risk management)

العملية المستمرة لتقييم المخاطر الذي تجريه منظمة للتحكم في المخاطر وإبقائها عند مستوى مقبولٍ. ويمكن استخدامها لتحديد سياسات الأمن الأكثر تكيفاً مع حماية أصول المنظمة.

التخريب (Sabotage)

عمل خبيث أو تخريب همجي، أو ضرر متعمد لمنع منظمة أو بنية تحتية أو خدمة أو مورد من العمل بصورة سوية، ويمكن أن يسفر عن خسائر.

الأمان/السلامة (Safety)

صفة ما هو غير ضار.

طبقة مقابس آمنة (SSL)

برمجية تستخدم لتأمين المبادلات على الإنترنت، طورتها نيتسكيب ويدعمها معظم برامج التصفح في السوق.

الأمن (Security)

هو الوضع الذي يكون فيه شخص ما أو شيء ما غير معرضاً لأي خطر. وهو آلية ترمي إلى منع وقوع حادث ضار، أو الحد من آثاره. والأمن المادي، مثلاً، يشير إلى التدابير المتخذة لحماية البيئات من الناحيتين الطبيعية والمادية، بينما يشير الأمن المنطقي إلى تدابير برمجيات ووسائل حماية.

مسؤول الأمن (Security administrator)

شخص مسؤول عن إقامة أو تنفيذ كل جزء من سياسة عامة للأمن.

التدقيق الأمني (Security audit)

تحليل منهجي لجميع مكونات الأمن، والقائمين عليه، وسياساته والحلول والتدابير والوسائل التي تستخدمها منظمة لتأمين بيئتها، ويتم إجراؤه لرصد الامتثال وتقييم الملاءمة بين الموارد التنظيمية والتقنية والبشرية المحشودة بين المخاطر المتجشمة، وتعظيم وترشيد الأداء والارتقاء به.

التدابير الأمنية (Security measures)

جميع الموارد التكنولوجية والتنظيمية والقانونية والمالية، والبشرية ووسائل العمل المستخدمة للوفاء بأهداف الأمن التي تحددها سياسات الأمن العامة. وهي توضع في فئات عادة تبعاً لدورها الوظيفي (تدابير وقائية، تدابير حمائية، وتدابير ردعية، إلخ).

احتياج أمني (Security need)

بالنسبة لبيئة تحتاج إلى حماية، تحديد مستويات التوافر والتعبير عنها، والسلامة والسرية المرتبطتان بالموارد والقيم المحتاجة إلى حماية.

سياسات الأمن العامة (Security policy)

الإطار المرجعي للأمن الذي تضعه منظمة من المنظمات، ويعكس استراتيجية الأمن ووضع وسائل التنفيذ.

الحساسية (Sensitivity)

خاصية كيان ما تشير إلى قيمته أو أهميته.

مفتاح دورة (Session key)

مفتاح سري يتولد باستخدام نظام تجفير لا تناظري عندما يفتتح المتراسلون دورة عمل، ويقتصر عمر هذا المفتاح على المدة التي تستغرقها الدورة، ويستخدم هذا المفتاح في تجفير كميات كبيرة من البيانات باستخدام خوارزمية تجفير تناظرية.

بروتوكول نقل النص الفوقي الآمن (S-http)

نسخة آمنة من بروتوكول http تسمح بمبادلات آمنة بين الزبون ومُخَدَم ويب.

برنامج تَحسُسْ البيانات (Sniffer)

برنامج ذكي يستخدم للتنصت على البيانات الجاري نقلها على شبكة.

التجسس (Sniffing)

عملية التجسس السلبية لجمع المعلومات التي تستخدم عندئذ بدون علم أصحابها الشرعيين لارتكاب خروقات غير مرخص بها.

الهندسة الاجتماعية (Social engineering)

التقنيات والتدابير والإجراءات التي يستخدمها المهاجمون الخبثاء الذين يستغلون سذاجة المستعلمين لعدة أغراض من بينها الحصول على كلمات المرور خاصتهم ومَعْلَمَات الاتصال وانتحال هويتهم الرقمية لأجل مخادعة النظام واختراقه بالتظاهر بأنهم زوار مرخص لهم.

المُقتَحِمْ (Spammer)

شخص ينخرط في إرسال الرسائل الاقتحامية.

إرسال الرسائل الاقتحامية (Spamming)

وهي تقنية تشتمل على إرسال رسائل غير مطلوبة إلى نظام رسائل إلكتروني.

المُخادِعْ (Spoofer)

شخص ينخرط في المخادعة.

المخادعة (Spoofing)

تقنية تستخدم لاختلاس عناوين بروتوكول الإنترنت لأجل خرق نظام من الأنظمة.

برنامج تجسس (Spyware)

برنامج يرسل معلومات حساسة من كمبيوتر مصاب بالعدوى إلى المهاجم.

التراسل غير المرئي (Steganography)

وهو أسلوب تقني يستخدم لإخفاء معلومة داخل معلومة أخرى بغرض نقلها أو خزنها بطريقة مستترة. فوضع العلامات المائية هي تطبيق لأسلوب التراسل غير المرئي يتكون من وضع علامات لا تنطمس فوق صورة.

التهديد (Threat)

علامة أو إشارة أو نذير خطر. عمل أو حادث قابل للحدوث، وتحويله إلى هجوم على بيئة أو مورد وخرق الأمن.

تحليل الحركة (Traffic analysis)

ملاحظة دفقات المعلومات ودراستها بين كياني المنشأ والمقصد (التواجد، الغياب، المبلغ، الاتجاه، التواتر، إلخ).

باب المصيدة – أنظر الباب الخلفي (Backdoor)

حصان طروادة (Trojan horse)

برنامج خبيث مستور داخل برنامج قانوني وداخل في أنظمة بغرض اختطافها (سرقة وقت مُعَالِجْ، إفساد البيانات والبرامج، أو تعديلها أو تدميرها، تسبب في الأعطال، والتنصت، إلخ).

الثقة (Trust)

الاعتماد الواثق على شخص ما أو شيء ما (معيار كيفي، شخص ونسبي إلى حد بعيد).

ميثاق المستعملين (User charter)

هو وثيقة تضعها منظمة تشمل حقوق موظفيها وواجباتهم ومسؤولياتهم من حيث استخدام تكنولوجيا المعلومات، وموارد الاتصالات التي توفرها لهم، مُوَقَعَة من جانب الأطراف المعنية.

بيان المستعمل (User profile)

قائمة بصفات المستعمل تساعد على إدارة الشبكة والأنظمة التي يرتبط بها المستعملون (مَعْلَمَات الهوية والاستيقان، حقوق النفاذ، والتراخيص والمعلومات المفيدة الأخرى) لأغراض مراقبة النفاذ، والفوترة وما إلى ذلك.

شبكة خاصة افتراضية (Virtual private network) (VPN)

يشير هذا المفهوم إلى استخدام أمن بروتوكول الإنترنت IPSec لفتح قناة اتصال خاص آمنة على شبكة عامة غير آمنة. وهي تستخدم غالباً بواسطة منظمة للربط بين مواقعها العديدة عبر الإنترنت مع ضمان سرية البيانات المتبادلة في نفس الوقت.

فيروس (Virus)

برنامج خبيث يتم إدخاله في نظام بدون علم المستعمل. ولدى هذا البرنامج القدرة على استنساخ نفسه (سواء في شكل مطابق تماماً أو، في حالة الفيروس متعددة الأشكال، بالطفرات)، وذلك للإضرار بالبيئة التي يتم تنفيذ ذلك فيها، ولتلويث المستعملين الآخرين الذين يتلامسون معه. وهناك أنواع مختلفة من الفيروسات، تبعاً لتوقيعاتها، وسلوكها وكيفية تكاثرها، وكيفية نقل العدوى للماكينات، والأعطال التي تسببها، إلخ. فالديدان، أحصنة طروادة والقنابل المنطقية هي شفرات خبيثة تنتمي إلى عائلة الفيروسات التنوعية.

التعرض (Vulnerability)

عيب أمني يمكن أن يسفر عن خرق مقصود أو غير مقصود للسياسة العامة للأمن.

الملحق B – جدول محتويات المعيار ISO/IEC standard 17799:2005 الذي يستخدم كمرجع في إدارة الأمن

مقدمـــة

1.0 ما هو أمن المعلومات؟

2.0 ما وجه الحاجة إلى أمن المعلومات؟

3.0 كيف تحدد متطلبات الأمن؟

4.0 تقييم المخاطر الأمنية

5.0 انتقاء الضوابط

6.0 نقطة البداية لأمن المعلومات

7.0 عوامل نجاح حرجة

8.0 وضع المبادئ التوجيهية الخاصة بك

1 النطاق

2 المصطلحات والتعريفات

3 بنية هذا المعيار

1.3 أحكام

2.3 فئات الأمن الرئيسية

4 تقييم المخاطر ومعالجتها

1.4 تقييم المخاطر الأمنية

2.4 معالجة المخاطر الأمنية

5 سياسة الأمن العامة

1.5 سياسة أمن المعلومات

1.1.5 وثيقة سياسة أمن المعلومات

2.1.5 مراجعة سياسة أمن المعلومات

6 تنظيم أمن المعلومات

1.6 التنظيم الداخلي

1.1.6 التزام الإدارة تجاه أمن المعلومات

2.1.6 تنسيق أمن المعلومات

3.1.6 تخصيص مسؤوليات أمن المعلومات

4.1.6 عملية الترخيص لمرافق معالجة المعلومات

5.1.6 اتفاقات السرية

6.1.6 الاتصال بالسلطات

7.1.6 الاتصال بجماعات المصالح الخاصة

8.1.6 مراجعة مستقلة لأمن المعلومات

2.6 أطراف خارجيون

1.2.6 تحديد المخاطر المتصلة بأطراف خارجين

2.2.6 تناول الأمن عند التعامل مع الزبائن

3.2.6 تناول الأمن في اتفاقات الطرف الثالث

7 إدارة الأصول

1.7 المسؤولية عن الأصول

1.1.7 قائمة الأصول

2.1.7 ملكية الأصول

3.1.7 الاستخدام المقبول للأصول

2.7 تصنيف المعلومات

1.2.7 المبادئ التوجيهية للتصنيف

2.2.7 وَسْمْ المعلومات ومناولتها

8 أمن الموارد البشرية

1.8 ما قبل التوظيف

1.1.8 الأدوار والمسؤوليات

2.1.8 الغربلة

3.1.8 شروط التوظيف

2.8 أثناء التوظيف

1.2.8 مسؤوليات الإدارة

2.2.8 الوعي والتثقيف والتدريب بشأن أمن المعلومات

3.2.8 عملية التأديب

3.8 إنهاء التوظيف أو تغييره

1.3.8 مسؤوليات الإنهاء

2.3.8 عودة الأصول

3.3.8 إزالة حقوق النفاذ

9 الأمن المادي والبيئي

1.9 مناطق آمنة

1.1.9 الحدود الخارجية للأمن المادي

2.1.9 ضوابط الدخول المادي

3.1.9 تأمين المكاتب، الغرب والمرافق

4.1.9 الحماية من التهديدات الخارجية والبيئية

5.1.9 العمل داخل أماكن آمنة

6.1.9 النفاذ العمومي، التسليم، ومناطق التحميل

2.9 أمن المعدات

1.2.9 اختيار أماكن المعدات والحماية

2.2.9 مرافق الدعم

3.2.9 أمن تشغيل الكبلات

4.2.9 صيانة المعدات

5.2.9 صيانة المعدات خارج المباني

6.2.9 التخلص الأمن من المعدات أو إعادة استخدامها

7.2.9 نقل الممتلكات

10 إدارة الاتصالات والعمليات

1.10 التدابير والمسؤوليات التشغيلية

1.1.10 تدابير التشغيل الموثقة

2.1.10 إدارة التغيير

3.1.10 الفصل بين الواجبات

4.1.10 فصل التطوير، والاختبار والمرافق التشغيلية

2.10 إدارة تأدية خدمات الطرف الثالث

1.2.10 تأدية الخدمات

2.2.10 متابعة ومراجعة خدمات الطرف الثالث

3.2.10 إدارة التغييرات لخدمة الطرف الثاني

3.10 تخطيط النظام وقبوله

1.3.10 إدارة القدرات

2.3.10 قبول الأنظمة

4.10 الوقاية من الشفرة الخبيثة والنقالة

1.4.10 الضوابط ضد الشفرة الخبيثة

2.4.10 الضوابط ضد الشفرة النقالة

5.10 المساندة

1.5.10 المعلومات المسانَدة

6.10 إدارة أمن الشبكة

1.6.10 ضوابط الشبكة

2.6.10 أمن خدمات الشبكة

7.10 مناولة الوسائط

1.7.10 إدارة الوسائط القابلة للنقل

2.7.10 التخلص من الوسائط

3.7.10 تدابير مناولة المعلومات

4.7.10 أمن وثائق النظام

8.10 تبادل المعلومات

1.8.10 سياسات وتدابير تبادل المعلومات

2.8.10 اتفاقية المبادلة

3.8.10 الوسائط المادية في حالة انتقال

4.8.10 إرسال الرسائل الإلكترونية

5.8.10 أنظمة معلومات الأعمال

9.10 خدمات التجارة الإلكترونية

1.9.10 التجارة الإلكترونية

2.9.10 المعاملات على الشبكة

3.9.10 المعلومات المتاحة جماهيرياً

10.10 المتابعة

1.10.10 التسجيل التدقيق

2.10.10 استخدام أنظمة المتابعة

3.10.10 حماية المعلومات اللوغاريتمية

4.10.10 لوغاريتمات المدير الإداري والمُشَغِلْ

5.10.10 تسجيل الأعطاب

6.10.10 مزامنة الميقاتية

11 التحكم في النفاذ

1.11 متطلبات العمل للتحكم في النفاذ

1.1.11 السياسات العامة للتحكم في النفاذ

2.11 إدارة نفاذ المستعملين

1.2.11 تسجيل المستعملين

2.2.11 إدارة الامتيازات

3.2.11 إدارة كلمات مرور المستعملين

4.2.11 مراجعة حقوق نفاذ المستعملين

3.11 مسؤوليات المستعمل

1.3.11 استعمال كلمة المرور

2.3.11 معدات المستعمل غير المصاحبة

3.3.11 سياسات المكتب النظيف والشاشة النظيفة

4.11 التحكم في النفاذ إلى الشبكة

1.4.11 سياسات عامة بشأن استخدام خدمات الشبكة

2.4.11 الاستيقان من المستعمل لأجل الوصلات الخارجية

3.4.11 تحديد المعدات الموجودة في الشبكات

4.4.11 الحماية عن بعد لميناء التشخيص والتشكيل

5.4.11 الفصل بين الشبكات

6.4.11 التحكم في ربط الشبكات

7.4.11 التحكم في تسيير الشبكات

5.11 التحكم في نظام التشغيل

1.5.11 تدابير الدخول الآمن إلى الشبكة

2.5.11 تحديد هوية المستعمل والاستيقان منها

3.5.11 نظام إدارة كلمات المرور

4.5.11 استخدام مرافق النظام

5.5.11 انتهاء وقت الدورة

6.5.11 تحديد وقت الاتصال

6.11 التحكم في النفاذ إلى التطبيق والمعلومات

1.6.11 تقييد النفاذ إلى المعلومات

2.6.11 عزل النظام الحساس

7.11 إجراء العمليات الحاسوبية المتنقلة والربط الشبكي

1.7.11 إجراء العمليات الحاسوبية والاتصالات المتنقلة

2.7.11 الأعمال البعدية

12 حيازة أنظمة المعلومات وتطويرها وصيانتها

1.12 المتطلبات الأمنية لأنظمة المعلومات

1.1.12 تحليل وتعيين متطلبات الأمن

2.12 المعالجة السليمة للتطبيقات

1.2.12 إثبات صحة المدخلات من البيانات

2.2.12 الرقابة على المعالجة الداخلية

3.2.12 سلامة الرسائل

4.2.12 إثبات صحة المخرجات

3.12 ضوابط الكتابة التجفيرية

1.3.12 سياسات عامة بشأن استخدام ضوابط التجفير

2.3.12 إدارة المفاتيح

4.12 أمن ملفات النظام

1.4.12 السيطرة على البرمجيات التشغيلية

2.4.12 حماية البيانات الإخبارية

3.4.12 التحكم في النفاذ إلى شفرة المصدر البرنامجي

5.12 الأمن في عمليات التنمية والدعم

1.5.12 تغيير تدابير التحكم

2.5.12 مراجعة تقنية للتطبيقات بعد التغيرات في نظام التشغيل

3.5.12 قيود على إدخال تغييرات على حَزِمْ البرمجيات

4.5.12 تسرب المعلومات

5.5.12 تنمية البرمجيات المعهود بها لجهات خارجية

6.12 إدارة التعرض التقني

1.6.12 التحكم في جوانب التعرض التقنية

13 إدارة حوادث أمن المعلومات

1.13 مواطن ضعف وحوادث أمن المعلومات

1.1.13 حوادث من إبلاغ المعلومات

2.1.13 جوانب ضعف أمن الإبلاغ

2.13 إدارة حوادث أمن المعلومات والتحسينات

1.2.13 مسؤوليات وتدابير

2.2.13 التعلم من حوادث أمن المعلومات

3.2.13 جمع القرائن

14 إدارة استمرار الأعمال

1.14 جوانب أمن المعلومات في إدارة استمرار الأعمال

1.1.14 إدراج أمن المعلومات في عملية إدارة استمرار الأعمال

2.1.14 استمرارية الأعمال وإدارة المخاطر

3.1.14 تطوير وتنفيذ خطط الاستمرارية بما في ذلك أمن المعلومات

4.1.14 إطار تخطيط استمرارية الأعمال

5.1.14 اختيار وصيانة وإعادة تقييم خطط استمرارية الأعمال

15 الامتثال

1.15 الامتثال للمتطلبات القانونية

1.1.15 تحديد التشريعات السارية

2.1.15 حقوق الملكية الفكرية (IPR)

3.1.15 حماية السجلات التابعة للمنظمة

4.1.15 حماية البيانات وسرية المعلومات الشخصية

الملحق C – اختصاصات وأنشطة قطاع تنمية الاتصالات في الأمن السيبراني

للاطلاع على مزيد من المعلومات يرجى الرجوع إلى العنوان التالي:
http://www.itu.int/ITU-D/e-strategy/e-security

يمكن في التقارن المبين أدناه فقرة أمام فقرة تقريباً تبين أوجه التآزر القوية بين الأولويات والإجراءات في هذا البرنامج في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية وخطة عمل جنيف للقمة العالمية لمجتمع المعلومات وبرنامج عمل تونس. وقد عين برنامج عمل تونس لعام 2005 الاتحاد الدولي للاتصالات باعتباره المنظمة الرائدة التي ترمي إلى تسهيل وتوجيه الإجراءات الرامية إلى تنفيذ خطة عمل جنيف في ميدان بناء الثقة والأمن فيما يتعلق باستعمال تكنولوجيا المعلومات والاتصالات. وقرر أعضاء الاتحاد الدولي للاتصالات في خطة عمل الدوحة التي اعتمدها المؤتمر العالمي لتنمية الاتصالات في مارس 2006، أن الأمن السيبراني ومكافحة الرسائل الاقتحامية هما الأولوية العليا للبرنامج رقم 3.

خط العمل ج.5 للقمة العالمية لمجتمع المعلومات (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات) واختصاصات الاتحاد في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية

خط العمل جيم5 للقمة العالمية لمجتمع المعلومات (WSIS)	اختصاصات الاتحاد فيما يتعلق بخط العمل جيم5
12. الثقة والأمن ركيزتان من الركائز الأساسية لمجتمع المعلومات.	تناول مسألة الأمن السيبراني في هذا البرنامج من أجل تحقيق إمكانات الشبكات في تقديم خدمات وتطبيقات إلكترونية مأمونة وسهلة المنال.
أ) تشجيع التعاون بين الحكومات في الأمم المتحدة ومع جميع أصحاب المصلحة في المحافل الملائمة الأخرى من أجل تعزيز الثقة لدى المستعملين، وبناء الطمأنينة وحماية البيانات وسلامة الشبكات؛ والنظر في الأخطار الحالية والمحتملة التي تهدد تكنولوجيا المعلومات والاتصالات؛ والتعامل مع القضايا الأخرى المتصلة بأمن المعلومات وأمن الشبكات.	من الضروري، من أجل تقليل ومنع واكتشاف التهديدات السيبرانية تيسير سبل الاتصال والتعاون لدعم عملية جمع ونشر المعلومات المتصلة بالأمن السيبراني وتبادل أفضل الممارسات ودعم المساعدة الناجعة المتبادلة، والاستجابة والاستعادة في ما بين الأعضاء وفيما بين الأعمال التي تديرها السلطات العمومية والشركات التجارية والمجتمع المدني.
ب) ينبغي أن تعمل الحكومات، بالتعاون مع القطاع الخاص، على منع واكتشاف ومواجهة الجرائم السيبرانية وإساءة استعمال تكنولوجيا المعلومات والاتصالات عن طريق: وضع خطوط توجيهية تأخذ في الاعتبار الجهود الجارية في هذه المجالات؛ والنظر في تطبيق تشريعات تسمح بالتحقيق الفعال في حالات إساءة الاستعمال ومقاضاتها؛ وتشجيع الجهود الفعالة في مجال المساعدات المتبادلة، وتعزيز الدعم المؤسسي على المستوى الدولي لمنع مثل هذه الجرائم واكتشافها وإصلاح ما يترتب عليها؛ وتشجيع التعليم والنهوض بالوعي العام.	وضع خطوط توجيهية وأدوات وكتيبات للتخطيط بشأن التكنولوجيا وجوانب السياسة العامة المتعلقة بالأمن السيبراني. إعداد مجموعة أدوات للأمن السيبراني من أجل وضع السياسات العامة والقطاعات ذات الصلة الأخرى. تقديم المساعدة إلى الدول الأعضاء في وضع القوانين والتشريعات النموذجية من أجل منع الجريمة السيبرانية. إعداد مواد للتدريب بشأن الاستراتيجيات الخاصة بالتكنولوجيا وتطور التكنولوجيا من أجل تنفيذ الأمن السيبراني.
ج) ينبغي أن تعمل الحكومات وأصحاب المصلحة الآخرون بنشاط على تعزيز تعليم وتوعية المستعملين بشأن الخصوصية على الخط وسبل المحافظة عليها.	المساعدة في إذكاء الوعي وتحديد المسائل الرئيسية دعماً لثقافة الأمن السيبراني، والتوصية بنماذج الممارسات الجيدة لدعم تطبيقات تكنولوجيا المعلومات والاتصالات والتقليل إلى أدنى حد من التهديدات السيبرانية.

خط العمل جيم5 للقمة العالمية لمجتمع المعلومات (WSIS)	اختصاصات الاتحاد فيما يتعلق بخط العمل جيم5
د) اتخاذ الإجراءات المناسبة بشأن الرسائل الاقتحامية على المستويين الوطني والدولي.	تكوين فهم مشترك لقضايا الرسائل الاقتحامية والتهديدات السيبرانية بما في ذلك التدابير المضادة لها. أخذ أعمال أصحاب المصلحة الآخرين وذات الصلة في الاعتبار، حسب الاقتضاء: بلدان منظمة التعاون والتنمية في الميدان الاقتصادي، والموقعون على الاتفاقات الرئيسية بشأن الأمن السيبراني والرسائل الاقتحامية.
هـ) تشجيع التقييم المحلي للقوانين الوطنية للتغلب على أي عقبات أمام الاستعمال الفعال للوثائق والمعاملات الإلكترونية، بما في ذلك أساليب التوثيق الإلكترونية.	تنظيم حلقة عمل واجتماعات وحلقات دراسية لتناول المسائل التقنية ومسائل السياسة العامة والمسائل القانونية والمسائل المتعلقة بالاستراتيجية من أجل تحقيق الأمن السيبراني. تقديم المساعدة إلى الدول الأعضاء في مجال وضع القوانين والتشريعات النموذجية من أجل منع الجريمة السيبرانية.
و) زيادة تعزيز إطار الثقة والأمن باتخاذ إجراءات تعزيز متبادلة في مجالات الأمن المتعلقة باستعمال تكنولوجيا المعلومات والاتصالات، مع اتخاذ مبادرات أو وضع خطوط توجيهية فيما يتعلق بالحق في الخصوصية، وفي حماية البيانات وحماية المستهلك.	تحديد متطلبات الأمن السيبراني واقتراح حلول لتطوير وتأمين تطبيقات تكنولوجيات المعلومات والاتصالات. والمساعدة في إذكاء الوعي وتحديد المسائل الرئيسية الرامية إلى دعم ثقافة الأمن السيبراني والتوصية بنماذج للممارسات الجيدة ودعم تطبيقات تكنولوجيا المعلومات والاتصالات والتقليل إلى أدنى حد من التهديدات السيبرانية.
ز) تبادل الممارسات الجيدة في مجال أمن المعلومات وأمن الشبكات وتشجيع استخدامها من جانب جميع الأطراف المعنية.	استحداث أدوات لتسهيل تقاسم المعلومات بشأن التكنولوجيا ومسائل السياسة العامة وبشأن أفضل الممارسات المتعلقة بالأمن السيبراني. العمل كميسر للتعاون الإقليمي والأقاليمي، ودعم الأنشطة الملائمة لبناء القدرات على المستوى الإقليمي.
ح) دعوة البلدان المهتمة إلى إنشاء نقاط اتصال للتعامل مع الحوادث والاستجابة لها وقت وقوعها، وإنشاء شبكة تعاونية بين نقاط الاتصال لتبادل المعلومات والتكنولوجيات من أجل الاستجابة لهذه الحالات.	يمكن أن تشمل الإجراءات، ضمن جملة أمور، وضع مذكرات تفاهم بين الدول الأطراف المهتمة بتعزيز الأمن السيبراني. تنفيذ مشروع عالمي لأصحاب المصلحة المتعددين [...] وتقديم حلول في عدة ميادين بما في ذلك: 1. إنشاء نقاط اتصال وطنية. 2. الاستجابة لمقتضيات الحوادث والمراقبة والإنذار بحث أفضل الممارسات من أجل إنشاء وتشغيل وسائل المراقبة والإنذار والاستجابة للحوادث والإصلاح، التي قد تستخدمها الدول الأعضاء من أجل بناء قدراتها الوطنية في هذا المضمار.
ط) التشجيع على المضي قدماً في تطوير التطبيقات الآمنة والموثوقة لتسهيل إجراء المعاملات على الخط.	تحديد متطلبات الأمن، واقتراح حلول لتطوير تطبيقات آمنة لتكنولوجيا المعلومات والاتصالات.
ي) تشجيع البلدان المهتمة على المساهمة بنشاط في أنشطة الأمم المتحدة الجارية بشأن بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.	دعوة الدول الأعضاء للأعضاء في الاتحاد وأعضاء القطاعات والمنتسبين إليها: تقديم مساهمات بشأن هذا الموضوع في لجنة الدراسات 1 لقطاع تنمية الاتصالات والمشاركة في الأنشطة الجارية لمشاريع قطاع تنمية الاتصالات. المساهمة في بناء الثقة والأمن فيما يتعلق باستعمال تكنولوجيا المعلومات والاتصالات على المستويات الوطنية والإقليمية والدولية من خلال الاضطلاع بالأنشطة على النحو المبين في الفقرة 12[64] من خطة عمل جنيف.

[64] الفقرة 12 هي النص الكامل لخط العمل ج5 للقمة WSIS الذي يرد في العمود 1 من هذه الوثيقة.

اختصاصات قطاع تنمية الاتصالات في الاتحاد في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية

في إطار المقررات التي اعتمدها أعضاء الاتحاد الدولي للاتصالات في مؤتمري المندوبين المفوضين للاتحاد في 2002-2006 (PP02 وPP06) والمؤتمرين العالميين لتنمية الاتصالات 2002 و2006 (WTDC02 وWTDC06)، فإن اختصاصات قطاع تنمية الاتصالات في الاتحاد في مجال الأمن السيبراني ومكافحة التهديدات السيبرانية والرسائل الاقتحامية مدرجة في المقررات التالية:

1. المؤتمر العالمي لتنمية الاتصالات – 2002 (WTDC-02) والمؤتمر العالمي لتنمية الاتصالات 2006 (WTDC-06) – البرنامج 3: الاستراتيجيات الإلكترونية وتطبيقات تكنولوجيا المعلومات والاتصالات.
2. المؤتمر العالمي لتنمية الاتصالات – 2006 (WTDC-06) القرار 45 – آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية.
3. المؤتمر العالمي لتنمية الاتصالات – 2006 الملحق 2 بالقرار 2 – لجنة الدراسات 1 لقطاع تنمية الاتصالات المسألة 22 – تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني.
4. القرار 130 (المراجع في أنطاليا، 2006) – تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

1. خطة عمل الدوحة (WTDC-2006) – البرنامج 3: (الاستراتيجيات الإلكترونية وتطبيقات تكنولوجيا المعلومات والاتصالات)

الأولويات

أ. من الضروري تناول مسألة الأمن السيبراني في هذا البرنامج من أجل تحقيق إمكانات الشبكات في تقديم خدمات وتطبيقات إلكترونية مأمونة وسهلة المنال

ب. ينبغي لهذا البرنامج أيضاً أن يوفر فهماً مشتركاً لمسائل الرسائل الاقتحامية والتهديدات السيبرانية، بما في ذلك التدابير المضادة.

ج. ومن الضروري، من أجل تقليل ومنع واكتشاف التهديدات السيبرانية تيسير سبل الاتصال والتعاون لدعم عملية جمع ونشر المعلومات المتصلة بالأمن السيبراني وتبادل أفضل الممارسات ودعم المساعدة الناجعة المتبادلة، والاستجابة والاستعادة في ما بين الأعضاء وفيما بين الأعمال التي تديرها السلطات العمومية والشركات التجارية والمجتمع المدني.

د. وينبغي أن يكون مكتب تنمية الاتصالات بمثابة المنسق لتسهيل التعاون الإقليمي والأقاليمي ودعم أنشطة بناء القدرات الملائمة على المستوى الإقليمي.

هـ. وقد يشمل ذلك عدة أمور منها تبادل مذكرات تفاهم بين الدول الأعضاء المهتمة لتعزيز الأمن السيبراني.

المهـــام

أ. المساعدة في صياغة خطوط توجيهية وأدوات تخطيطية وكتيبات عن جوانب التكنولوجيا وجوانب السياسة العامة المتصلة بالأمن السيبراني.

ب. استحداث مجموعات أدوات لتوفير الأمن السيبراني من أجل صانعي السياسات والقطاعات الأخرى ذات الصلة.

ج. وضع مواد تدريبية عن الاستراتيجيات والتطورات التكنولوجية اللازمة لتنفيذ الأمن السيبراني.

د. تنظيم ورش العمل، والاجتماعات والحلقات الدراسية، لمناقشة القضايا التقنية والقانونية والسياسية والاستراتيجية المتصلة بالأمن السيبراني.

هـ. تقديم المساعدة إلى الدول الأعضاء في صياغة القوانين ونماذج التشريعات لمنع الجرائم السيبرانية.

و. تحديد متطلبات الأمن، واقتراح حلول لتطوير تطبيقات آمنة لتكنولوجيا المعلومات والاتصالات. والمساعدة في زيادة التوعية وتحديد القضايا الرئيسية المتصلة بدعم ثقافة الأمن السيبراني والتوصية بنماذج من الممارسات الجيدة لدعم تطبيقات تكنولوجيا المعلومات والاتصالات وتقليل التهديدات السيبرانية إلى أدنى حد.

ز. استحداث أدوات لتسهيل تقاسم المعلومات بشأن القضايا التكنولوجية والسياسات وبشأن أفضل الممارسات المتعلقة بتوفير الأمن السيبراني.

ح. العمل عند الاقتضاء، على مراعاة الأعمال ذات الصلة التي يقوم بها أصحاب مصلحة آخرون: منظمة التعاون والتنمية في الميدان الاقتصادي، الموقعون على الاتفاقات الرئيسية بشأن الأمن السيبراني والرسائل الاقتحامية، ومنها مثلاً خطة *عمل لندن ومذكرة تفاهم سيؤول – ملبورن لمكافحة الرسائل الاقتحامية*.

2. المؤتمر العالمي لتنمية الاتصالات – 2006 القرار 45 – آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية

إذ يذكّر

بدعمه الأساسي للبرنامج 3 (الاستراتيجيات الإلكترونية وتطبيقات تكنولوجيا المعلومات والاتصالات) مع التأكيد على أن يكون هذا البرنامج مسؤولاً بالدرجة الأولى عن خط العمل جيم5 الوارد في برنامج عمل تونس (بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات)،

وإذ يلاحظ

أن القرار 50 (فلوريانوبوليس، 2004) للجمعية العالمية لتقييس الاتصالات حول الأمن السيبراني، قد اقتصر على دراسة الجوانب التقنية فقط بالنسبة للتخفيف من آثار هذه الظاهرة،

يهيب بالدول الأعضاء

أن تقدم الدعم اللازم لتنفيذ هذا القرار،

يقرر

تكليف مدير مكتب تنمية الاتصالات

أ) أن يقوم، بالاشتراك مع البرنامج 3 واستناداً إلى مساهمات الأعضاء، بتنظيم اجتماعات للدول الأعضاء وأعضاء القطاع لمناقشة سبل تعزيز الأمن السيبراني بما في ذلك مذكرة تفاهم لتعزيز الأمن السيبراني ومكافحة الرسائل الاقتحامية بين الدول الأعضاء المهتمة؛

ب) أن يقدم تقريراً عن نتائج هذه الاجتماعات إلى مؤتمر المندوبين المفوضين (أنطاليا، 2006).

نتائج القرار 45: آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية

يضطلع مكتب تنمية الاتصالات بالتنسيق مع البرنامج 3 بوضع مشروع عالمي لأصحاب مصلحة متعددين يحقق الارتباط بين المبادرات القائمة وهدف تلبية احتياجات البلدان النامية. وسيركز المشروع الذي من المقرر أن يبدأ في عام 2007 على تقديم حلول في الميادين التالية:

1. التشريعات القوية
2. تنمية التدابير التقنية
3. إقامة شراكات في مجال الصناعة لا سيما مع مقدمي خدمات الإنترنت وشركات الخدمة المتنقلة ورابطات التسويق المباشر
4. توعية المستهلكين والأطراف الفاعلة الصناعية بشأن التدابير الموجهة نحو مكافحة الرسائل الاقتحامية وممارسات أمن الإنترنت
5. التعاون الدولي على مستوى الحكومات والصناعة والمستهلكين والأعمال التجارية وجماعات مكافحة الرسائل الاقتحامية، للسماح باتباع نهج عالمي ومنسق إزاء هذه المشكلة.

وبالإضافة إلى القائمة المذكورة أعلاه تبين أثناء المناقشات والعروض أن المجالات الواردة أدناه لا تندرج في أي ترتيب للأولويات ولكنها ذات أهمية للتعاون ومساعدة الدول الأعضاء، ويمكن لقطاع تنمية الاتصالات أن يشارك فيها بالتعاون مع الكيانات ذات الخبرة المشهود بها في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية:

أ. بناء الوعي الأساسي

ب. التشريعات الوطنية الملائمة

ج. بناء القدرات البشرية والمؤسسية

د. الإنفاذ (مجال بناء القدرات)

هـ. الاستراتيجيات والسياسات الوطنية في مجال الأمن السيبراني

و. تبادل المعلومات بين البلدان وأصحاب المصلحة المعنيين

ز. إنشاء نقاط اتصال وطنية

ح. رصد وتقييم التقدم في مجال المبادرات القائمة

ط. الاستجابة للحوادث ومراقبتها والإنذار بشأنها

ي. تقييم مواطن الضعف والتهديدات فيما يتعلق بالأمن السيبراني

ك. الأدوات والتطبيقات الفعالة للشبكات والأمن السيبراني

ل. الشراكات

م. التعاون الدولي

وفيما يتعلق بهذا المشروع:

- العنوان "مشروع لتعزيز التعاون بشأن الأمن السيبراني ومكافحة الرسائل الاقتحامية"، وسيستغرق هذا المشروع 4 سنوات تبدأ من 2007، وسيكون جزءاً من الخطة التشغيلية لمكتب تنمية الاتصالات لعام 2007.
- ستعد تقارير سنوية تقدم إلى دورات مجلس الاتحاد بشأن التقدم المحرز في التنفيذ.

- ينبغي للمشروع أثناء عملية التنفيذ أن يأخذ في الحسبان القرارات الصادرة عن المؤتمر العالمي لتنمية الاتصالات لعام 2006 بشأن اختصاصات قطاع التنمية في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية.
- ينبغي للمشروع أن يرمي في المقام الأول إلى تقديم المساعدة إلى البلدان النامية في المجالات المعنية التي حددها الاجتماع والمذكورة أعلاه باعتبارها مجالات ذات أهمية حيوية للتعاون في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية.
- ينبغي للمشروع فيما يتعلق بالتشريعات ذات الصلة أن يأخذ في الحسبان حسب الاقتضاء العمل الذي يضطلع به مجلس أوروبا عند تقديمه المساعدة للبلدان في إعداد التشريعات الوطنية وذلك وفقاً لأحكام الاتفاقية المتعلقة بالجريمة السيبرانية.
- ينبغي لتنفيذ الأنشطة في إطار هذا المشروع أن يرتكز على الطلبات التي أعربت عنها البلدان مع التأكيد على البلدان النامية بوجه خاص.
- ينبغي عرض المشروع بعد إعداده على كيانات التمويل المحتملة بما في ذلك الدول الأعضاء والقطاع الخاص والمنظمات الدولية مثل البنك الدولي والمفوضية الأوروبية.

3. القرار 2 من المؤتمر العالمي لتنمية الاتصالات (WTDC-2006) – لجنة الدراسات 1 التابعة لقطاع تنمية الاتصالات المسألة 22 – تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

أ) دراسة وإحصاء ووصف العناصر التالية وزيادة التوعية بها:

- المسائل الرئيسية التي تواجه صانعي السياسات الوطنية وجميع أصحاب المصلحة، لبناء ثقافة الأمن السيبراني؛
- المصادر الرئيسية للمعلومات والمساعدة المتعلقة ببناء ثقافة الأمن السيبراني؛
- أفضل الممارسات الناجحة التي يستخدمها صانعو السياسات الوطنية من أجل تحديد وتنفيذ استراتيجية الأمن السيبراني بالتعاون مع جميع أصحاب المصلحة وبناء ثقافة الأمن السيبراني؛
- التحديات الفريدة من نوعها التي تواجه البلدان النامية في معالجة أمن الشبكات، وأفضل الممارسات الكفيلة بمواجهة هذه التحديات؛

ب) بحث أفضل الممارسات من أجل إنشاء وتشغيل وسائل المراقبة والإنذار والاستجابة للحوادث والإصلاح، التي قد تستخدمها الدول الأعضاء من أجل بناء قدراتها الوطنية في هذا المضمار.

توجيه تقرير أو عدة تقارير إلى الأعضاء بشأن المسائل المحددة في القسم 2 أعلاه. وسيوضح هذا التقرير (أو هذه التقارير) أن شبكات المعلومات والاتصالات المؤمّنة تشكل جزءاً لا يتجزأ من بناء مجتمع المعلومات ومن التنمية الاقتصادية والاجتماعية لجميع البلدان.

4. القرار 130 (المراجع في أنطاليا، 2006) – تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات

يقرر

أن يعطي أولوية عالية لهذه الأعمال داخل الاتحاد وفقاً لاختصاصاته وخبراته التقنية،

يكلّف الأمين العام ومديري المكاتب الثلاثة

1 باستعراض:

'1' العمل الذي أنجزه الاتحاد حتى الآن والمنظمات الأخرى المعنية وكذلك مبادرات التصدي للتهديدات القائمة والمقبلة لشبكات تكنولوجيا المعلومات والاتصالات، مثل مكافحة الرسائل الاقتحامية؛

'2' التقدم المحرز في تنفيذ هذا القرار وفي دور الاتحاد بوصفه جهة تنسيق/تسهيل لخط العمل جيم5 للقمة العالمية، وذلك بمساعدة الأفرقة الاستشارية وبما لا يتعارض مع اتفاقية الاتحاد ودستور الاتحاد؛

2 بتسهيل النفاذ إلى الأدوات المطلوبة لتعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات لصالح جميع الدول الأعضاء، وذلك تمشياً مع أحكام القمة العالمية بشأن النفاذ الشامل وغير التمييزي إلى تكنولوجيا المعلومات والاتصالات أمام جميع البلدان؛

3 الحفاظ على بوابة الأمن السيبراني باعتبارها طريقة لتقاسم المعلومات عن المبادرات على المستويات الوطنية والإقليمية والدولية المتصلة بالأمن السيبراني في أنحاء العالم؛

4 بتقديم تقرير سنوي إلى المجلس عن هذه الأنشطة وعرض مقترحات حسب الاقتضاء،

يكلّف مدير مكتب تنمية الاتصالات

1 بأن يقوم، اتساقاً مع نتائج المؤتمر العالمي لتنمية الاتصالات (الدوحة، 2006) والاجتماع الذي عُقد بعد ذلك عملاً بالقرار 45 (الدوحة، 2006) لنفس المؤتمر، بتطوير مشروع لتعزيز التعاون بشأن الأمن السيبراني ومكافحة الرسائل الاقتحامية يستجيب لحاجات البلدان النامية، بالتعاون الوثيق مع الشركاء المعنيين؛

2 بتقديم الدعم المالي والإداري اللازم لهذا المشروع في حدود الموارد الحالية، والتماس موارد إضافية (نقدية وعينية) لتنفيذ هذه المشاريع من خلال اتفاقات الشراكة؛

3 بتأمين تنسيق هذه المشاريع في سياق الأنشطة الشاملة التي يقوم بها الاتحاد بناء على دوره كجهة تنسيق/تسهيل في خط العمل جيم5 للقمة العالمية؛

4 بتنسيق هذه المشاريع مع أنشطة وبرامج لجان دراسات قطاع التنمية بشأن هذا الموضوع؛

5 بمواصلة التعاون مع المنظمات ذات الصلة بغية تبادل أفضل الممارسات ونشر المعلومات من خلال ورش عمل ودورات تدريبية مشتركة على سبيل المثال؛

6 بتقديم تقرير سنوي إلى المجلس عن هذه الأنشطة وعرض مقترحات حسب الاقتضاء.

استعراض عام لأنشطة قطاع تنمية الاتصالات في الاتحاد فيما يتعلق بتنفيذ خط العمل جيم5 للقمة WSIS – بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات

1. مقدمة

تتوافر لتكنولوجيا المعلومات والاتصالات إمكانية تقديم الخدمات الأساسية من خلال الصحة الإلكترونية والتعليم الإلكتروني والتجارة الإلكترونية والحكومة الإلكترونية إلى سكان البلدان النامية حيث لا يزال مواطنون كثيرون لا تتوافر لهم سبل النفاذ إلى الأبنية التحتية المادية من مثل المستشفيات والمدارس أو خدمات الإدارة العمومية.

وأصبحت المعاملات الإلكترونية بين الأطباء والمرضى، والنفاذ إلى خدمات الإدارة العمومية على الخط، واستعمال الإنترنت لبيع السلع والخدمات إلى زبائن مقيمين في أماكن نائية ممكنة اليوم نتيجة للتقدم المحرز في ميادين تكنولوجيا المعلومات والاتصالات. وإن الإمكانيات التي تتيحها تطبيقات تكنولوجيا المعلومات والاتصالات في سد بعض الفجوات فيما يتعلق بالنفاذ إلى الخدمات الأساسية وتمكين البلدان النامية من أن تصبح مشاركة مشاركةً كاملة في مجتمع المعلومات ويمكن أن تصبح حقيقة واقعة.

ولا يمكن تحقيق فوائد مجتمع المعلومات للحكومات ودوائر الأعمال والمواطنين تحقيقاً كاملاً إلاّ إذا تم تناول الشواغل المتعلقة بالأمن والثقة ووضع حلول لمعالجة مسائل الجريمة السيبرانية والتشريعات القابلة للنفاذ وسرقة الهوية، وسرية البيانات وحماية أنظمة المعلومات البالغة الأهمية. وإن الاعتماد الكبير على تكنولوجيا المعلومات والاتصالات كوسيلة لتعزيز التنمية الاجتماعية والاقتصادية والسرعة التي يمكن بها النفاذ إلى أنظمة المعلومات والبيانات البالغة الأهمية وتداولها وإتلافها قد وضع مسألة الأمن السيبراني في قمة جدول الأعمال باعتباره أحد التحديات الرئيسية التي تواجه مجتمع المعلومات الناشئ والاقتصاد القائم على المعرفة.

2. الأنشطة والمبادرات

يتخذ الاتحاد الدولي للاتصالات مع شركائه إجراءات كثيرة ترمي إلى بناء الثقة والأمن فيما يتعلق باستعمال تكنولوجيا المعلومات والاتصالات كجزء من اختصاصات الاتحاد التي اعتمدها الأعضاء في مؤتمرات المندوبين المفوضين والمؤتمرات والجمعيات العالمية وفي الاضطلاع بدوره كوسيط/منسق لخط العمل ج.5 للقمة WSIS.

ويعرض هذا التقرير بإيجاز بعض الإجراءات التي نُفّذت والبعض الآخر المخطط لتنفيذه. ويجمع التقرير هذه الإجراءات في خمسة مجالات رئيسية للأنشطة (**تأمين تطبيقات تكنولوجيا المعلومات والاتصالات، التشريعات والسياسات والاستراتيجيات وبناء القدرات، إذكاء الوعي، والتعاون فيما بين الأعضاء**). ويتضمن التقرير أيضاً بعض الإحالات إلى مصادر معلومات أخرى بشأن الأنشطة المتعلقة بتحقيق أهداف خط العمل ج5 للقمة WSIS، كما يدعو جميع الأطراف المهتمة إلى الانضمام إلى الجهود المبذولة في مجال بناء الثقة والأمن فيما يتعلق بتكنولوجيا المعلومات والاتصالات.

1.2 تأمين تطبيقات تكنولوجيا المعلومات والاتصالات – تنفيذ المشاريع

تمثل الشواغل المتعلقة بالأمن عائقاً أمام استعمال تكنولوجيا المعلومات والاتصالات بالنسبة لبعض الخدمات ذات المهام البالغة الأهمية من مثل الحكومة الإلكترونية، والتجارة الإلكترونية والمدفوعات الإلكترونية والصحة الإلكترونية حيث من المهم حماية البيانات الحساسة، وضمان سلامة البيانات والمعاملات، وتحديد هويات الأطراف. ومن خلال تناول

مسائل الأمن والثقة هذه ووضع حلول عملية، يمكن تحقيق الإمكانيات الحقيقية لتكنولوجيا المعلومات والاتصالات فيما يتعلق بتقديم خدمات ميسورة التكلفة وذات قيمة مضافة.

وكان من شأن الحلول العملية التي تكفل تحقيق فعالية إمكانيات تكنولوجيا المعلومات والاتصالات في تقديم الخدمات البالغة الأهمية والمستندة إلى التكنولوجيا المحققة للأمن والثقة أن مكنت البلدان من السير قدماً من أنظمة نشر المعلومات البسيطة إلى إجراء المعاملات البالغة الأهمية وتقديم طائفة واسعة من الخدمات للسكان.

وبفضل الاتحاد الدولي للاتصالات، أصبحت بلدان نامية عديدة لأول مرة مشاركة نشطة في نشر واستعمال الحلول المستندة إلى تكنولوجيات تحقيق الأمن والثقة، مما زاد من فوائد تكنولوجيا المعلومات والاتصالات في مجالات من مثل الخدمات الحكومية والخدمات الصحية.

وقد نُفِّذت وتنفَّذ مشاريع تستخدم التكنولوجيات المتقدمة في مجال بناء الأمن والثقة بالاستناد إلى الأبنية التحتية للمفاتيح العمومية (PKI) بما في ذلك الاستيقان الإحصائي الحيوي، والبطاقات الذكية، والشهادات الرقمية وتقنيات التواقيع الرقمية ITU-T X.509 في **بربادوس**، **وبوتان**، **وبلغاريا**، **وبوركينا فاصو**، **وكمبوديا**، **والكاميرون**، **وكوت ديفوار**، **وجورجيا**، **وجامايكا**، **وباراغواي**، **وبيرو**، **والسنغال**، **وتركيا**، **وزامبيا** ومشاريع أخرى من المخطط تنفيذها في عام 2007.

1.1.2 جورجيا

يتصدى مشروع الاتحاد الدولي للاتصالات هذا للتحديات التي يواجهها من خلال تقديم حلول تتسم بالفعالية بالقياس إلى التكلفة من أجل الإرسال والنفاذ والمعالجة المُؤمَّنين للوثائق الحكومية المرقمنة، ومن ثم زيادة كفاءة وشفافية الخدمات الحكومية. وقد زوِّد كبار المسؤولين في وزارة النقل والاتصالات في جورجيا بحلول ترمي إلى تعزيز أوتوماتية تدفق العمل وتمكين المسؤولين من التوقيع والنشر الرقميين للوثائق الرسمية ومن ثم الاستعاضة عن الأساليب الورقية البطيئة العالية التكلفة. وأمكن توفير النفاذ المخوّل إلى الوثائق الحساسة من خلال حلول تقوم على الأمن والثقة لتحديد هويات الموظفين المخولين داخل الوزارة.

2.1.2 باراغواي

وفّر هذا المشروع لمشغلي وموردي الخدمات منصة لآلية مؤمَّنة وموثوقة تستند إلى الإنترنت من أجل تبادل المعلومات الحساسة (من مثل الإقرارات عن الدخل) في نسق إلكتروني مع الوكالة الوطنية القائمة بالتنظيم (CONATEL). وينفذ هذا المشروع حلولاً لتكنولوجيا المعلومات والاتصالات مؤمَّنة وموثوقة بدرجة عالية من أجل تبسيط عملية إصدار التراخيص إلى مشغلي الهواتف العمومية وزيادة الكفاءة في العمليات التجارية للهيئة التنظيمية.

3.1.2 بربادوس وجامايكا

قُدِّمت المساعدة من أجل وضع إطار للسياسة العامة الوطنية فيما يتعلق باستعمال التصديق الرقمي وعمليات سلطات التصديق. كما شملت مساعدة الاتحاد تحديد مواصفات التكنولوجيا وتقديم إرشادات بشأن السياسات العامة من أجل تنفيذ برنامج وطني في بربادوس وجامايكا من أجل إصدار وإدارة الشهادات الرقمية، وتوفير خدمات استيقان قوية وضمان الأمن والثقة لمعاملات الحكومة الإلكترونية والأعمال التجارية الإلكترونية. وبالنسبة لجامايكا بعد اعتماد قانون المعاملات الإلكترونية من قبل البرلمان في نهاية عام 2006، قُدمت مساعدة الخبراء من أجل ضمان أن يكون برنامج إدارة الهوية والسياسات العامة المتعلقة به متفقة مع التشريعات. واشترك الاتحاد مع حكومة جامايكا في تمويل البنية التحتية العمومية الرئيسية الوطنية والتي من المقرّر أن تباشر عملها في عام 2007.

4.1.2 الكاميرون

يمكّن مشروع الاتحاد هذا من الإرسال المؤمّن للوثائق الحكومية الحساسة عن طريق الإنترنت، ويوفر خدمات حكومية على الهواء قائمة على الإنترنت إلى المواطنين في المناطق الحضرية والنائية حيث لا وجود للبنية التحتية الإدارية المادية. واستناداً إلى التوقيعات الإلكترونية وتكنولوجيات التجفير، فإن حلولاً من مثل الاستيقان القوي، وسريّة البيانات، وسلامتها، وعدم التنصل جعلت في الإمكان التصدي لبعض تهديدات الأمن السيبراني بما في ذلك سرقة الهوية.

5.1.2 بلغاريا

تمكّن المساعدة التي يقدّمها الاتحاد في مجال تنفيذ خطة للأمن السيبراني من تحقيق درجة عالية من الأمن للاتصالات بين وزارة النقل والاتصالات ووزارة المالية ومجلس الوزراء ولجنة تنظيم الاتصالات (CRC)، باستعمال البنية التحتية للمفاتيح العمومية PKI والتطبيقات التمكينية لهذه البنية. وتتيح التفاعل المؤمّن والفعّال والمتسم بالفعالية بالقياس إلى تكلفة بين كبار المسؤولين الحكوميين مما يعزّز عقد الاجتماعات المباشرة ويزيد الإنتاجية. ويتم التأمين والتوقيع الرقمي لجميع البيانات المتبادلة بين المسؤولين المشاركين باستعمال الوسائل التي تكفل سرية البيانات، وعدم التنصل، وسلامة البيانات، وتقنيات الاستيقان القوي المستند إلى الشهادات.

6.1.2 تركيا

يتمثل أحد الأهداف الاستراتيجية لهذا المشروع في تحسين خدمات الرعاية الصحية في تركيا من خلال استحداث وسيلة مؤمنة لتوفير المعلومات الصحية تمكّن مقدمي خدمات الرعاية الصحية (الأولية والثانوية) والمهنيين في المجال الصحي والمواطنين من النفاذ السهل الآمن إلى المعلومات المتعلقة بالصحة من خلال استعمال آخر تطورات تكنولوجيا المعلومات والاتصالات.

وتتمثل الأركان الأساسية للمشروع في استحداث نظام لمعلومات الرعاية الصحية الأولية يدعم نظام أطباء الأسرة، وتنفيذ السجلات الصحية الإلكترونية ووضع أنظمة قابلة للتشغيل البيني بين مقدمي خدمات الرعاية الصحية بما في ذلك مراكز الرعاية الصحية الأولية والمستشفيات ووكالات التأمين العمومية/الخاصة.

7.1.2 بوتان

بغية التصدي لاحتياجات سكان الريف فيما يتعلق بالوصول إلى الخدمات التي تتطلب السفر عدّة أيام إلى العاصمة الإدارية، نفّذ الاتحاد مشروعاً وطنياً يستند إلى البنية التحتية للمفاتيح العمومية بما في ذلك الاستيقان البيولوجي الإحصائي والتجفير القوي والتكنولوجيات التي تكفل سلامة البيانات من أجل بوتان. وتوفّر خطة الأمن السيبراني هذه التي يمولها الاتحاد وحكومة بوتان الخدمات من أجل إدارة الهوية والتحقق منها، والاستيقان المستند إلى الشهادات، والتوقيعات الرقمية، وسرية البيانات، وخدمات سلامة البيانات. وبفضل دعم الاتحاد هذا سيكون في استطاعة المستعملين المقيمين في الأماكن النائية في بوتان النفاذ إلى الخدمات البالغة الأهمية المستندة إلى التكنولوجيات الموفِّرة للثقة والأمن وبالتالي زيادة مقدرات وفوائد تكنولوجيا المعلومات والاتصالات فيما يتعلق بتقديم الخدمات إلى سكان الريف والحضر.

8.1.2 المشروع العالمي بشأن الأمن السيبراني ومكافحة الرسائل الاقتحامية

نظّم الاتحاد الاجتماع الأول للدول الأعضاء وأعضاء القطاعات لمناقشة سبل تعزيز التعاون بشأن الأمن السيبراني بما في ذلك مكافحة الرسائل الاقتحامية. وكان الغرض من الاجتماع هو تحقيق الأهداف الرئيسية الثلاثة التالية:

أ) التوصل إلى فهم مشترك، وربما إلى اتفاق في ميادين الأمن السيبراني والرسائل الاقتحامية حيث تلزم آلية لتعزيز التعاون فيما بين الدول الأعضاء.

ب) تحديد الآليات الممكنة اللازمة للتوصل ضمن جملة أمور، إلى مذكرة للتفاهم بين الدول الأعضاء المهتمة من أجل تعزيز التعاون بشأن الأمن السيبراني بما في ذلك بشأن مكافحة الرسائل الاقتحامية.

ج) تقديم مقترحات تستند إلى المساهمات المقدمة من الأعضاء في شكل تقارير لتقديمها إلى مؤتمر المندوبين المفوضين لعام 2006 من أجل النظر فيها.

وقد نجم عن الاجتماع تحديد الأعضاء للتحديات الرئيسية الحيوية (انظر القائمة الواردة أدناه) التي تواجه التعاون العالمي في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية.

أ. بناء الوعي الأساسي

ب. وضع وسن تشريعات وطنية ملائمة وقوية

ج. بناء القدرات البشرية والمؤسسية

د. الإنفاذ (مجال بناء القدرات)

هـ. الاستراتيجيات والسياسات الوطنية في مجال الأمن السيبراني

و. تيسير تبادل المعلومات بين البلدان وأصحاب المصلحة المعنيين

ز. إنشاء نقاط اتصال وطنية

ح. رصد وتقييم التقدم في مجال المبادرات القائمة

ط. تنفيذ حلول من أجل الاستجابة للحوادث ومراقبتها والإنذار بشأنها

ي. تقييم مواطن الضعف والتهديدات فيما يتعلق بالأمن السيبراني

ك. توفير الأدوات والتطبيقات الفعالة للشبكات والأمن السيبراني

ل. الشراكات

م. التعاون الدولي

وتوصل الاجتماع إلى توافق في الآراء بأن الاتحاد ينبغي له أن يؤدي دوراً رئيسياً في تحقيق الارتباط بين المبادرات القائمة، وتوفير إطار توحيدي يجمع ما بين المبادرات القائمة وهدف تلبية احتياجات البلدان النامية. وقُدّم التقرير الخاص بهذا الاجتماع إلى مؤتمر المندوبين المفوضين للاتحاد الذي عُقد في أنطاليا في 2006 الذي أقر أيضاً نشاطاً رئيسياً للاتحاد يتمثل في إنشاء آلية للتعاون في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية. وسيُنفّذ من خلال مشروع عالمي معنون: مشروع تعزيز التعاون بشأن الأمن السيبراني ومكافحة الرسائل الاقتحامية، وسيستغرق المشروع مدة أربع سنوات تبدأ من عام 2007. ويشكل المشروع جزءاً من الخطة التشغيلية لعام 2007 لقطاع تنمية الاتصالات في الاتحاد.

وفيما يتعلق بهذا المشروع:

- ينبغي للمشروع أن يأخذ في الحسبان أثناء عملية التنفيذ اختصاصات الاتحاد في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية.
- ينبغي للمشروع أن يرمي في المقام الأول إلى تقديم المساعدة إلى البلدان النامية في المجالات المعنية التي حددها الاجتماع والمذكورة أعلاه باعتبارها مجالات ذات أهمية حيوية للتعاون في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية.

- ينبغي للمشروع فيما يتعلق بالتشريعات ذات الصلة أن يأخذ في الحسبان حسب الاقتضاء العمل الذي يضطلع به مجلس أوروبا عند تقديمه المساعدة للبلدان في إعداد التشريعات الوطنية وذلك وفقاً لأحكام الاتفاقية المتعلقة بالجريمة السيبرانية.
- ينبغي أن يرتكز تنفيذ الأنشطة في إطار هذا المشروع على الطلبات التي أعربت عنها البلدان مع التأكيد على البلدان النامية بوجه خاص.
- ينبغي عرض المشروع بعد إعداده على كيانات التمويل المحتملة بما في ذلك الدول الأعضاء والقطاع الخاص والمنظمات الدولية مثل البنك الدولي والمفوضية الأوروبية.

2.2 التشريعات

مساعدة البلدان النامية في وضع قوانين نموذجية وقوانين لمكافحة الرسائل الاقتحامية

طلب المشاركون في ندوة الاتحاد العالمية للهيئات التنظيمية إلى الاتحاد مساعدتهم في وضع تشريع لمكافحة الرسائل الاقتحامية. ويصف ويحلل الفصل 7 من طبعة 2006 من منشور الاتحاد *اتجاهات ملحوظة في إصلاح الاتصالات*، محتويات قانون نموذجي لمكافحة الرسائل الاقتحامية، بما في ذلك الأحكام الخاصة بمدونات قواعد سلوك قابلة للإنفاذ ومعدة على نطاق محدود لمقدمي خدمات الإنترنت (ISP). ومن شأن مدونات السلوك القابلة للتنفيذ هذه أن تمنع زبائن مقدمي خدمات الإنترنت من استعمال نواتج مقدمي الخدمات هؤلاء، كمصدر للرسائل الاقتحامية وما يتصل بها من أعمال سيئة من مثل الخداع والاحتيال، كما ستمنع مقدمي خدمات الإنترنت من وضع ترتيبات للنظراء مع مقدمي خدمات إنترنت آخرين لا يتبعون مدونات سلوك مماثلة. والفصل 7، ***الاتجاهات الملحوظة في إصلاح الاتصالات 2006***، كبح الموجة الدولية للرسائل الاقتحامية، متيسر على الخط على العنوان التالي:

http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf

2.3 السياسات والاستراتيجيات وبناء القدرات

1.3.2 حلقات العمل والحلقات الدراسية

نظم الاتحاد الدولي للاتصالات حلقات عمل وحلقات دراسية وطنية وإقليمية تتناول السياسات والاستراتيجيات التكنولوجية فيما يتعلق بالأمن السيبراني في عدد من البلدان من مثل أذربيجان، بربادوس، الكاميرون، شيلي (بالنسبة لدول المخروط الجنوبي)، لاتفيا (بالنسبة لدول الجماعة الاقتصادية الأوروبية، وكومنولث الدول المستقلة ودول البلطيق)، منغوليا، باكستان، باراغواي، بيرو (بالنسبة لمنطقة جبال الأندين في أمريكا اللاتينية)، ورومانيا، وسيشل، والجمهورية العربية السورية وأوزبكستان.

ونُظمت أنشطة محددة لبناء القدرات البشرية والمؤسسية في مجال تكنولوجيات الأمن السيبراني وسياساته واستراتيجياته في الكاميرون وزامبيا وبربادوس وجامايكا وبلغاريا وبوتان وسورية.

2.3.2 اجتماع عالمي

نُظِّم في جنيف اجتماع عالمي حضره نحو 50 خبيراً في شؤون الأمن وأكثر من 500 مندوب يمثلون زهاء 120 بلداً لمناقشة مسائل التكنولوجيا والاستراتيجيات والسياسات والمسائل القانونية المتعلقة بالتوقيعات الإلكترونية، والتصديق الرقمي والحلول الخاصة بالتحفير من أجل البلدان النامية.

3.3.2 الندوة الإقليمية للاتحاد بشأن الحكومة الإلكترونية وبروتوكول الإنترنت من أجل المنطقة العربية

كانت المسائل المتعلقة بالأمن والثقة من المواضيع الرئيسية التي نوقشت في هذه الندوة التي أصدرت إعلان دبي الذي يؤكد على ضرورة مواصلة أنشطة الاتحاد في مجال الأمن السيبراني من أجل التطبيقات والخدمات الإلكترونية. وقد ضم هذا الاجتماع واضعي السياسة العامة من المنطقة العربية لمناقشة القضايا المشتركة ووضع إطار مشترك لمواجهة التحديات الرئيسية في مجال الأمن السيبراني. ومن المزمع في عام 2007 القيام بأنشطة للمتابعة في مجالات محددة موضع اهتمام للمنطقة (من مثل إدارة الهوية والتوقيعات الإلكترونية).

4.3.2 *ندوة الأمم المتحدة أثناء مؤتمر تكنولوجيا المعلومات في عالم الصحة*

نظم الاتحاد الدولي للاتصالات بالاشتراك مع منظمة الصحة العالمية واليونسكو ومعهد الأمم المتحدة للبحث والتدريب وشركاء من دوائر الصناعة ندوة للأمم المتحدة أثناء مؤتمر تكنولوجيا المعلومات في عالم الصحة كان فيه الأمن السيبراني من أجل الصحة أحد مواضيع المناقشة الرئيسية. وضمّت ندوة الأمم المتحدة التي نُظمت يوم 10 أكتوبر 2006 في معرض جنيف Palexpo أعضاء من أربع وكالات للأمم المتحدة لمناقشة مواضيع عدة من بينها الدور البالغ الأهمية للأمن السيبراني في المعاملات والتطبيقات الطبية والصحية. وللحصول على مزيد من المعلومات يمكن الاطلاع على العنوان التالي: http://www.worldofhealthit.org/about/about_partners.asp

4.2 إذكاء الوعي

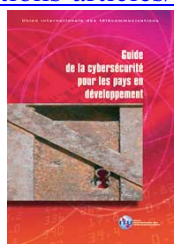
1.4.2 المطبوعات والمقالات

دليل الأمن السيبراني للبلدان النامية ©ITU 2006

Guide de la cybersecurité pour les pays en développement ©ITU 2006

أُعد دليل مرجعي للأمن السيبراني لمساعدة البلدان النامية وأقل البلدان نمواً على بناء قدرات محلية وإذكاء الوعي بشأن بعض التحديات الرئيسية في مجال الأمن من أجل مجتمع المعلومات. ويوضّح هذا الدليل المرجعي بعض المشاكل الرئيسية من مثل الرسائل الاقتحامية، والبرمجيات الضارة (الفيروسات والفيروسات المتسللة، والفيروسات المختبئة)، وسرية البيانات، وعدم الاستيقان، وضرورة المحافظة على سرية البيانات وسلامتها. وتشمل الموضوعات الأخرى التي تمت تغطيتها دراسة حالة عن التشريعات من الأجل الأمن السيبراني، وأمثلة للأساليب التي طُبّقت من أجل حماية البنية التحتية البالغة الأهمية. ويمكن تحميل نسخة من هذا الدليل باللغتين الإنكليزية والفرنسية مجاناً من موقع قطاع تنمية الاتصالات ITU-D على الويب على العنوان التالي:

http://www.itu.int/ITU-D/e-strategy/publications-articles/



بحث بشأن التشريع في مجال سرية البيانات والأمن ومنع الجريمة السيبرانية – ©ITU 2006

ثمة بعض جوانب لتكنولوجيا المعلومات والاتصالات تحتاج إلى حماية من منظور تشريعي، لا سيما فيما يتعلق بالتشريعات القائمة بشأن أمن البيانات وحقوق الملكية الفكرية، فضلاً عن الأشكال القديمة للجرائم التي تُرتكب على طريق المعلومات فائقة السرعة الجديد، من مثل الاحتيال والسلب. ومن الواضح أن التشريع يحتاج إلى مراجعة وموائمة

مع تكنولوجيا المعلومات والاتصالات فضلاً عن إدراك أن أنماطاً جديدة من الجرائم المتصلة بالحاسوب قائمة وأن أجهزة جديدة للأمن لازمة لاستيقان تدفقات المعلومات.

ويتناول هذا المطبوع البحثي المقتضيات التشريعية اللازمة لحماية المصالحة الوطنية للدول النامية وضمان تطور تكنولوجيا المعلومات والاتصالات والتجارة الإلكترونية مع تأمين البنية التحتية بحماية تشريعية ملائمة في الوقت ذاته. وهناك ثلاثة مبادئ شائعة أصبحت معترف بها باعتبارها مكونات هامة للأمن السيبراني. وتتمثل في السرية والتكاملية والتيسر مسائل الثلاث مجالات متراكبة مترابطة ترابطاً وثيقاً للغاية ومن الصعب أحياناً رسم خط دقيق بين مختلف الفئات وتحديد أي نمط من التشريعات يغطي مجالاً محدداً على النحو الملائم. ويمكن تحميل نسخة من هذا المطبوع من موقع الاستراتيجيات الإلكترونية للاتحاد على الويب على العنوان التالي:
http://www.itu.int/ITU-D/e-strategy/publications-articles/

دليل جديد للبلدان النامية بشأن الجريمة السيبرانية ITU 2007©

في حوالي نهاية عام 2006، أتم الاتحاد إعداد مادة مرجعية جديدة ترمي إلى إذكاء الوعي بشأن مسائل الجريمة السيبرانية، وتسهيل الأنشطة اللازمة لبناء القدرات البشرية والمؤسسية. كما تتناول الحاجة إلى تحقيق فهم مشترك للتهديدات السيبرانية وللتدابير المضادة لها. ويرمي هذا المطبوع الذي يتألف من 160 صفحة في المقام الأول إلى توفير إرشادات ومادة مرجعية للبلدان النامية. وهو يتضمن استعراضاً عاماً لمختلف أشكال الجرائم السيبرانية بما في ذلك ملامح المجرمين السيبرانيين. ويوضح مواطن الضعف الحالية في الإنترنت والهجمات السيبرانية، والأدلة الرقمية والمبادئ الأساسية وتقنيات التحقيق الخاصة بالحاسوب وتحقيقات الحاسوب كما يوفّر مسرداً بالمصطلحات والمراجع المتعلقة بالجريمة السيبرانية. وسيكون هذا الدليل الجديد والدليل السابق (بشأن الأمن السيبراني) أحد المواد المرجعية للأنشطة المخطط لها الرامية إلى بناء القدرات البشرية والمؤسسية في مجال الأمن السيبراني والجريمة السيبرانية. وسيترجم هذا الدليل الذي نُشِر أولاً بالإنكليزية إلى جميع لغات الاتحاد الست، وسيتيسر للبلدان المهتمة أثناء الربع الثاني من عام 2007 في نسق ورقي، ويمكن استجلابه من موقع الاتحاد على الويب.

5.2 التعاون فيما بين الأعضاء

وفر الاتحاد من أجل تسهيل تبادل الخبرات وأفضل الممارسات بين أعضائه، منصة من خلال لجنة دراسته التابعة لقطاع تنمية الاتصالات (ITU-D) يمكن للأعضاء من خلالها الاتفاق على نُهُج مشتركة في مواجهة التحديات القائمة في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية. وفي سبتمبر 2006، عُقد الاجتماع الأول للجنة الدراسات التابعة لقطاع تنمية الاتصالات لبحث المسائل المتعلقة بالأمن السيبراني وأقر الاجتماع برنامج العمل الخاص بهذه الدورة الجديدة. وبالنسبة للفترة 2006-2009 يشمل برنامج العمل والنواتج المتوقعة للجنة الدراسات التابعة للقطاع ITU-D المسائل التالية:

أ) دراسة وإحصاء ووصف العناصر التالية وزيادة التوعية بها:

- المسائل الرئيسية التي تواجه صانعي السياسات الوطنية وجميع أصحاب المصلحة، لبناء ثقافة الأمن السيبراني؛

- المصادر الرئيسية للمعلومات والمساعدة المتعلقة ببناء ثقافة الأمن السيبراني؛
- أفضل الممارسات الناجحة التي يستخدمها صانعو السياسات الوطنية من أجل تحديد وتنفيذ استراتيجية الأمن السيبراني بالتعاون مع جميع أصحاب المصلحة وبناء ثقافة الأمن السيبراني؛
- التحديات الفريدة من نوعها التي تواجه البلدان النامية في معالجة أمن الشبكات، وأفضل الممارسات الكفيلة بمواجهة هذه التحديات؛

ب) بحث أفضل الممارسات من أجل إنشاء وتشغيل وسائل المراقبة والإنذار والاستجابة لمقتضيات الحوادث والإصلاح، التي قد تستخدمها الدول الأعضاء من أجل بناء قدراتها الوطنية في هذا المضمار.

إصدار تقرير أو عدّة تقارير تُقدَّم إلى الأعضاء بشأن المسائل المحددة في القسم 2 أعلاه. وسيعكس التقرير أو التقارير المعنية واقع أن المعلومات المؤمَّنة وشبكات الاتصالات هي جزء لا يتجزأ من بناء مجتمع المعلومات، ومن التنمية الاقتصادية والاجتماعية لجميع الدول.

3. ملخص

يمثل الأمن السيبراني شاغلاً وينبغي أن يؤخذ في الاعتبار بصورة جدية من جانب جميع الدول. وبالنسبة للدول النامية يمكن لتطبيقات تكنولوجيا المعلومات والاتصالات المستندة إلى برامج مؤمَّنة وذات موثوقية عالية أن توفر خدمات بالغة الأهمية للسكان في مجالات من مثل الصحة والشؤون المالية والإدارة العمومية والتجارة.

ويمكن للبلدان المتقدمة أيضاً أن تحصد ثمار هذه الفوائد بالإضافة إلى ضرورة حماية بنيتها التحتية البالغة الأهمية والمحافظة على البيانات والمعاملات الحساسة.

ولا يمكن التصدي للتحديات الناشئة في هذا المجال إلاّ من خلال معالجة فعّالة عن طريق التعاون والتضافر بين الحكومات وأوساط الصناعة والمنظمات الدولية والمجتمع المدني وغيرها من أصحاب المصلحة ذوي الصلة. ويشكل إذكاء الوعي الأساسي بالتحديات والفرص، وبناء القدرات المحلية، ووضع التشريعات التي يمكن تنفيذها، وتنفيذ مشاريع تُقدم حلولاً مؤمَّنة وذات موثوقية عالية، ووضع سياسات ملائمة بعض المجالات الرئيسية التي ينبغي أن يعمل الشركاء فيها متضافرين من أجل تحقيق الهدف المُتفق عليه بوجه عام المتمثل في إقامة مجتمع معلومات شامل ومؤمَّن ومكفول للجميع.

ويضطلع الاتحاد الدولي للاتصالات في إطار اختصاصاته بمبادرات من خلال تنفيذ المشاريع وتسهيل تبادل المعلومات وبناء القدرات وإذكاء الوعي ووضع برامج للتعاون والشراكة من أجل معالجة القضايا المتعلقة بالأمن السيبراني على المستوى العالمي. وللتحرك قُدُماً صوب تحقيق الأهداف المُحدّدة في القمة العالمية لمجتمع المعلومات WSIS، يدعو الاتحاد جميع الشركاء المهتمين إلى الانضمام إلى جهوده المبذولة من أجل بناء الأمن والثقة في استعمال تكنولوجيا المعلومات والاتصالات.

الملحق D – الأسئلة الرئيسية لقطاع تقييس الاتصالات والمتعلقة بالأمن المطروحة للدراسة خلال فترة الدراسة 2005-2008

مقتبسة من

www.itu.int/ITU-T/studygroups/com17/questions.html

الأسئلة المخصصة للجنة الدراسات 17 التابعة لقطاع تقييس الاتصالات (فترة الدراسة 2005-2008)

لجنة الدراسات 17: الأمن، اللغات وبرمجيات الاتصالات

السؤال 2/17 خدمات الدليل، أنظمة الدليل، شهادات المفاتيح العامة/النعوت

1.2 خدمات الدليل

أ) ما هي تعاريف الخدمة الجديدة والمظاهر الجانبية اللازمة التي تستطيع أن تستفيد من تكنولوجيات الدليل التي تحظى بدعم واسع، مثل X.500 وLDAP؟

ب) ما هي التغيرات التي لحقت بالسلستين هاء وواو من التوصيات و/أو ما هي التوصيات الجديدة اللازمة لتعيين التعزيزات، وإصلاح الأعطاب، في التعاريف والمظاهر الجانبية لخدمة الدليل الحالية؟

2.2 أنظمة الدليل

أ) ما هي التعزيزات اللازم إدخالها على الدليل لزيادة دعم المستعملين الحاليين والمحتملين له، كزيادة اتساق معلومات الدليل عبر المواقع المستنسخة، ودعم التشغيل على المجاميع المتصاحبة لنعوت الدليل المحددة حسب المستعملين، وتحسين الأداء عند استعادة أعداد كبيرة من النتائج المعادة، أو حَسْم الارتباك الناتج عن إمساك مقدمي خدمات الدليل المتعددة بالمعلومات المختلفة تحت أسماء متماثلة تمام التماثل؟

ب) ما هي التعزيزات الأخرى اللازمة للدليل للسماح باستخدامه في البيئات المتنوعة، مثل، البيئات التي تعاني من ضيق الموارد كالشبكات اللاسلكية، والشبكات متعددة الوسائط؟

د) ما هي التعزيزات الأخرى اللازمة للدليل لتحسين دعمه لمجالات من قبيل الشبكة الذكية، وشبكات الاتصال وخدمات الدليل العمومية؟

هـ) ما هي التغييرات في سلسلة X.500 للتوصيات و/أو ما هي التوصيات اللازمة لتعيين التعزيزات للدليل أو لتصويب الأخطاء فيه؟

وسوف يتم عمل الأنظمة الدليلية بالتعاون والتضافر مع JTC 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC) في عملهما بشأن تمديد ISO/IEC 9594، الذي هو نص مشترك به التوصيتان X.500-X.530. وسوف يتم الحفاظ على الاتصال والتعاون الوثيق مع فريق مهام هندسة الإنترنت (IETF) ولا سيما في مجالات بروتوكول النفاذ لدليل الوزن الخفيف LDAP.

3.2 شهادات المفاتيح العمومية/النعوت

أ) ما هي التعزيزات اللازمة لشهادات المفاتيح العمومية والنعوت بحيث تسمح باستخدامها في البيئات المتنوعة، مثل، البيئات ضيقة الموارد كالشبكات اللاسلكية والشبكات متعددة الوسائط؟

ب) ما هي التعزيزات الأخرى اللازمة لشهادات المفاتيح العامة والنعوت لزيادة فائدتها في مجالات مثل الإحصاء البيولوجي (البيومتركس) والاستيقان والتحكم في النفاذ والتجارة الإلكترونية؟

ج) ما هي التغييرات على التوصية X.509 اللازمة لتحديد التعزيزات لـــ، وتصحيح الأعطاب في X.509؟

سوف تؤدي شهادات المفاتيح العمومية/النعوت عملها بالتعاون والتضافر مع JTC 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC) في عملها لتمديد ISO/IEC 9594-8، التي هي نص مشترك مع التوصيات X.509. وسوف تتم المحافظة على الاتصال والتعاون الوثيق مع فريق مهام هندسة الإنترنت (IETF) وبخاصة في مجالات البنية التحتية للمفاتيح العمومية.

السؤال 4/17 – مشروع أمن أنظمة الاتصالات

إن موضوع الأمن رحب المجال والمواضيع. إذْ يمكن تطبيق الأمن في كل منحى تقريباً من مناحي تكنولوجيا المعلومات والاتصالات ويمكن لنهج تحديد متطلبات الأمن أن يكون نهجاً:

- من القاعدة للقمة ينطبق حينما تتفق أذهان خبراء المنطقة عن تدابير أمنية لتقوية ولحماية ميدانهم الخاص بالشبكة، أي الإحصاء البيولوجي (البيوميتركس) والكتابة السرية، إلخ. وهذه هي الطريقة الأوسع انتشاراً غير أنها تتشظى بشأن الكيفية التي يجري بها الآن دراسة الأمن لدى منظمات متعددة.
- النهج النازل من القمة إلى القاعدة وهو الطريقة رفيعة المستوى والاستراتيجية للنظر إلى الأمن. وهو يحتاج إلى الإلمام بالصورة الكلية. وهو ذلك النهج الأكثر صعوبة لأن العثور على خبراء ذوي إلمام تفصيلي بكل جزئية من أجزاء الشبكة ومن ثم باحتياجات أمنها أصعب من خبراء المناطق ذوي المعرفة المحددة بمنطقة محددة أو اثنتين.
- وثمة بديل هو توليفة النهجين معاً الصاعد والنازل، مع بذل جهد للتنسيق للجمع بين الأجزاء المختلفة. وقد ثبت أن هذا الأمر يمثل تحدياً إلى أبعد الحدود مع اختلاف المصالح وجداول الأعمال.

وهذا السؤال مخصص لتحديد الرؤية ولتنسيق وتنظيم كامل نطاق أنشطة أمن الاتصالات داخل قطاع تقييس الاتصالات. وسوف يستخدم النهج النازل من القمة إلى القاعدة من خلال التعاون والتضافر مع لجان الدراسات الأخرى وتشغيلات بيانات المصدر (SDO) الأخرى. وهذا المشروع موجه نحو تحقيق المزيد من الجهود الهادفة على مستوى المشروع والمستوى الاستراتيجي.

الأسئلة

أ) ما هي التسليمات لمشروع أمن أنظمة الاتصالات؟

ب) ما هي العمليات وبنود العمل وطرق العمل والخط الزمني المحدد للمشروع لتحقيق هذه التسليمات؟

ج) ما هي المواجيز والكتيبات الأمنية التي يلزم إنتاجها والمثابرة عليها من جانب الاتحاد الدولي للاتصالات؟

د) ما هي الحلقات العملية اللازمة بشأن الأمن؟

هـ) ما الذي يلزم لبناء علاقات فعالة مع عمليات تشغيل بيانات المصدر (SDO) بغية النهوض بالعمل الخاص بالأمن؟

و) ما هي المعالم الرئيسية ومعايير النجاح؟

ز) كيف يمكن تحفيز عضو بالقطاع ومصلحة الإدارة والإبقاء على قوة الاندفاع بشأن أعمال الأمن؟

ح) كيف يمكن لجوانب الأمن أن تصير أكثر جاذبية للسوق؟

ط) كيف يمكن الإفصاح بوضوح عن المصلحة الحرجة للحكومات والحاجة العاجلة لحماية المصالح الاقتصادية العالمية، التي تعتمد على بنية تحتية متينة وآمنة للاتصالات؟

السؤال 5/17 – معمار الأمن وإطاره

إذ وضعنا في الاعتبار التهديدات الأمنية لبيئة الاتصالات والتقدم الراهن الذي لحق بإجراءات الأمن المضادة للتهديدات، فإنه ينبغي التحقيق في احتياجات الأمن الجديدة والحلول.

وينبغي دراسة أمن الأنواع الجديدة من الشبكات وكذلك أمن الخدمات الجديدة.

الأسئلة

أ) ما هي الكيفية التي ينبغي بها وضع تعريف كامل ومتماسك لحل أمن الاتصالات؟

ب) ما هو معمار حل كامل ومتماسك لأمن الاتصالات؟

ج) ما هو الإطار لتطبيق معمار الأمن لأجل وضع حل أمني جديد؟

د) ما هو الإطار اللازم لتطبيق معمار الأمن لأجل تقييم (ومن ثم تحسين) الحل الأمني القائم؟

هـ) ما هي الدعامات المعمارية للأمن؟

'1' ما هو معمار الأمن للتكنولوجيات البازغة؟

'2' ما هو معمار الأمن من طرف إلى طرف؟

'3' ما هو معمار الأمن لبيئة نقالة؟

'4' ما هي معمارات الأمن التقني اللازمة؟ مثلاً:

أ) ما هو معمار أمن الأنظمة المفتوحة؟

ب) ما هو معمار أمن الشبكات القائمة على بروتوكول الإنترنت؟

ج) ما هو معمار أمن شبكات الجيل الثاني (NGN)؟

و) كيف يمكن تعديل توصيات نموذج أمن الطبقة العليا والطبقة الأدنى بحيث تتناسب مع البيئة المتغيرة، وأي التوصيات الجديدة قد تكون لازمة؟

ز) كيف يمكن للمعايير المعمارية أن تُبَنين إزاء التوصيات الراهنة بشأن الأمن؟

ح) كيف يمكن تعديل توصيات الأمن الإطارية بحيث تتماشى مع التكنولوجيات البازغة، وأي التوصيات الإطارية الجديدة قد تلزم؟

ط) كيف تطبق خدمات الأمن لتوفير حلول أمنية؟

السؤال 6/17 – الأمن السيبراني

تم استحداث العديد من آليات الحماية والكشف مثل حوائط النيران وأنظمة كشف الاقتحام (IDS)، غير أن معظم هذه الآليات تسلط الضوء فقط على الجوانب التقنية. وعلى الرغم من أهمية هذه الحلول التقنية، فإن الأمر يحتاج إلى المزيد من البحث والمناقشة بشأن الأمن السيبراني من زاوية التقييس على المستوى الدولي.

الأسئلة

ينبغي إخضاع مجالات الأمن السيبراني التالية للدراسة:

- عمليات توزيع معلومات التعرض وتقاسمها وإفشائها؛
- تدبير موحد لعمليات مناولة الحوادث في الفضاء السيبراني؛
- استراتيجية لحماية البنية التحتية الحرجة للشبكات.

السؤال 7/17 – إدارة الأمن

الأسئلة

أ) ما هي الكيفية التي ينبغي بها تحديد وإدارة مخاطر الأمن في أنظمة الاتصالات؟

ب) ما هي الكيفية التي ينبغي بها تحديد وإدارة الأصول المعلوماتية لأنظمة الاتصال؟

ج) الكيفية التي ينبغي بها تحديد قضايا الإدارة النوعية للموجات الحاملة للاتصالات؟

د) ما هي الطريقة السليمة التي ينبغي بها إنشاء أنظمة إدارة أمن المعلومات (ISMS) للموجات الحاملة للاتصالات بما يتمشى مع المعايير الراهنة لـــISMS؟

هـ) ما هي الكيفية التي يمكن بها مناولة وإدارة حالات حدوث حوادث الأمن في الاتصالات؟

السؤال 8/17 – الإحصاءات الحيوية عن بعد

الأسئلة

أ) كيف يمكن تحسين تحديد هوية والاستيقان من المستعملين باستخدام طرق إحصائية حيوية عن بعد (telebiometric)؟

ب) كيف يستخدم الجزء الجديد من "المجموعة الفرعية الفيزيولوجية" للجنة الكهرتقنية الدولية IEC 60027 أن تستخدم في قطاع تقييس الاتصالات لتوفر عناصر لنموذج مناسب لتصنيف الأدوات الإحصائية الحيوية المأمونة عن بعد؟

ج) أي نظام مرجعي لمستويات الأمن ينبغي استخدامه لجلْب حلول مأمونة وآمنة في نظام هيرارشي؟

د) ما هي الكيفية التي ينبغي بها التعرف على قضايا تكنولوجيات الاستيقان الإحصائي الحيوي (البيومتري)؟

هـ) ما هي الكيفية التي ينبغي بها التعرف على احتياجات تكنولوجيات الاستيقان البيومتري للاتصالات القائمة على تكنولوجيا تجفيرية مثل البنية التحتية للمفاتيح العمومية؟

و) كيف يمكن التعرف على نموذج وتدبير لتكنولوجيا الاستيقان البيومتري للاتصالات القائمة على تكنولوجيا التجفير مثل البنية التحتية للمفاتيح العمومية؟

السؤال 9/17 – خدمات الاتصال الآمنة

الأسئلة

أ) ما هي الكيفية التي ينبغي بها التعرف على خدمات الاتصال وتعريفها في اتصال نقال أو خدمات ويب؟

ب) كيف يمكن التعرف على، والتعاطي مع، التهديدات الموجهة لخدمات الاتصالات؟

ج) ما هي تكنولوجيات الأمن لدعم خدمات الاتصال الآمنة؟

د) ما هي الكيفية التي ينبغي بها الحفاظ على الموصلية البينية لخدمات الاتصال وصيانتها؟

هـ) ما هي الأساليب التقنية للأمن اللازمة لخدمات اتصال آمنة؟

و) ما هي الأساليب التقنية أو البروتوكول اللازمة لخدمات الويب الآمنة البازغة؟

ز) ما هي بروتوكولات التطبيق الآمنة ينبغي تطبيقها لخدمات اتصال آمنة؟

ح) ما هي الحلول الأمنية العالمية لخدمات اتصال آمنة وتطبيقاتها؟

الملحق E – ثبت المراجع

نص مرجعي تعليمي يصف معايير الأمن لدى قطاع تقييس الاتصالات المنتشرة في عالم الاتصالات:

الأمن في الاتصالات وتكنولوجيا المعلومات: نظرة شاملة على القضايا ونشر توصيات قطاع تقييس الاتصالات لتحقيق أمن الاتصالات قطاع تقييس الاتصالات، أكتوبر 2004: http://www.itu.int/itudoc/itu-t/86435.html.

بعض الأعمال المرجعية

Ross Anderson: Security Engineering, A Guide To Building Dependable Distributed Systems, Wiley, 2001, ISBN 0-471-38922-6

Matt Bishop: Computer security: art and science, Addisson-Wesley, 2002, ISBN 0-201-44099-7

Ulyses Black: Internet Security Protocols, Protecting IP Traffic, Prentice Hall, ISBN 0-13-014249-2

Dorothy E. Denning: Information Warfare and Security, Addison-Wesley, 1999, ISBN 0-201-43303-6

Arnaud Dufour, Solange Ghernaouti-Hélie: *Internet – PUF, Que sais-je?* N° 3073 – ISBN 2-13-053190-3

Niels Ferguson, Bruce Schneier: Practical Cryptography, Wiley, 2003, ISBN 0-471-22357-3

Solange Ghernaouti-Hélie: *Internet & Sécurité – PUF Que sais-je?* N° 3609 – ISBN 2-13-051010-8

Solange Ghernaouti-Hélie: *Sécurité informatique et réseaux, cours et exercices corrigés* – Dunod 2006.

Raymond Panko: Corporate Computer and Network Security, Prentice Hall, 2004, ISBN 0-13-038471-2

Guillaume Poulin, Julien Soyer, Marc-Éric Trioullier: *Sécurité des architectures Web, «ne pas prévoir c'est déjà gémir»*, Dunod, 2004.

Bruce Schneier: Beyond Fear, Thinking Sensibly About Security In An Uncertain World, Copernicus Books, 2003, ISBN 0-387-02620-7

Bruce Schneier: Secrets and Lies: Digital Security in a Networked World, Wiley, 2000, ISBN

0-471-25311-1

Bruce Schneier: Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition, Wiley, 1996, ISBN 0-471-11709-9

Simon Singh: Histoire des codes secrets, JC Lattès, 1999, ISBN 2-7096-2048-0

William Stallings: Cryptography And Network Security, Principles and Practice, Prentice Hall, 1999, ISBN 0-13-869017-0

William Stallings: Network And Internetwork Security, Principles and Practice, Prentice Hall, 1995, ISBN 0-13-180050-7

William Stallings: Network Security Essentials, Applications and Standards, Prentice Hall, 2000, ISBN 0-13-016093-8

مواقع مرجعية

مواقع بالفرنسية:

French Prime Minister's site: http://www.premier-ministre.gouv.fr

(See in particular under: *Technologie de l'information dans la thématique: communication*)

http://www.internet.gouv.fr: site relating to development of the information society

French public service portal: http://www.service-public.gouv.fr. Leads to all online services, see under «*se documenter*»

French public service site on law: http://www.legifrance.gouv.fr

French documentation service site: http://www.ladocfrancaise.gouv.fr

http://www.foruminternet.org/: Information and discussion forum on law, the internet and networks

French National Civil Liberties Commission: http://www.cnil.fr

French Central Office for combating ICT-related crime:

http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

Information System and Network Security Observatory: http://www.ossir.org

Clusif: www.clusif.asso.fr.

Panorama of cybercrime: https://www.clusif.asso.fr/fr/production/ouvrages/

مواقع أخرى

CERT: www.cert.org (Computer Emergency Response Team)

NIST: http://www.nist.gov (US National Institute of Standards and Technology)

NSA: http://www.nsa.gov (US National Security Agency)

CSE: http://www.cse.dnd.ca (Canadian Telecommunication Security Centre)

CESG: http://www.cesg.gov.uk (UK National Technical Authority for Information Assurance)

BSI: http://www.bsi.bund.de (German Federal Information Security Office) – site in German and English

DSD: http://www.dsd.gov.au (Defence Signals Directorate operating in Australia and New Zealand).

Site devoted to digital watch and information security..

National White Collar Crime Center: IFCC – Internet fraud complaint center:

http://www1.ifccfbi.gov/index.asp; Internet Fraud – Crime Report – 2004:

http://www1.ifccfbi.gov/strategy/2004_IC3Report.pdf

رسائل إخبارية

Cryptogram – Bruce Schneier: [schneier@counterpane.com]

crypto-gram-list@listserv.modwest.com

Internet Rights Forum infoletter: infolettre@listes.foruminternet.org

US-CERT Security Bulletins: security-bulletins@us-cert.gov

Cyberpolice information letter: http://cyberpolice.over-blog.com/

cyberpolice.over-blog.com [newsletter@over-blog.com]

الملحق F – المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي بشأن أمن أنظمة وشبكات المعلومات: نحو ثقافة أمنية

تصدير

لقد تغير استخدام شبكات وأنظمة المعلومات وبيئة تكنولوجيا المعلومات كلية بصورة مثيرة منذ عام 1992، عندما وضعت المنظمة الدولية للتعاون والتنمية في المجال الاقتصادي لأول مرة: *المبادئ التوجيهية لأمن أنظمة المعلومات*. وتقدم هذه التغيرات المستمرة مميزات كبيرة، ولكن تتطلب أيضاً تركيزاً أكبر بكثير على الأمن، من جانب الحكومات ودوائر الأعمال والمنظمات الأخرى والمستعملين الآخرين الذين يطورون أو يمتلكون أو يوفرون أو يديرون خدمة ويستخدمون أنظمة وشبكات المعلومات (المشتركين).

لقد حلت أجهزة الكمبيوتر الشخصية الأكثر قوة والتكنولوجيات المتقاربة، والاستخدام واسع النطاق للإنترنت، محل الأنظمة البسيطة المعتمدة على ذاتها وذلك داخل شبكات مغلقة في الغالب.

أما اليوم، فيتزايد الاتصال البيني فيما بين المشتركين، وتعبر التوصيلات الحدود القطرية، وعلاوة على ذلك، فإن الإنترنت تدعم البنى التحتية الحرجة مثل الطاقة والنقل والمالية، وتلعب دوراً رئيسياً في كيفية أداء الشركات لأعمالها التجارية، وكيفية توفير الحكومات الخدمات للمواطنين والمؤسسات، وكيفية تواصل المواطنين فرادى وتبادلهم المعلومات. وقد تغيرت أيضاً طبيعة ونوعية التكنولوجيات التي تشكل البنية التحتية للاتصالات والمعلومات بشكل كبير. وكثرت أعداد وأشكال أجهزة النفاذ لتشمل الأجهزة الثابتة واللاسلكية والنقالة، وهناك نسبة متزايدة من النفاذ من خلال وصلات عاملة دائمة.

وكان من نتيجة ذلك أن اتسعت طبيعة وحجم وحساسية المعلومات المتبادلة قد بصورة كبيرة.

ونتيجة لتزايد التوصيلية البينية، أصبحت أنظمة وشبكات المعلومات الآن معرضة بشكل متزايد لأنواع مختلفة وعديدة من التهديدات ولأخطار التعرض، ومما يثير قضايا جديدة بالنسبة للأمن.

ومن أجل هذه الأسباب، تنطبق هذه المبادئ التوجيهية على كل المشتركين في مجتمع المعلومات الجديد، وتشير إلى الحاجة إلى المزيد من الوعي والفهم لمسألة الأمن والحاجة لبلورة ثقافة أمنية.

1.F نحو ثقافة أمنية

تستجيب هذه المبادئ التوجيهية لبيئة الأمن دائمة التغير، وذلك من خلال الترويج لبلورة ثقافة أمنية، بمعنى التركيز على الأمن أثناء تطوير أنظمة وشبكات المعلومات، واعتماد طرق جديدة في التفكير والسلوك لدى استعمال شبكات وأنظمة المعلومات، والتجاوب معها. والمبادئ التوجيهية إشارة إلى انقضاء العهد الذي كان التصميم واستخدام للشبكات والأنظمة الآمنة فيه ضرباً من الأفكار التي ترد متأخرة عن الفعل. وأصبح المشتركون اليوم يعتمدون بشكل متزايد على أنظمة وشبكات المعلومات والخدمات ذات الصلة، وكلها بحاجة لأن تكون محل ثقة وآمنة، والسبيل الوحيد لتوفير الأمن بشكل فعال هو اتباع نهج يراعي جيداً مصالح جميع المشتركين، وطبيعة الأنظمة والشبكات والخدمات ذات الصلة.

وكل مشترك عامل مهم لكفالة تحقيق الأمن، ويجب على المشتركين، حسبما يتناسب، طبقاً لدورهم، أن يكونوا على وعي بالمخاطر الأمنية ذات الصلة والتدابير الوقائية، وأن يتحملوا المسؤولية، وأن يتخذوا خطوات من أجل تعزيز أمن أنظمة وشبكات المعلومات.

وسوف يتطلب تعزيز الثقافة الأمنية كلا من القيادة والمشاركة الموسعة، ويجب أن يؤدي ذلك إلى الارتفاع بأولوية تخطيط وإدارة الأمن، فضلاً عن فهم الحاجة للأمن فيما بين المشتركين. وينبغي أن تكون مسائل الأمن موضوعات تثير الانشغال، وتكرس المسؤولية على كل مستويات الحكومة والأعمال التجارية، ولدى كل المشتركين. وتشكل هذه

المبادئ التوجيهية أساساً للعمل من أجل الوصول إلى الثقافة الأمنية في المجتمع بأكمله. وسوف يؤدي ذلك إلى تمكين المشتركين من وضع الأمن كعامل في تصميم واستخدام كل أنظمة وشبكات المعلومات، وتقترح هذه المبادئ التوجيهية أن يتبع جميع المشتركين وأن يعززوا ثقافة أمنية كطريقة للتفكير بشأن عمليات شبكات وأنظمة المعلومات وتقييمها والعمل على أساسها.

2.F الغايات

تهدف هذه المبادئ التوجيهية إلى:

- تشجيع ثقافة أمنية فيما بين جميع المشتركين كوسيلة لحماية أنظمة وشبكات المعلومات
- تعميق الوعي بشأن المخاطر بالنسبة لأنظمة وشبكات المعلومات: بما في ذلك السياسات العامة والممارسات والتدابير والإجراءات المتاحة لمواجهة هذه المخاطر، والحاجة إلى اتباعها وتنفيذها.
- بناء المزيد من الثقة بين جميع المشتركين في أنظمة وشبكات المعلومات، والطريقة التي يتم توفيرها واستخدامها من خلالها.
- خلق إطار مرجعي عام يساعد المشتركين على فهم أية مسائل تتعلق بالأمن واحترام القيم الأخلاقية في بلورة وتنفيذ سياسات عامة وممارسات وتدابير وإجراءات متماسكة، من أجل تحقيق أمن أنظمة وشبكات المعلومات.
- النهوض بالتعاون وتقاسم المعلومات، حيثما يتناسب، فيما بين جميع المشتركين في بلورة وتنفيذ السياسات العامة والممارسات والتدابير والإجراءات
- تشجيع اعتبار الأمن هدفاً مهماً فيما بين المشتركين الضالعين في بلورة أو تنفيذ المقاييس.

3.F مبادئ

المبادئ التسعة التالية يكمل كل منها الآخر وينبغي قراءتها ككل، وهي تُعنى بالمشتركين على كافة المستويات، بما في ذلك مستويات السياسات العامة والمستويات التشغيلية. وتتفاوت مسؤوليات المشتركين في إطار هذه المبادئ التوجيهية تبعاً لأدوارهم، وسوف يتم مساعدة كل المشتركين من خلال التوعية والتعليم وتقاسم المعلومات والتدريب، ويمكن أن يؤدي ذلك إلى التحلي بفهم أفضل للأمن وممارساته، ويجب أن تكون الجهود المبذولة لتعزيز أمن أنظمة وشبكات المعلومات متمشية مع قيم المجتمع الديمقراطي، وخاصة الحاجة إلى تدفق حر ومفتوح للمعلومات والمشاغل الأساسية بشأن الخصوصية الشخصية[65].

1) الوعي

ينبغي أن يكون المشتركون واعين بالحاجة إلى أمن أنظمة وشبكات المعلومات، وما الذي بإمكانهم عمله لتعزيز الأمن.

إن الوعي بالمخاطر والضمانات المتوافرة هو خط الدفاع الأول لأمن أنظمة وشبكات المعلومات. إذ يمكن أن تتأثر أنظمة وشبكات المعلومات بكل من المخاطر الداخلية والخارجية، وينبغي على المشتركين أن يفهموا أن القصور في

[65] بالإضافة إلى هذه المبادئ التوجيهية للأمن، فقد قامت منظمة التعاون والتنمية في الميدان الاقتصادي ببلورة توصيات تكميلية خاصة بمبادئ توجيهية بشأن مسائل أخرى هامة بالنسبة لمجتمع المعلومات العالمي، وهي تتصل بالخصوصية (*المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي لعام 1980 التي تنظم حماية الخصوصية وتدفقات البيانات الشخصية العابرة للحدود*) وبعلم التجفير (*المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي لعام 1997 بشأن السياسة العامة لعلم التجفير*)، ويجب قراءة المبادئ التوجيهية للأمن جنباً إلى جنب مع المبادئ التوجيهية الأخرى.

الأمن قد يسبب ضرراً كبيراً للأنظمة والشبكات الواقعة تحت سيطرتهم. ويجب أن يكونوا أيضا واعين بالضرر المحتمل الذي قد يلحق بالآخرين، والذي ينشأ عن الاتصالية البينية والاعتمادية المتبادلة. ويجب أن يكون المشتركون واعين بتشكيلة نظامهم والتحديثات المتاحة له وموقعه بداخل الشبكة، والممارسات الجيدة التي بإمكانهم تنفيذها لتعزيز الأمن، واحتياجات المشتركين الآخرين.

2) المسؤولية

جميع المشتركين مسؤولون عن أمن أنظمة وشبكات المعلومات

يعتمد المشتركون على أنظمة وشبكات المعلومات المتصلة بينياً وذلك على المستوى المحلي والعالمي، ويجب عليهم فهم مسؤوليتهم نحو أمن أنظمة وشبكات المعلومات هذه. يجب أن يكونوا مسؤولين بطريقة تتناسب مع أدوارهم الفردية. ويجب على المشتركين استعراض السياسات العامة والممارسات والتدابير والإجراءات الخاصة بهم بشكل دوري، وتقييم ما إذا كانت هذه الأمور ملائمة لبيئتهم. كما يجب على من يقومون بالتطوير والتصميم والإمداد للمنتجات والخدمات تناول أمن الأنظمة والشبكات وتوزيع المعلومات الملائمة، بما في ذلك التحديثات وفي التوقيت المناسب ليتمكن المستعملون من فهم الطبيعة الوظيفية للأمن بالنسبة للمنتجات والخدمات جيداً، وفهم مسؤولياتهم فيما يتصل بالأمن.

3) الاستجابة

يجب على المشتركين التصرف في التوقيت السليم وبشكل متعاون من أجل منع حوادث الأمن واكتشافها والاستجابة لها.

يجب على المشتركين بناء على إدراكهم للتوصيلية البينية لأنظمة وشبكات المعلومات التصرف في التوقيت السليم، وبشكل متعاون وذلك من أجل تناول حوادث الأمن. ويجب عليهم تقاسم المعلومات بشأن الأخطار وإمكانيات التعرض للضرر، حسبما يتناسب، وتنفيذ إجراءات للتعاون السريع والفعال من أجل منع حوادث الأمن واكتشافها والاستجابة لها، وحيثما يكون مسموحاً، قد يتضمن ذلك تقاسماً للمعلومات وتعاوناً عابر للحدود

4) الأخلاقيات

يجب أن يحترم المشتركون الاهتمامات المشروعة للآخرين.

نظراً لسعة انتشار أنظمة وشبكات المعلومات في مجتمعاتنا، فإن المشتركين يحتاجون إلى إدراك أن ما يعملونه أو ما يتقاعسون عن عمله قد يضر بالآخرين. ولهذا فإن السلوك الأخلاقي مهم للغاية، ويجب على المشتركين الاجتهاد من أجل بلورة واستخدام أفضل الممارسات، وللنهوض بالسلوك الذي يُقر بالاحتياجات الأمنية، ويحترم الحقوق المشروعة للآخرين.

5) الديمقراطية

يجب أن يكون أمن أنظمة وشبكات المعلومات متوافقاً مع القيم الأساسية لمجتمع ديمقراطي.

يجب تنفيذ الأمن بطريقة متماشية مع القيم التي تدركها المجتمعات الديمقراطية بما في ذلك حرية تبادل الخواطر والأفكار، والتدفق الحر للمعلومات وسرية المعلومات والاتصالات والحماية الملائمة للمعلومات الشخصية والانفتاح والشفافية.

6) تقييم المخاطر

يجب على المشتركين القيام بتقييم للمخاطر

يقوم تقييم المخاطر بتحديد المخاطر وأوجه التعرض، ويجب عليه أن يكون واسع القاعدة يشمل أهم العوامل الداخلية والخارجية، مثل التكنولوجيا والعوامل المادية والبشرية والسياسات العامة وخدمات الأطراف الثالثة التي لها تداعيات على الأمن. ويسمح تقييم المخاطر بتحديد مستوى المخاطر الذي يمكن قبوله والمساعدة في انتقاء أساليب الضبط الملائمة من أجل إدارة المخاطرة ذات الضرر المحتمل لأنظمة وشبكات المعلومات وذلك في ضوء طبيعة وأهمية المعلومات المطلوب حمايتها، ونظراً لتزايد التوصيلية البينية لأنظمة المعلومات، يجب على تقييم المخاطر أن يأخذ في الاعتبار الضرر المحتمل الذي قد ينشأ عن آخرين أو يلحق بآخرين.

7) تصميم الأمن وتنفيذه

ينبغي للمشتركين أن يدرجوا الأمن كعنصر أساسي في أنظمة المعلومات وشبكاتها

وهناك حاجة لتصميم الأنظمة والشبكات والسياسات العامة تصميماً سليماً، وتنفيذه وتصميمه لأجل تعظيم الأمن. وثمة تركيز رئيسي وإن كان غير حصري لهذا الجهد ينصب على التصميم واعتماد الإجراءات الوقائية المناسبة والحلول لتفادي أو الحد من الضرر المحتمل الذي ينجم عن تهديدات وجوانب تعرض معروفة. فالإجراءات الوقائية والحلول سواء التقنية أو غير التقنية مطلوبة يجب أن تتناسب مع قيمة المعلومات الموجودة على أنظمة وشبكات المنظمة. وينبغي للأمن أن يكون عنصراً أساسياً لكل النواتج والخدمات والأنظمة والشبكات، وجزءاً لا يتجزأ من تصميم النظام ومعماره. وبالنسبة للمستعملين النهائيين يتألف التصميم الأمني والتنفيذ إلى حد بعيد من اختيار وتشكيل النواتج والخدمات لأنظمتهم

8) إدارة الأمن

ينبغي للمشتركين اتباع نهج شامل نحو إدارة الأمن

يجب أن تنبني إدارة الأمن على تقييم المخاطر، ويجب أن تكون دينامية وشاملة لكل مستويات أنشطة المستعملين وكافة أوجه عملياتهم التشغيلية، ويجب أن تشمل استجابات تطلعية إزاء التهديدات التي تظهر، وأن تتناول الحماية والاكتشاف والاستجابة للحوادث، واستعادة الأنظمة، والصيانة الجارية، والمراجعة والتدقيق. يجب أن يتم تنسيق السياسات العامة والممارسات والتدابير والإجراءات وإدماجها من أجل إنشاء نظام متماسك للأمن. وتعتمد متطلبات إدارة الأمن على مدى المشاركة ودور المشتركين والمخاطر الكامنة ومتطلبات النظام.

9) إعادة التقييم

ينبغي على المشتركين مراجعة وإعادة تقييم أمن المعلومات والشبكات، وإجراء التعديلات الملائمة للسياسات العامة للأمن والممارسات والإجراءات والتدابير الخاصة به.

يتواصل باستمرار اكتشاف التهديدات وجوانب التعرض الجديدة والمتغيرة، ويجب على المشتركين مداومة مراجعة وإعادة تقييم وتعديل كل جوانب الأمن من أجل التعامل مع هذه المخاطر المتطورة.

توصية المجلس الخاصة بالمبادئ التوجيهية لأمن أنظمة وشبكات المعلومات– نحو ثقافة أمنية

إن المجلس،

إذْ يأخذ في اعتباره اتفاقية منظمة التعاون والتنمية في الميدان الاقتصادي المؤرخة في 14 ديسمبر 1960 وخاصة المواد 1 ب)، 1 ج)، 3 أ) و 5 ب) منه؛

وإذْ يضع في اعتباره توصيات المجلس بشأن المبادئ التوجيهية التي تنظم حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود المؤرخة في 23 سبتمبر 1980 [C(80) 58 (Final)] ؛

وإذْ يضع في اعتباره الإعلان بشأن تدفقات البيانات الشخصية عبر الحدود الذي اعتمدته حكومات البلدان الأعضاء في منظمة التعاون والتنمية في الميدان الاقتصادي بتاريخ 11 أبريل 1985 [(ملحق الوثيقة (139 (85)C]؛

وبالنظر إلى توصية المجلس بشأن المبادئ التوجيهية للسياسة العامة للتجفير المؤرخة في 27 مارس 1997 [(الوثيقة C(97)62/FINAL)]؛

وإذْ يأخذ في اعتباره الإعلان الوزاري بشأن حماية الخصوصية في الشبكات العالمية بتاريخ 7-9 ديسمبر 1998 [(ملحق الوثيقة C(98)177/FINAL)]؛

وإذْ يضع نصب عينيه الإعلان الوزاري بشأن الاستيقان من التجارة الإلكترونية بتاريخ 7-9 ديسمبر 1998 [(ملحق الوثيقة C(98)177/FINAL)]؛

وإذْ يُقر بأن أنظمة وشبكات المعلومات يتزايد استخدامها وقيمتها بالنسبة للحكومات وللأعمال التجارية والمنظمات الأخرى والمستعملين فرادى؛

وإذْ يُقر بأن الدور المتزايد الأهمية لأنظمة وشبكات المعلومات والاعتماد المتنامي عليها من أجل الاستقرار والفعالية للاقتصاديات الوطنية والتجارة الدولية وللحياة الاجتماعية والثقافية والسياسية، يدعو إلى بذل جهود خاصة لحماية وبناء الثقة فيها؛

وإذْ يُقر بأن أنظمة وشبكات المعلومات وانتشارها عالمياً قد صاحبته مخاطر جديدة ومتزايدة؛

وإذْ يُقر بأن البيانات والمعلومات المخزونة في أنظمة وشبكات المعلومات والمرسلة عبرها هي عرضة للتهديدات من قبل العديد من الوسائل غير المصرح بها للنفاذ والاستخدام والاختلاس والتغيير والتبديل وعمليات الإرسال الخبيثة للشفرات ومنع الحصول على الخدمة أو التدمير، وتتطلب إجراءات وقائية مناسبة؛

وإذْ يُقر بأن هناك حاجة لرفع الوعي بمخاطر أنظمة وشبكات المعلومات وبالسياسات العامة والممارسات والتدابير والإجراءات للاستجابة لتلك المخاطر، ولتشجيع السلوك الملائم كخطوة مهمة للغاية نحو بلورة الثقافة الأمنية؛

وإذْ يدرك أن هناك حاجة لاستعراض السياسات العامة والممارسات والتدابير والإجراءات الحالية من أجل المساعدة في التأكد من تصديها للتحديات المتنامية التي تطرحها مخاطر أنظمة وشبكات المعلومات؛

وإذْ يدرك أن هناك مصلحة مشتركة في النهوض بأمن أنظمة وشبكات المعلومات من خلال الثقافة الأمنية التي ترعى التنسيق والتعاون الدولي من أجل ملاقاة التحديات التي تطرحها الأضرار المحتملة لحالات القصور الأمني على الاقتصاديات الوطنية والتجارة الدولية والمشاركة في الحياة الثقافية والاجتماعية والسياسية؛

وإذْ يدرك أيضاً أن *(المبادئ التوجيهية لأمن أنظمة وشبكات المعلومات – نحو ثقافة أمنية)* الموضحة هذا في ملحق هذه التوصية إنما هي أمور طوعية، ولا تؤثر على حقوق السيادة للدول؛

وإذْ يدرك أن هذه المبادئ التوجيهية ليس المقصود منها الإشارة إلى وجود حل واحد للأمن أو إلى أية سياسات عامة أو ممارسات أو تدابير أو إجراءات ملائمة لأي موقف بعينه، وإنما هي بالأحرى من أجل توفير إطار من المبادئ للارتقاء بالفهم لكيفية استفادة المشتركين من بلورة ثقافة أمنية وأيضاً إضافتهم إليها.

يثني على هذه *(المبادئ التوجيهية لأمن أنظمة وشبكات المعلومات – نحو ثقافة أمنية)* للحكومات والأعمال التجارية والمنظمات الأخرى والمستعملين الأفراد الذين يقومون بتطوير وامتلاك وتوفير وإدارة وخدمة واستخدام أنظمة وشبكات المعلومات .

ويوصـــي بأن تقوم البلدان الأعضاء:

بإرساء سياسات عامة أو ممارسات أو تدابير أو إجراءات جديدة أو تعديل ما هو قائم منها، لكي تعكس وتراعي *(المبادئ التوجيهية لأمن الأنظمة والشبكات – نحو ثقافة أمنية)* عن طريق اتباع وتشجيع ثقافة أمنية على نحو ما وردت في المبادئ التوجيهية؛

بالتشاور والتنسيق والتعاون على المستويات الوطنية والدولية لتنفيذ المبادئ التوجيهية،

بنشر المبادئ التوجيهية في أرجاء القطاعين العام والخاص، بحيث يشمل ذلك الحكومات والأعمال التجارية والمنظمات الأخرى والمستعملين الأفراد، وذلك لتعزيز الثقافة الأمنية، ولتشجيع كل الأطراف المعنية على تحمل المسؤولية واتخاذ الخطوات الضرورية من أجل تنفيذ المبادئ التوجيهية بطريقة ملائمة لأدوارها الفردية.

توفير المبادئ التوجيهية للبلدان غير الأعضاء، وذلك في الوقت المناسب وبالشكل السليم؛

مراجعة المبادئ التوجيهية كل خمس سنوات من أجل رعاية التعاون الدولي بشأن المسائل المتعلقة بأمن أنظمة وشبكات المعلومات؛

يكلف لجنة منظمة التعاون والتنمية في الميدان الاقتصادي بشأن السياسة العامة للمعلومات والحاسوب والاتصال بتعزيز تنفيذ المبادئ التوجيهية؛

تحل هذه التوصية محل توصية المجلس بشأن المبادئ التوجيهية لأمن أنظمة المعلومات المؤرخة في 26 نوفمبر 1992 [(الوثيقة C(92)188/FINAL)]؛

التاريخ الإجرائي

استُكملت المبادئ التوجيهية بشأن الأمن لأول مرة في عام 1992 وتمت مراجعتها في 1997، وأُجريت المراجعة الحالية في عام 2001 من خلال الطرف العامل بشأن أمن وخصوصية المعلومات (WPISP) وذلك تبعاً لولاية لجنة السياسة العامة للمعلومات والحاسوب والاتصال (ICCP) وتسارعت في أعقاب حادث 11 سبتمبر المؤسف.

تمت صياغة مشروع الوثيقة على يد فريق من الخبراء من الطرف العامل بشأن أمن وخصوصية المعلومات (WPISP) الذي اجتمع في واشنطن في 10-11 ديسمبر 2001، وسيدني في 12-13 فبراير 2002 وباريس في 4 و6 مارس 2002، واجتمع الطرف في باريس 5-6 مارس 2002 و22-23 أبريل 2002 و25-26 يونيو 2002.

وقد تم اعتماد هذه الوثيقة لمنظمة التعاون والتنمية في الميدان الاقتصادي *(المبادئ التوجيهية لأمن أنظمة وشبكات المعلومات: نحو ثقافة أمنية)* كتوصية مجلس المنظمة في دورته رقم 1037 بتاريخ 25 يوليو 2002.

الاتحاد الدولي للاتصالات
مكتب تنمية الاتصالات (BDT)
Place des Nations, CH-1211, GENEVA 20
Switzerland

ولمزيد من المعلومات يُرجى الاتصال
بشعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني
البريد الإلكتروني: cybmail@itu.int
الموقع الإلكتروني: www.itu.int/ITU-D/cyb

طبع في سويسرا
جنيف، 2009