الاتحـاد الـدولي للاتصـالات
قطـاع التنميـة

منشورات ITU
فترة الدراسة 2018-2021

لجنة الدراسات 2 المسألة 3

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

التقرير النهائي للمسألة 3/2 لقطاع تنمية الاتصالات

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

فترة الدراسة 2018-2021

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني: التقرير النهائي للمسألة 3/2 لقطاع تنمية الاتصالات لفترة الدراسة 2018-2021

ISBN 978-92-61-34106-0 (النسخة الإلكترونية)
ISBN 978-92-61-34116-9 (نسخة EPUB)
ISBN 978-92-61-34126-8 (نسخة Mobi)

شكر وتقدير

تمثل لجان الدراسات لقطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات (ITU-D) منصة محايدة يلتقي في إطارها خبراء من الحكومات ومن دوائر الصناعة ومنظمات الاتصالات والهيئات الأكاديمية من جميع أنحاء العالم لإنتاج الأدوات والموارد العملية لمعالجة قضايا التنمية. ولهذا الغرض، تضطلع لجنتا دراسات قطاع تنمية الاتصالات بمسؤولية إعداد التقارير والمبادئ التوجيهية والتوصيات على أساس المدخلات الواردة من الأعضاء. ويُتخذ القرار كل أربع سنوات في المؤتمر العالمي لتنمية الاتصالات (WTDC) فيما يتعلق بالمسائل التي ستخضع للدراسة. ووافق أعضاء الاتحاد المشاركون في المؤتمر العالمي لتنمية الاتصالات لعام 2017 (WTDC-17) في بوينس آيرس في أكتوبر 2017 على أن تتناول لجنة الدراسات 2 في الفترة 2018-2021 سبع مسائل ضمن النطاق العام بشأن "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني."

وأُعد هذا التقرير استجابة للمسألة 3/2: **تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني،** بتوجيه عام وتنسيق من جانب فريق إدارة لجنة الدراسات 2 لقطاع تنمية الاتصالات بقيادة السيد أحمد رضا شرفات (جمهورية إيران الإسلامية)، بصفته الرئيس، بمساعدة نواب الرئيس التالية أسماؤهم: السيد ناصر المرزوقي (الإمارات العربية المتحدة) (استقال في 2018)؛ والسيد عبد العزيز الزرعوني (الإمارات العربية المتحدة)؛ والسيد فيليبي ميغيل أنطونيس باتيستا (البرتغال) (استقال في 2019)؛ والسيدة نورا عبد الله حسن بشير (السودان)؛ والسيدة ماريا بولشاكوفا (الاتحاد الروسي)؛ والسيدة سيلينا ديلغادو كاستيون (نيكاراغوا)؛ والسيد ياكوف غاس (الاتحاد الروسي) (استقال في 2020)؛ والسيد أناندا راج كانال (جمهورية نيبال)؛ السيد رونالد ياو كودوزيا (غانا)؛ والسيد توليبجون أولتينوفيتش ميرزاكولوف (أوزبكستان)؛ والسيدة ألينا مودان (رومانيا)؛ والسيد هنري شوكوودوميمي نكيمادو (نيجيريا)؛ والسيدة كي وانغ (الصين)؛ والسيد دومينيك فورغيس (فرنسا).

وأُعد التقرير تحت قيادة المقررين المشاركين المعنيين بالمسألة 3/2، السيد مايكل بيرن (الولايات المتحدة) (استقال في (2020؛ والسيد كوادوي بورجي (الولايات المتحدة) (استقال في 2020)؛ والسيدة إيمي ك. ميتشام (الولايات المتحدة) والسيد دومينيك فورغيس (فرنسا)، وبمساعدة نواب المقررين التالية أسماؤهم: السيد دامنام كانلانفي باغوليبي (توغو)؛ والسيد دوم بخيت (تشاد)؛ والسيدة ماريا بولشكوفا (الاتحاد الروسي)؛ والسيدة سونام شوكي (بوتان)؛ والسيد ياكوف غاس (الاتحاد الروسي) (استقال في 2020)؛ والسيد كريم حسناو (الجزائر)؛ والسيد سيسيه كان (المجتمع المدني الأفريقي من أجل مجتمع المعلومات)؛ والسيدة ميهو ناغانوما (اليابان)؛ والسيد جان-دافيد رودني (هايتي)؛ والسيدة جابين فاهورا (الولايات المتحدة)؛ والسيدة شينجين وان (الصين)؛ والسيد جايسوك يون (جمهورية كوريا)؛ والسيد محمدو زارو (مالي).

ونتقدم بشكر خاص لمنسقي الفصول لتفانيهم ودعمهم وخبرتهم.

وأُعد هذا التقرير بدعم من مسؤولي الاتصال في مكتب تنمية الاتصالات، والمحررين، وكذلك فريق إنتاج المنشورات وأمانة لجان الدراسات التابعة لقطاع تنمية الاتصالات.

جدول المحتويات

قائمة بالجداول والأشكال

الجداول

الأشكال

ملخص تنفيذي

يتمثل هدف المسألة 3/2 ("تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني") التابعة لقطاع تنمية الاتصالات بالاتحاد (ITU-D) في وضع تقارير لأفضل الممارسات بشأن الجوانب المختلفة للأمن السيبراني.

وهذه الوثيقة عبارة عن التقرير النهائي للمسألة 3/2 لآخر فترة دراسة مدتها أربع سنوات (2018-2021) والتي كان المؤتمر العالمي لتنمية الاتصالات الذي عُقد عام 2017 (WTDC-17) في بوينس آيرس قد وضع برنامج العمل المتعلق بالمسألة 3/2.

وقد ركزت الأنشطة التي نُفذت في فترات الدراسة السابقة على الدورات التدريبية التي تم توفيرها (2010-2014) وورش العمل لجلب مجموعة واسعة من الأطراف الفاعلة والمحتويات إلى البلدان النامية (2014-2017).

وخلال فترة الدراسة 2018-2021، عالجت لجنة الدراسات 2 لقطاع تنمية الاتصالات معظم بنود برنامج العمل. كما نُظمت ورشة عمل خلال فترة الدراسة هذه.

يستند تقرير المسألة 3/2 هذا إلى المواد المقدمة في مساهمات أعضاء الاتحاد خلال فترة الدراسة. ويقدم التقرير نظرة عامة عن الرسائل الاقتحامية والبرمجيات الضارة، فضلاً عن وسائل مواجهتها. كما يسرد عدداً من الدروس للتخطيط للاستجابة لتحديات الأمن السيبراني وحملات بناء الوعي على الصعيد الوطني. كما يتطرق إلى إجراءات معينة للفئات الضعيفة من السكان، بما في ذلك الأشخاص ذوو الإعاقة والأطفال. وإلى جانب ذلك، يحتوي التقرير على أفكار عن المدن الذكية والتكنولوجيات الناشئة وحماية البيانات.

وفي العالم الحالي المرقمن، حيث أصبحت الحياة اليومية للمواطنين وكذلك الاقتصادات بوجه عام تعتمد بشكل متزايد على التكنولوجيات الرقمية، تتزايد مخاطر تفاقم التعرض للهجمات السيبرانية. وقد تحدد الأمن السيبراني كأولوية وأكبر مصدر قلق للصناعة والحكومات ومستعملي الإنترنت في جميع أنحاء العالم، وهو أمر بالغ الأهمية لتحقيق تقدم مأمون وآمن يسمح للمجتمع بالنمو.

ويهدف هذا التقرير إلى توفير أفكار وممارسات محدثة تستند إلى تجارب أعضاء الاتحاد. ومع الإقرار باستمرار تتطور البيئة العامة والتهديدات، فإن التقرير يهدف ببساطة إلى أن يكون لقطة حالية في مجال الأمن السيبراني هذا الحساس للغاية. وقد نُشر هذا التقرير أيضاً في سياق محدد جداً وغير مسبوق: فبينما لا توجد إشارات محددة للوباء الحالي، فقد كان تأثير وباء COVID-19 في ذهن العديد من المساهمين وفي صلب المناقشات التي جرت خلال الأنشطة المضطلع بها في إطار المسألة 3/2.

وتهدف الردود والمقترحات التي تم تجميعها في هذا التقرير إلى المساعدة على تحقيق مستوى عالٍ من الأمن السيبراني لدى أعضاء الاتحاد، وربما يمكن أن يعمل أيضاً كأداة مفيدة لمواجهة الأزمات المستقبلية المحتملة، بالإضافة إلى الإجراءات الأخرى المتخذة من قبل الاتحاد.

ويقدم **الفصل 1** من التقرير تحديثاً بشأن حالة الرسائل الاقتحامية والبرمجيات الضارة، بما في ذلك إجراءات التخفيف منها. ويُلاحظ أن لجنة الدراسات لم تتلق مساهمات مباشرة بشأن هذا الموضوع.

ويناقش **الفصل 2** كيفية تحسين المواقف الوطنية للأمن السيبراني، من خلال فرص زيادة الوعي وبناء القدرات.

ويقدم **الفصل 3** معلومات عن أنشطة حماية الأطفال على الإنترنت (COP).

ويناقش **الفصل 4** تحديات الأمن السيبراني المحددة التي يواجهها الأشخاص ذوو الإعاقة.

ويناقش **الفصل 5** تحديات الأمن السيبراني التي تواجه التكنولوجيات الناشئة مثل إنترنت الأشياء (IoT) والحوسبة السحابية.

ويطرح **الفصل 6** وجهات نظر بشأن الكيفية التي يمكن بها للأمن السيبراني أن يدعم حماية البيانات الشخصية.

وأخيراً، يتناول **الفصل 7** مجالات الدراسة في المستقبل.

وإلى جانب هذا التقرير، جدير بالذكر أيضاً أن المسألة 3/2 استعرضت الاستبيان الذي يستخدم كأساس للرقم القياسي العالمي للأمن السيبراني (GCI)، وقدمت تعليقات ومقترحات مما مكن مكتب تنمية الاتصالات (BDT) من أن يجري استقصاءه السنوي بين الدول الأعضاء في الاتحاد. وعلى وجه الخصوص، ومن خلال مبادرة البرازيل، أعدت المسألة 3/2 الاستقصاء، الذي تم تضمينه في الرقم القياسي GCI كملحق. وتم دمج التنقيحات المقترحة في التكرار الرابع للرقم القياسي GCI لعام 2020.

ولا يتناول هذا التقرير على نطاق واسع الرقم القياسي GCI. ومع ذلك، تسلط المسألة 3/2 الضوء على النتيجة الإيجابية للجهود الجماعية والتعاون الثري مع مكتب تنمية الاتصالات، حيث ستوفر الردود على الملحق المعلومات التي تم جمعها عن السياسات التنظيمية التي سيتيحها مكتب تنمية الاتصالات للأعضاء، وبالتالي الوفاء ببند الدراسة "ن" من اختصاصات المسألة 3/2.

الفصل 1 - تحديث لحالة الرسائل الاقتحامية والبرمجيات الضارة، بما في ذلك إجراءات التخفيف منها

يتناول هذا القسم تطور الرسائل الاقتحامية والبرمجيات الضارة ويحدد عدداً من الإجراءات المضادة التي يتعين تنفيذها على الصعد الوطني والإقليمي والدولي، استجابة للقرار 45 (المراجَع في دبي، 2014) للمؤتمر العالمي لتنمية الاتصالات (WTDC)[1] بشأن آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية والتصدي لها. ومن ثم، يستجيب هذا القسم للبندين 2(ب) و(م) من اختصاصات المسألة 3/2 الواردة في التقرير النهائي للمؤتمر العالمي لتنمية الاتصالات لعام 2017:

(ب) مناقشة النهج وأفضل الممارسات المتصلة بتقييم أثر الرسائل الاقتحامية والبرمجيات الخبيثة داخل الشبكات، فضلاً عن التهديدات المتنامية والناشئة، ووضع التدابير والمبادئ التوجيهية اللازمة، بما في ذلك تقنيات التخفيف من أثارها والتشريعات والجوانب التنظيمية التي يمكن للبلدان استخدامها، مع أخذ المعايير القائمة والأدوات المتاحة في الاعتبار؛

(م) إعداد مبادئ توجيهية بشأن تدابير مكافحة الرسائل الاقتحامية والبرمجيات الخبيثة على الصعيد الوطني والإقليمي والدولي.[2]

1.1 حالة الرسائل الاقتحامية والبرمجيات الضارة

على الرغم من عدم وجود تعريف متفق عليه عالمياً للرسائل الاقتحامية، فإنها تشير عموماً إلى الاتصالات الإلكترونية الجماعية غير المرغوب فيها، التي يتم توصيلها عبر أجهزة الحاسوب أو الهواتف المحمولة عبر البريد الإلكتروني والرسائل النصية.[3] ويرى المستهلكون عادةً الرسائل الاقتحامية في شكل إعلانات، بما في ذلك رسائل البريد الإلكتروني التجارية التطفلية أو غير المرغوب فيها والنصوص وبيانات الاتصال على وسائل التواصل الاجتماعي.

على الرغم من أن الرسائل الاقتحامية يقصد بها عادة التنقيب التجاري، إلا أنها يمكن أن تستخدم أيضاً بيانات مماثلة أنشأها المستعمل لأغراض إجرامية، بما في ذلك التصيد الاحتيالي. ومن خلال التظاهر بأنهم أطراف ثالثة موثوق بها، يستخدم المهاجمون رسائل البريد الإلكتروني الاحتيالية لتشجيع مستلمي الرسائل على الكشف عن البيانات الشخصية (النفاذ إلى الحسابات وكلمات المرور وما إلى ذلك) و/أو البيانات المصرفية.

وتفرز الرسائل الاقتحامية مخاطر على أمن المستعملين والمنظمات الموصولة، ليس فقط لأنها تنتشر بسهولة عبر الإنترنت وخدمات الاتصالات الإلكترونية (البريد الإلكتروني، ومواقع الويب، ووسائل التواصل الاجتماعي، والرسائل النصية القصيرة ورسائل الوسائط المتعددة)، ولكن أيضاً لأنها يمكن أن تحمل برمجيات ضارة. وتقوم البلدان بتنفيذ آليات تقنية وتنظيمية مختلفة لمكافحة الرسائل الاقتحامية، تحقق بعض النجاح.

وشهدت البرمجيات الضارة، من جانبها، نمواً كبيراً في السنوات الأخيرة بسبب تطور الإنترنت، وبشكل أكثر تحديداً، الإنترنت عبر الأجهزة المتنقلة. والبرمجيات الضارة هي مصطلح عام للبرمجيات المصممة خصيصاً لإلحاق الضرر بأجهزة الحاسوب أو الأنظمة الحاسوبية.[4]

علاوةً على ذلك، أتاحت زيادة التوصيلية والتكنولوجيات الجديدة والنمو في عدد المستعملين فرصاً جديدة لإنشاء البرمجيات الضارة واستخدامها. ويطرح هذا النموذج تعقيداً أكبر بالنسبة للأمن السيبراني من خلال فتح الثغرات وتوسيع أسطح الهجوم المتاحة لتهديدات البرمجيات الضارة. وبالإضافة إلى البرمجيات الضارة التقليدية (الفيروسات، والديدان، وأحصنة طروادة، وبرمجيات التجسس، والبرمجيات الدعائية، والرسائل الاقتحامية،

---

[1] الاتحاد الدولي للاتصالات. التقرير النهائي للمؤتمر العالمي لتنمية الاتصالات (بوينس آيرس، 2017)، صفحة 409.

[2] الحاشية السابقة، الصفحتان 727 و728.

[3] انظر التوصيات من ITU-T X.1230 إلى ITU-T X.1240، بشأن مكافحة الرسائل الاقتحامية.

[4] انظر الإضافة 9 للتوصية ITU-T X.1205 (2011/09). إضافة بشأن المبادئ التوجيهية للحد من البرمجيات الخبيثة في شبكات تكنولوجيا المعلومات والاتصالات.

والجذور الخفية، وما إلى ذلك)، ظهرت أنواع جديدة أكثر تعقيداً من البرمجيات الضارة، مثل الروبوتات، وبرمجيات طلب الفدية، والبرمجيات الضارة للأجهزة المتنقلة.

باختصار، تعتبر مكافحة الرسائل الاقتحامية والبرمجيات الضارة أمراً بالغ الأهمية لأمن المستخدمين ونمو الأعمال.

2.1 الرسائل الاقتحامية والبرمجيات الضارة: الإحصاءات والاتجاهات والتطور والآثار على شبكات الاتصالات الإلكترونية

في مارس 2020، بلغت نسبة الرسائل الاقتحامية في حركة البريد الإلكتروني العالمية 53,95 في المائة.[5] وفي السنوات الأخيرة، انخفضت هذه النسبة بشكل كبير، من 69 في المائة في عام 2012 إلى 55 في المائة في عام 2018، ربما نتيجة للتقدم في الوعي بالأمن السيبراني والتقدم التكنولوجي. ومعظم الرسائل الاقتحامية التي يتلقاها المستعملون ترويجية بطبيعتها، بما في ذلك معلومات التسويق. ووفقاً لأحد التقديرات، فإن الرسائل الاقتحامية تكلف شركات الأعمال ما يقرب من 20,5 مليار دولار أمريكي سنوياً من حيث الإنتاجية المفقودة والنفقات التقنية. ويُرى أن هذه التكلفة قد ترتفع إلى 257 مليار دولار أمريكي سنوياً إذا استمرت الرسائل الاقتحامية في النمو بمعدلاتها الحالية.[6]

ووفقاً لأحد التقديرات، تمثل عمليات التلاعب والاحتيال حوالي 2,5 في المائة من جميع الرسائل الاقتحامية، والتي قد تكون نسبة كبيرة منها (92 في المائة) ضارة بطبيعتها، أي مرتبطة ببرمجيات ضارة بهدف إلحاق الضرر بالمستعملين أو المساس بأنظمة تكنولوجيا المعلومات الخاصة بهم لأغراض مختلفة.[7] ووفقاً لتقدير آخر، سُجلت حوالي 812,67 مليون إصابة مرتبطة بالبرمجيات الخبيثة من مختلف الأنواع في عام 2018.[8] وزادت البرمجيات الضارة الخاصة بالأجهزة المتنقلة بنسبة 54 في المائة وبرمجيات طلب الفدية بنسبة 350 في المائة، في حين تقدر الخسائر المالية المتعلقة بإصابات برمجيات طلب الفدية بنحو 6 مليارات دولار سنوياً (حتى 2021).

وحيث إن بإمكان الرسائل الاقتحامية والبرمجيات الضارة توليد حركة كبيرة، فإنه يمكن أن يكون لها تأثير سلبي كبير على البنية التحتية للشبكات والمشغلين، وبالتالي على تجربة المستعمل للمستهلكين. وقد تؤدي المشكلات المتعلقة بالرسائل الاقتحامية، بما في ذلك مشكلات الشبكة الناتجة، إلى الإضرار بسمعة المشغلين.

ولمواجهة هذه المخاوف، بما في ذلك التدفقات الهائلة المحتملة للحركة غير المرغوب فيها، ولضمان جودة الشبكة، يتعين على المشغلين تطوير أدوات جديدة، بما في ذلك الاستثمار في حماية البنية التحتية القائمة وتوسيعها. فعلى سبيل المثال، يمكن لموردي الخدمات الاستثمار في تركيب مرشحات ضد الرسائل الاقتحامية لتحسين جودة الخدمات التي يقدمونها. وقد تستوجب هذه الإجراءات تكاليف إضافية ضرورية للمشغلين وموردي خدمات الاتصالات الإلكترونية.

3.1 النهج المتبعة في مكافحة الرسائل الاقتحامية والبرمجيات الضارة والتخفيف من آثارها

1.3.1 النهج النموذجية لمكافحة الرسائل الاقتحامية والبرمجيات الضارة والتخفيف من آثارها

يعد البريد الإلكتروني غير المرغوب فيه أحد القنوات الرئيسية لإرسال البرمجيات الضارة. ولمكافحة الرسائل الاقتحامية والبرمجيات الضارة بشكل فعال، يجب كسر سلسلة الإرسال. ومع تقدم التكنولوجيا، لا تزال أدوات مثل مرشحات الرسائل الاقتحامية وبرمجيات مكافحة الفيروسات آليات فعالة لمكافحة الرسائل الاقتحامية والبرمجيات الضارة. ويمكن زيادة فعالية هذه الأدوات من خلال استخدامها بالاقتران مع تقنيات جديدة، مثل الذكاء الاصطناعي (AI). لذلك، يعد التحديث المنتظم لمرشحات الرسائل الاقتحامية وبرمجيات مكافحة الفيروسات ممارسة جيدة للمستعملين.

---

[5] شركة Statista. حجم الرسائل الاقتحامية العالمية كنسبة مئوية من إجمالي حركة البريد الإلكتروني من يناير 2014 إلى سبتمبر 2020، بالشهر.

[6] قوانين الرسائل الاقتحامية. إحصاءات ووقائع الرسائل الاقتحامية.

[7] الموقع DataPort. ماذا يوجد على الجانب الآخر من بريدك الوارد – 20 إحصائية للرسائل الاقتحامية لعام 2021.

[8] شركة PurpleSec. إحصاءات الأمن السيبراني لعام 2021 - القائمة النهائية للإحصاءات والبيانات والاتجاهات.

وبالنسبة لموردي الخدمات، فهناك سياسات على غرار إطار سياسة المرسل (SPF)[9] والبريد المعرف بمفاتيح الميادين (DKIM)[10] واستيقان الرسائل والإبلاغ عنها ومطابقتها على أساس الميادين[11] والتسجيل في قوائم الحجب في الوقت الفعلي، يمكن استخدامها لتقليص سلاسل الإرسال هذه.

يمكن لمشغلي شبكات الاتصالات الإلكترونية وموردي خدمات الإنترنت أيضاً اتخاذ تدابير معينة لمعالجة المخاوف المتعلقة بحجب عناوين بروتوكول الإنترنت. ومن أمثلة ذلك أمن بروتوكول بوابة الحدود باستخدام البنية التحتية للمفاتيح العمومية للموارد.[12] وتشمل المبادرات الأخرى:

- المعايير المتفق عليها بشكل متبادل لأمن التسيير، والتي تهدف بشكل تعاوني إلى منع أحدث سبل سرقة المسيرات، وانتحال عنوان بروتوكول الإنترنت والأنشطة الضارة الأخرى التي يمكن أن تؤدي إلى هجمات رفض الخدمة الموزعة (DDoS)، والتنصت، وخسارة الإيرادات، والإضرار بالسمعة، إلخ.[13]
- فريق العمل المعني بمكافحة إساءة استعمال المراسلة والبرمجيات الضارة والاتصالات المتنقلة، والذي ينشر بانتظام أفضل الممارسات لمكافحة الرسائل المسيئة وجميع أنواع البرمجيات الضارة (بما في ذلك البرمجيات الروبوتية) والرسائل الاقتحامية والفيروسات وهجمات رفض الخدمة (DoS) وإساءة الاستخدام عبر الإنترنت من أي نوع.[14]

وتشمل المبادرات الأخرى في مجال مكافحة الرسائل الاقتحامية والبرمجيات الضارة جمعية الإنترنت،[15] ورابطة النظام العالمي للاتصالات المتنقلة،[16] ومشروع Spamhaus،[17] وفريق العمل المعني بمكافحة التصيد الاحتيالي[18] وتحالف مكافحة برمجيات التجسس.[19]

2.3.1 أمثلة على النهج التنظيمية لمكافحة الرسائل الاقتحامية والبرمجيات الضارة والتخفيف من آثارها

نظراً للمخاوف والتكاليف المرتبطة بمكافحة الرسائل الاقتحامية والبرمجيات الضارة، اعتمدت بعض المناطق والدول في السنوات الأخيرة تشريعات أو عززت التشريعات القائمة من أجل توفير الأدوات اللازمة لتكثيف مكافحة هذه الهجمات. وتعمل البلدان على وضع تشريعات وسياسات بناءً على احتياجاتها المحلية، مثل لائحة حماية البيانات العامة (GDPR) للاتحاد الأوروبي، والتي تتطلب موافقة المستعمل لجمع البيانات.

وهناك مثال آخر وهو اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء السيبراني وحماية البيانات الشخصية (اتفاقية ماليبو)، التي تحدد مجموعة من المعايير التي تُحث الدول الأطراف في منطقة إفريقيا على إدراجها ضمن تشريعاتها الوطنية. وفي المادة 3.4، تنص الاتفاقية على أن "*تلتزم الدول الأطراف في الاتحاد الإفريقي بحظر التسويق المباشر الذي يتم عبر أي شكل من أشكال الاتصال غير المباشر من خلال استعمال بيانات لشخص طبيعي، بأي شكل من الأشكال، لم يوافق مسبقاً على تلقي هذا التسويق المباشر عن طريق الوسائل المذكورة آنفاً*". ومع ذلك تبيح الاتفاقية التسويق المباشر طبقاً لشروط معينة؛ على سبيل المثال "*يرخص بالتسويق المباشر عبر البريد الإلكتروني في الحالات التالية: (أ) إذا تم الحصول على البيانات ذات الطابع الشخصي الخاصة بالمرسل إليه منه مباشرة؛ (ب) إذا وافق المتلقي على اتصال شركاء التسويق؛ (ج) إذا تعلق التسويق المباشر بمنتجات أو خدمات مشابهة يقدمها نفس الشخص الطبيعي أو المعنوي*" (الفقرة 4.4).

ومع تطبيق كل من لائحة حماية البيانات العامة للاتحاد الأوروبي واتفاقية ماليبو، سنكون قادرين على تقييم وفهم تأثيرهما الكامل على الحد من الرسائل الاقتحامية والبرمجيات الضارة.

---

9 شركة Mimecast. كل ما تحتاج أن تعرفه عن إطار سياسة المرسل.
10 DKIM.org. البريد المعرف بمفاتيح الميادين (DKIM).
11 DMARC. استيقان الرسائل والإبلاغ عنها ومطابقتها على أساس الميادين.
12 محرر طلب تقديم التعليقات (RFC) RFC 6480 – بنية تحتية لدعم التسيير الآمن للإنترنت.فبراير 2012.
13 المعايير المتفق عليها بشكل متبادل لأمن التسيير (MANRS).
14 فريق العمل المعني بمكافحة إساءة استعمال المراسلة والبرمجيات الضارة والاتصالات المتنقلة (M³AAWG). ما سبب إنشاء الفريق M³AAWG؟
15 جمعية الإنترنت. مجموعة أدوات جمعية الإنترنت لمكافحة الرسائل الاقتحامية.
16 رابطة النظام العالمي للاتصالات المتنقلة. أمن رابطة النظام العالمي للاتصالات المتنقلة.
17 Spamhaus. Spamhaus ZEN + DBL + RPZ.
18 فريق العمل المعني بمكافحة الانتحال. توحيد الاستجابة العالمية للجرائم السيبرانية عبر تبادل البيانات والبحوث والتوعية العامة.
19 تحالف مكافحة برمجيات التجسس. *الإنترنت والتسوق الفعلي*.

3.3.1 المساهمات ذات الصلة بالعمل المتعلق بمكافحة الرسائل الاقتحامية والبرمجيات الضارة والتخفيف من آثارها في إطار المسألة 3/2

خلال فترة الدراسة، قدمت بعض البلدان وأعضاء قطاعات الاتحاد أمثلة إضافية لنهج مكافحة الرسائل الاقتحامية والبرمجيات الضارة:

- أوضح بعض مقدمي المساهمات كيف يقومون بجمع معلومات في الوقت الحقيقي حول تهديدات الأمن السيبراني من أجل تنوير وبناء استراتيجيات مرنة للأمن السيبراني. وفي عالم تكنولوجيا المعلومات المعقد، تعد بيانات الوقت الفعلي ضرورية لحماية المعلومات. ويساعد الوعي بالأوضاع والمعلومات المتعلقة بالتهديدات السيبرانية، عند الجمع بينهما، البلدان والمؤسسات العامة والخاصة على تحديد التهديدات فور ظهورها حتى تتمكن من حماية مواردها بفعالية أكبر. ومن هنا، من الضروري وضع استراتيجيات مرنة سيبرانياً تغذيها معلومات الأمن، وذلك لتحقيق حماية أفضل للمنظمات من الهجمات محددة الأهداف والتهديدات المتواصلة[20].

- يقوم بعض المساهمين برسم خرائط لتهديدات الجرائم السيبرانية لفهم التأثيرات المختلفة للرسائل الاقتحامية والبرمجيات الضارة على مستعملي الإنترنت (مثل التصيد الاحتيالي والاحتيال في اليانصيب) والشركات (مثل النفاذ غير المصرح به إلى النظام وهجمات رفض الخدمة). فعلى سبيل المثال، في عام 2017، رصدت كوت ديفوار التهديدات والمخالفات المتعلقة بالجرائم الإلكترونية، والتي سجلتها منصة مكافحة الجريمة السيبرانية (PLCC)، وبالتالي وفرت معلومات مفيدة ونوعية لتوجيه الأنشطة التشغيلية لتحسين تثقيف المستهلكين والشركات. وقد تم تحديد أنماط الاحتيال في الخدمات المالية المتنقلة، حيث سُجلت 453 حالة، قدرت خسائرها بمبلغ 800 000 دولار أمريكي تقريباً. ويعد الاحتيال في الخدمات المالية المتنقلة عملية احتيال متقنة الصنع، يحدث فيها، بعد تحويل الأموال إلى أو من أحد حسابات الخدمات المالية المتنقلة باستخدام قواعد بيانات الخدمات التكميلية غير المبنية (USSD)، أن يتلقى الضحية مكالمة من المحتالين يدعون فيها وجود مشكلة في عملية التحويل؛ فإذا وقع الضحية في عملية الاحتيال يكون بمقدور القيام بسحب أموال عن بُعد من حساب الخدمات المالية المتنقلة للضحية عليه باستخدام نفس قواعد بيانات الخدمات التكميلية غير المبنية.[21]

- أوضح بعض المساهمين كيف يقومون بإنشاء عمليات مفتوحة وشفافة لتحديد وتعزيز الإجراءات التي يجب اتخاذها من قبل أصحاب المصلحة المعنيين بهدف الحد بشكل كبير من التهديدات التي تشكلها الهجمات الآلية والموزعة (مثل البرمجيات الروبوتية). ومع ظهور برمجيات روبوتية جديدة يمكن أن تولد ضغطاً هائلاً على الشبكات، باستخدام أكثر من تيرابتة من البيانات في الثانية، لم تعد تقنيات تخفيف هجمات الرفض الموزع للخدمة التقليدية القائمة على حجز الموارد من قبل موردي خدمات النفاذ إلى الشبكة فعالة. ويتطلب التخفيف من تهديدات الهجمات الإلكترونية المؤتمتة والموزعة تعاوناً مستمراً بين القطاعين العام والخاص.[22]

- ويمكن للشركات، من خلال اتخاذ بعض الخطوات البسيطة، المساعدة في حماية نفسها بشكل فعال من التهديد الخاص بهجمات برمجيات طلب الفدية. وفي مشورة حديثة بشأن برمجيات طلب الفدية، يوصي المركز الوطني للأمن السيبراني (NCSC) في المملكة المتحدة بعدد من تقنيات تخفيف المخاطر المباشرة، مثل:

  - تحديث الأجهزة والشبكات (على سبيل المثال من خلال التحديثات والإصلاحات السريعة وعمليات الفحص المنتظمة)؛
  - منع واكتشاف الحركات الجانبية في شبكات الشركات؛
  - استخدام ماسح الفيروسات؛
  - إعداد نسخ احتياطية لجميع الملفات.[23]

  ويمكن الاطلاع على قائمة كاملة ومفصلة بالتوصيات في الموقع الإلكتروني للمركز الوطني للأمن السيبراني.[24]

---

[20] الوثيقة 2/167 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من شركة Symantec (الولايات المتحدة)
[21] الوثيقة 2/174 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من كوت ديفوار
[22] الوثيقة SG2RGQ/153 + الملحقات للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الولايات المتحدة
[23] الوثيقة SG2RGQ/155 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة
[24] المركز الوطني للأمن السيبراني (NCSC). توجيه: التخفيف من البرمجيات الضارة وبرمجيات طلب الفدية.

- وصف بعض المساهمين كيف يقومون بإنشاء إطار عمل وطني مرن للأمن السيبراني يتكيف مع الاحتياجات المتغيرة. فعلى سبيل المثال، أطلقت المملكة المتحدة برنامج Active Cyber Defense، الذي يركز على اتخاذ خطوات تقنية إيجابية لتحسين بيئة الإنترنت للجميع. وقد حقق هذا البرنامج فوائد كبيرة يمكن قياسها للشبكات الحكومية. وقد تم تنفيذه عبر شبكات الخدمات العمومية في المملكة المتحدة من أجل توضيح الفوائد العملية وخطوات المتابعة المحتملة.[25] وفي إطار الجهود المستمرة لمواجهة مثل هذه التحديات، قدمت المملكة المتحدة تحديثاً للبرنامج بعد عام من إطلاقه.[26]
- يتخذ بعض المساهمين خطوات لتثقيف المجتمعات الضعيفة (مثل الأشخاص ذوي الإعاقة) بشأن مستوى المخاطر المتزايد لديهم. ويستخدم مرسلو الرسائل الاقتحامية وقراصنة الحاسوب تقنيات معقدة بشكل متزايد لتحديد ما إذا كانت أهداف الاختطاف المحتملة معاقة أم لا. وفي بعض الحالات، يستخدم الخاطفون إعاقة الشخص كوسيلة للادعاء بأنهم هذا الشخص من حساب البريد الإلكتروني الذي تم اختطافه.[27]
- يوفر بعض المساهمين خدمات الإبلاغ عن رسائل البريد الإلكتروني الاحتيالية. وتعد الاستعانة بمصادر جماعية لجمع رسائل البريد الإلكتروني الضارة، واتخاذ إجراءات ضد الميادين والكيانات الأخرى التي تحتوي عليها، أداة فعالة للحد من الجرائم السيبرانية والاحتيال. فعلى سبيل المثال، في الأشهر الأربعة الأولى من تشغيل خدمة الإبلاغ عن البريد الإلكتروني المشبوه، أزال المركز الوطني للأمن السيبراني في المملكة المتحدة وشرطة مدينة لندن أكثر من 16 000 تهديد عبر الإنترنت أبلغ عنها الجمهور.[28]

[25] الوثيقة SG2RGQ/55 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة
[26] الوثيقة SG2RGQ/175 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة
[27] الوثيقة 2/71 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المبادرة العالمية لتكنولوجيا المعلومات والاتصالات الشاملة (G3ict)
[28] الوثيقة SG2RGQ/234 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة

الفصل 2 - تحسين الأوضاع الوطنية للأمن السيبراني: فرص زيادة الوعي وبناء القدرات

شهدت تكنولوجيا المعلومات والاتصالات في السنوات الأخيرة نمواً سريعاً مع الابتكار. ولتكنولوجيا المعلومات والاتصالات حول العالم دور مهم في تمكين البلدان من توسيع اقتصاداتها الرقمية ودعم الازدهار الاجتماعي. وعلاوةً على ذلك، أظهر وباء COVID-19 أن الناس يعتمدون بشكل متزايد على تكنولوجيا المعلومات والاتصالات في حياتهم اليومية. وبالنظر إلى هذا الواقع، من الأهمية بمكان أن تستمر البلدان في اتخاذ خطوات مهمة لتحسين وتعزيز أوضاع الأمن السيبراني الوطنية لديها من أجل الحماية من مخاطر وتحديات الأمن السيبراني.

ويتناول هذا الفصل مجالات التركيز الرئيسية لتحسين الأوضاع الوطنية للأمن السيبراني، بما في ذلك:

- إنشاء السلطات الوطنية ذات الصلة للأمن السيبراني
- أفرقة الاستجابة للطوارئ الحاسوبية (CERT)/أفرقة الاستجابة للحوادث الأمنية الحاسوبية (CSIRT)/ أفرقة الاستجابة للحوادث الحاسوبية (CIRT)
- حملات لزيادة الوعي بالأمن السيبراني
- أطر لإدارة مخاطر الأمن السيبراني
- شراكات بين القطاعين العام والخاص
- مبادرات بناء القدرات الأخرى.

وخلال فترة الدراسة، قدم عدد من الكيانات مساهمات بشأن هذه القضايا. ارجع إلى **الملحق 1** للاطلاع على خلاصة وافية لأنشطة الأمن السيبراني الجارية ذات الصلة التي تنفذها الدول الأعضاء والمنظمات والقطاع الخاص والمجتمع المدني على الصُعد الوطني والإقليمي والدولي. ارجع إلى **الملحق 2** للاطلاع على قائمة بأفضل الممارسات والدروس المستفادة ذات الصلة المقدمة من بعض هذه الكيانات.

1.2 إنشاء السلطات الوطنية ذات الصلة للأمن السيبراني

مع حدوث تطورات وابتكارات جديدة في تكنولوجيا المعلومات والاتصالات، تزداد أيضاً مخاطر وتحديات الأمن السيبراني. ويجب على الحكومات تقييم أوضاعها واستراتيجياتها الخاصة بالأمن السيبراني بشكل مستمر وتحسينها لمواجهة هذه التحديات، بما في ذلك من خلال إنشاء السلطات الوطنية ذات الصلة للأمن السيبراني. وخلال فترة الدراسة، شرحت الدول الأعضاء نهجها في إنشاء مثل هذه السلطات. واتبعت البلدان المختلفة نُهج مختلفة طبقاً لهياكلها وقواعدها ولوائحها وسياساتها الإدارية المحلية.

وتتفاوت سلطات الأمن السيبراني هذه في الخبرة والتركيز، ولكنها تؤدي عموماً نفس الوظائف الرئيسية، بما في ذلك وضع وتنسيق السياسات التنظيمية، وتطوير وتنفيذ حملات التوعية بالأمن السيبراني، وتزويد المستعملين (من المؤسسات الكبيرة إلى الأفراد والشركات الصغيرة) بآخر المعلومات وإصدار البيانات والإرشادات بشأن حوادث الأمن السيبراني. وبالنظر إلى مشهد الأمن السيبراني ككل، من الأهمية بمكان أن تعزز الحكومات التنسيق والتعاون بين مختلف السلطات والكيانات وبين القطاعين العام والخاص.

فعلى سبيل المثال، في المملكة المتحدة، يعمل المركز الوطني للأمن السيبراني مع الكيانات الحكومية الأخرى ذات الصلة ويقود الجهود للحد بشكل ملموس من تأثير هجمات برمجيات طلب الفدية.[29] وفي حالة وقوع هجوم، تُنصح المنظمات بالاتصال بالوكالة الوطنية للجريمة، أو شركة معتمدة من شركات الاستجابة للحوادث السيبرانية أو شراكة من شراكات تبادل معلومات الأمن السيبراني. وقاد المركز الوطني للأمن السيبراني استجابة المملكة المتحدة لهجوم WannaCry لبرمجيات طلب الفدية، بالتعاون مع الوكالة الوطنية للجريمة. وعلى مدار كل حادث، ينشر المركز بيانات وإرشادات للمؤسسات الكبيرة، وكذلك للمستعملين المنزليين والشركات الصغيرة. كما تم الإعلان عن آخر المعلومات عبر حساب المركز على تويتر (@NCSC).

[29] الوثيقة SG2RGQ/155 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة

وقد اعتمدت البرازيل إستراتيجيتها الوطنية للأمن السيبراني (E-Ciber)، والتي صدق عليها الرئيس البرازيلي ونُشرت في فبراير 2020.[30] وبالنسبة لهذه الاستراتيجية التطلعية، التي تمثل رؤية الحكومة الفيدرالية إزاء الأمن السيبراني للفترة 2020-2023، قامت البرازيل بتنفيذ نهج عام وشامل، ينطوي على مشاركة العديد من أصحاب المصلحة، بما في ذلك أصحاب المصلحة من الحكومة والقطاع الخاص والأوساط الأكاديمية. وبالتصديق على الاستراتيجية E-Ciber، اضافت البرازيل إطاراً قانونياً كان ينقصها سابقًا. وفي إطار الاستراتيجية E-Ciber، حددت البرازيل 10 إجراءات استراتيجية، حددت في إطار كل منها الإجراءات والمبادرات. ومن أمثلة الإجراءات الاستراتيجية تلك ما يلي:

- تعزيز إدارة الأمن السيبراني؛
- إنشاء نموذج وطني مركزي لإدارة الأمن السيبراني؛
- تحسين الإطار القانوني الوطني للأمن السيبراني؛
- توسيع نطاق التعاون الدولي للبرازيل في مجال الأمن السيبراني.

وفي بنن تشارك الكيانات الحكومية المختلفة في إدارة تكنولوجيا المعلومات والاتصالات في البلاد.[31] ووكالة أنظمة وخدمات المعلومات (ASSI)، المعروفة سابقاً باسم وكالة بنن لتكنولوجيا المعلومات والاتصالات (ABETIC)، هي الكيان الوطني المكلّف بالتنفيذ العملي للبرامج ووضع استراتيجيات تطوير أنظمة وخدمات المعلومات الرقمية المأمونة في البلاد. والوكالة مسؤولة عن عدد من الأنشطة الرئيسية، منها ما يلي:

- تنفيذ المشاريع الرئيسية في مجال الإدارة الذكية والتجارة الإلكترونية؛
- وضع الخطط الرئيسية لأنظمة المعلومات الوطنية وتحديثها وتنفيذها عملياً؛
- ضمان الاتساق التقني والتطبيقي والمالي لأنظمة وخدمات المعلومات الوطنية؛
- ضمان استضافة ومراقبة المعلومات والبيانات الحرجة للدولة ولمشغلي البنى التحتية الحرجة والنفاذ الآمن إليها.

وفي تشاد، ترفع الوكالة الوطنية لأمن المعلومات وإصدار الشهادات الإلكترونية (ANSICE)، التي تأسست في فبراير 2015، تقاريرها مباشرة إلى مكتب الرئيس.[32] وتعمل الوكالة منذ يناير 2018 وتتمتع بسلطات واختصاصات واسعة، بما في ذلك في مجال أمن أنظمة وشبكات المعلومات في جميع أنحاء البلاد.

وعرضت المملكة المتحدة أيضاً دراسة حالة محدثة عن جهودها في تنفيذ ممارسات الأمن الجيدة لأجهزة إنترنت الأشياء (IoT) الاستهلاكية، ولا سيما من خلال:

- نشر مدونة الممارسات الخاصة بأمن المستهلك لإنترنت الأشياء، والتي تحدد 13 مبدأً رفيع المستوى (متاحة أيضاً باللغات الألمانية والإسبانية والفرنسية واليابانية والكورية والماندرين والبرتغالية)؛
- إجراء مشاورة عامة بشأن اللوائح والتشريعات المقترحة؛
- دعم المعيار ETSI EN 303 645،[33] أول معيار قابل للتطبيق عالمياً لأمن إنترنت الأشياء، نشره المعهد الأوروبي لمعايير الاتصالات (ETSI). وقد اعتمد العديد من المنظمات بالفعل في منتجاتها وخطط منح الشهادات على هذا المعيار وسابقه، المعيار ETSI TS 103 645؛
- نشر دعوة لإبداء الآراء حول المقترحات التنظيمية للمملكة المتحدة لجمع التعليقات من أصحاب المصلحة بشأن ما هو مقترح من نطاق والتزامات ومتطلبات أمنية ونهج للإنفاذ؛
- تكليف وزارة التكنولوجيا الرقمية والثقافة والإعلام والرياضة والمركز الوطني للأمن السيبراني بإعداد مواد إرشادية وحلقات دراسية عبر الإنترنت بشكل مشترك لمصنعي إنترنت الأشياء، بحيث تُنظم بشكل متكرر لمراعاة المناطق الزمنية العالمية؛
- الحفاظ على خريطة شاملة تحدد المعايير الحالية، ودعم المنظمات في تنفيذ الممارسات الجيدة عبر إنترنت الأشياء.[34]

---

30 الوثيقة SG2RGQ/216 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من البرازيل
31 الوثيقة 2/152 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بنن
32 الوثيقة 2/136 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من تشاد
33 المعهد الأوروبي لمعايير الاتصالات. المعيار ETSI EN 303 645. الأمن السيبراني لإنترنت الأشياء الاستهلاكية: المتطلبات الأساسية.
34 الوثيقة SG2RGQ/241 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة

2.2 أفرقة الاستجابة للطوارئ الحاسوبية (CERT)/أفرقة الاستجابة للحوادث الأمنية الحاسوبية (CSIRT)/ أفرقة الاستجابة للحوادث الحاسوبية (CIRT)

تعد قدرات الاستجابة الوطنية للحوادث (في شكل أفرقة الاستجابة للطوارئ الحاسوبية/أفرقة الاستجابة للحوادث الأمنية الحاسوبية/أفرقة الاستجابة للحوادث الحاسوبية) أدوات أساسية لمواجهة تحديات الأمن السيبراني التشغيلية. وتسهل هذه القدرات تنسيق معلومات الأمن السيبراني والاستجابات للحوادث الأمنية. وخلال فترة الدراسة، تلقت لجنة الدراسات مساهمات رئيسية من الدول الأعضاء في الاتحاد ومن أعضاء القطاع حول هذا الموضوع، طرح العديد منها الرأي القائل بأنه ينبغي لأفرقة الاستجابة للطوارئ الحاسوبية/أفرقة الاستجابة للحوادث الأمنية الحاسوبية/أفرقة الاستجابة للحوادث الحاسوبية الوطنية أن تعمل كجهة اتصال رئيسية لقضايا الأمن السيبراني وكجهات لتنسيق الاستجابة للحوادث.

فعلى سبيل المثال، أُنشئ فريق بوتان للاستجابة للحوادث الحاسوبية (BtCIRT) في أبريل 2016 لتعزيز الأمن السيبراني في البلاد من خلال تسهيل تنسيق معلومات الأمن السيبراني وإنشاء القدرات الوطنية للتعامل مع الحوادث الأمنية الحاسوبية.[35] والفريق BtCIRT هو وحدة تابعة لإدارة تكنولوجيا المعلومات والاتصالات في وزارة المعلومات والاتصالات. ويعمل الفريق BtCIRT، وفقاً لولايته، كجهة اتصال وطنية لقضايا الأمن السيبراني ويمثل البلاد في المنتديات الدولية. ومن شأن وجود منظمة واحدة لتنسيق جميع مبادرات الأمن السيبراني أن يضمن عدم وجود الازدواجية في الجهود أو أعمال التطوير. ونظراً إلى أن معظم المنتديات والمجموعات الدولية التي تركز على الأمن السيبراني تتواصل مع أفرقة الاستجابة للحوادث الحاسوبية التي لديها ولاية وطنية، فمن المهم أن تعين الحكومات إما فريق للاستجابة للحوادث الحاسوبية أو منظمة واحدة معينة لقيادة مبادرات وخطط الأمن السيبراني الوطنية.

وعلى الرغم من إنشاء الفريق BtCIRT كجهة اتصال للقضايا المتعلقة بالأمن السيبراني في بوتان، فقد كان من الصعب على الفريق اكتساب ثقة أصحاب المصلحة، ويرجع ذلك أساساً إلى قدراته التقنية المحدودة وكونه فريقاً جديداً إلى حد ما. وعلاوةً على ذلك، تمتلك الشركات الكبيرة مثل مشغلي الاتصالات والبنوك بالفعل بنية تحتية قوية لتكنولوجيا المعلومات والاتصالات تتمتع بقدرات تقنية، مما يجعل التعاون بين الحكومة وهذه المنظمات الكبيرة أمراً صعباً. ويعد التعاون والتعاضد بين أصحاب المصلحة، خاصة موردي خدمات الإنترنت والأفرقة CIRT، أمراً ضرورياً لتوفير حلول أمنية منسقة لمستعملي الإنترنت. ولجأت بوتان إلى المنظمات الدولية للمساعدة في بناء القدرات التقنية الحرجة للفريق BtCIRT.

وأخيراً، أشارت الشركة الليتوانية NRD للأمن السيبراني إلى أنه بالإضافة إلى العمل كجهة اتصال رئيسية لحوادث الأمن السيبراني وكجهات لتنسيق الاستجابات، ينبغي لأفرقة الاستجابة للحوادث الأمنية الحاسوبية الوطنية والقطاعية أن تعمل أيضاً كجهات تيسير أو تحفيز لتطوير قدرات إضافية مرنة مستقلة وموزعة ضد التهديدات الإلكترونية في البلاد.[36]

3.2 حملات زيادة الوعي

يستفيد العديد من أصحاب المصلحة في جميع أنحاء العالم - من الحكومات والكيانات التجارية إلى المنظمات المجتمعية وفرادى المواطنين - بشكل مكثف من تكنولوجيا المعلومات والاتصالات. ومع ذلك، فإن العديد من المستعملين لا يدركون تماماً مخاطر الأمن السيبراني المترتبة عن استخدامهم لها. وبالنسبة لبعض البلدان النامية، يتمثل التحدي الأكبر في نقص وعي المستعملين. وفي المساهمات الواردة خلال فترة الدراسة، كان هناك فهم مشترك بأن لحملات زيادة الوعي بالأمن السيبراني دور مهم في مواجهة مثل هذه التحديات. والغرض الأساسي من هذه الحملات هو تشجيع تبني السلوك الآمن على الإنترنت.

وتبحث البلدان والشركات عن طرق مبتكرة لإعداد حملات فعالة، بما في ذلك كيفية الوصول إلى مجموعة واسعة من المستعملين.

فعلى سبيل المثال، عرضت المكسيك تجربتها في تطوير وإجراء استقصاء لمستعملي الإنترنت، يمكن تطبيقه لتوجيه النهج المختلفة لحملات زيادة الوعي بالأمن السيبراني.[37]

---

[35] الوثيقة SG2RGQ/79 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان

[36] الوثيقة 2/172 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من شركة NRD للأمن السيبراني (ليتوانيا)

[37] الوثيقة 2/165 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المكسيك

وقد استخدمت بعض البلدان الاستقصاءات لتحديد الاهتمامات الرئيسية للمواطنين وإعداد حملات توعية مصممة بناءً على النتائج. وبناءً على تجربتها، حددت المكسيك أيضاً الدروس التالية:

- تثبيت وتحديث برمجيات الحماية من الفيروسات؛
- تغيير كلمات المرور بانتظام والتأكد من أن كلمات المرور قوية (أي استخدام توليفة من الأرقام والأحرف والرموز الخاصة)؛
- إعداد نسخ احتياطية للبيانات بانتظام؛
- التوصيل بالشبكات العامة المأمونة فقط.

وفي مثال آخر، طور الفريق BtCIRT في بوتان برامج توعية مصممة لتلبية احتياجات الأمن السيبراني الناشئة عن التعاملات المهنية والشخصية اليومية للمستعملين النهائيين العموميين في جميع أنحاء البلاد.[38] وعُرض على المشاركين الكيفية التي تُنفذ بها الهجمات من خلال الهندسة الاجتماعية وعمليات التصيد الاحتيالي، وكيفية التوصيل المأمون باستخدام البريد الإلكتروني وخدمات وسائل التواصل الاجتماعي، وما هي التهديدات الشائعة والاستجابات العلاجية. وقد حققت برامج التوعية في بوتان نجاحاً باهراً في توعية المستعملين بالمخاطر الأمنية وتلقت تعليقات إيجابية. وبينما ينصب تركيزه حالياً على المسؤولين الحكوميين، يتطلع الفريق BtCIRT إلى توسيع جهوده لتشمل الأطفال وغيرهم من المستعملين الضعفاء.

وهناك مثال آخر خلاق قدمته بوتان، وهو إطلاق مسابقة وطنية سنوية للمواقع الإلكترونية، تنظمها إدارة تكنولوجيا المعلومات والاتصالات بوزارة المعلومات والاتصالات.[39] وتشارك جميع المواقع الحكومية في المسابقة، حيث يتم اختيار أفضل موقع إلكتروني في البلاد بناءً على المعايير الأساسية التالية:

- إمكانية الاستخدام والموثوقية
- المحتوى والسريان
- الأمن والتيسر
- المظهر العام
- التصميم التفاعلي.

وبالمثل، أطلقت البرازيل، في نوفمبر 2019، حملة "Safe Connection" (#ConexãoSegura) للتوعية بالأمن السيبراني من خلال وكالة الاتصالات الوطنية البرازيلية (Anatel).[40] وقدمت الحملة نصائح للمستهلكين حول حماية البيانات الشخصية وإعداد كلمات مرور مأمونة. وكانت الحملة مدفوعة بشكاوى المستهلكين حول محاولات الاحتيال والشكوك حول كيفية حماية البيانات الشخصية. ومع ظهور جائحة COVID-19 وزيادة عمليات الاحتيال الجديدة، تم إعداد منشورات إلكترونية جديدة حول عمليات الاحتيال والتصيد الخاصة بجائحة COVID-19 لمساعدة المستعملين. وقد نُشرت هذه المنشورات أيضاً عبر شبكات التواصل الاجتماعي التابعة لشركة Anatel، بما في ذلك Facebook وTwitter وInstagram وLinkedIn. وفيما يلي بعض أفضل الممارسات الرئيسية للحملة:

- استخدام جميع خيارات الأمن التي توفرها التطبيقات المتنقلة، مثل الاستيقان ذي العاملين؛
- إنشاء كلمات مرور قوية وآمنة من خلال الجمع بين الأحرف الكبيرة والصغيرة والأرقام والرموز الخاصة؛
- الحذر من رسائل البريد الإلكتروني والرسائل المرفق بها فواتير والاتصال دائماً بقسم خدمة العملاء بالشركة للتحقق مما إذا كان المستند حقيقياً؛
- عدم تقديم معلومات شخصية أو كلمات مرور عند الرد على مكالمات غير معروفة.[41]

[38] الوثيقة SG2RGQ/79 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان
[39] الوثيقة SG2RGQ/135 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان
[40] الوثيقة SG2RGQ/215 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من البرازيل
[41] يمكن الاطلاع على مزيد من المعلومات عن حملة Safe Connection لشركة Anatel على الموقع الإلكتروني التالي: https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaoseguro-confira-dicas-para-proteger-dados-pessoais

وقدمت المملكة المتحدة دراسة حالة عن أفضل الممارسات المتعلقة بمرونة الأمن السيبراني للشركات الصغيرة والمتوسطة، حيث أوجزت الجهود المبذولة لتحسين المرونة السيبرانية للمنظمات في جميع أنحاء البلاد.[42] ومن الأمثلة على هذه الجهود حملة الاتصالات Cyber Aware، والتي، تسعى بخلاف زيادة الوعي، إلى تبني سلوكيات الأمن السيبراني الأساسية على نطاق واسع. وأطلقت الحملة، التي تستهدف الجمهور والشركات الصغيرة، في أبريل 2020، بعد أن أعيد تطويرها بسرعة لمواجهة مشهد التهديد السيبراني المتغير الناتج عن جائحة COVID-19. وروجت الحملة لتدابير التخفيف القابلة للتنفيذ، المدعومة بإرشادات جديدة حول كيفية العمل بأمان من المنزل، ونقل الأعمال التجارية عبر الإنترنت، واستخدام المؤتمرات الفيديوية. وتشمل الأدوات الأخرى:

- دليل شركات الأعمال الصغيرة بشأن الأمن السيبراني؛
- دليل شركات الأعمال الصغيرة بشأن الاستجابة والتعافي، والذي يوفر خطة استمرارية الأعمال لمساعدة الشركات الصغيرة والمتوسطة على الاستعداد للحوادث السيبرانية وتخفيف آثارها المحتملة؛
- التمرين في صندوق، أداة مجانية عبر الإنترنت لمساعدة الشركات الصغيرة والمتوسطة على اختبار مرونتها السيبرانية وإكمال الدورات التدريبية الصغرية دون الحاجة إلى معارف تقنية واسعة؛
- إرشادات COVID-19 لمساعدة الشركات على البقاء آمنة مع التكيف مع الوباء، وتغطي موضوعات مثل العمل في المنزل ونقل العمليات التجارية عبر الإنترنت.

وقدمت المملكة المتحدة أيضاً تفاصيل عن مخطط منح الشهادات المدعوم من الحكومة، Cyber Essentials، الذي يهدف إلى حماية الشركات من الهجمات السيبرانية للسلع الأساسية دون إلزامها بالامتثال لمعايير معقدة متعددة. وقد صُمم المخطط Cyber Essentials بحيث يمكن تنفيذه من قبل جميع المنظمات، حتى تلك التي ليس لديها معرفة مسبقة بالأمن السيبراني أو فريق سيبراني مخصص.

4.2 أُطر مخاطر الأمن السيبراني

تعد أُطر مخاطر الأمن السيبراني ضرورية لكل من المنظمات الحكومية وغير الحكومية. وعادة ما تكون هذه الأطر طوعية توفر المبادئ التوجيهية وأفضل الممارسات لإدارة المخاطر الرقمية. وخلال فترة الدراسة، تلقت لجنة الدراسات مساهمات من الكيانات التي قدمت أمثلة ونهجاً مختلفة لأُطر مخاطر الأمن السيبراني.

فعلى سبيل المثال، قام المعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة مؤخراً بتحديث إطاره لتحسين الأمن السيبراني للبنية التحتية الحرجة.[43] وهو إطار استباقي تحركه مصالح الأعمال من أجل الإدارة الطوعية للمخاطر السيبرانية وهو مصمم للشركات، أياً كان حجمها، التي تعمل في قطاعات مختلفة من الاقتصاد. وهو يمثل نقطة انطلاق ولغة مشتركتين لتقييم المخاطر السيبرانية، وهو قابل للتكيف بسهولة، بما يمكن المنظمات - أياً كان حجم أو درجة مخاطر الأمن السيبراني أو تعقد هذا الأمن - من تطبيق المبادئ وأفضل الممارسات الخاصة بإدارة المخاطر لتحسين أمن البنية التحتية الحرجة وقدرتها على تجاوز العثرات.

وقد وُضع الإطار من خلال التعاون الناجح بين القطاعين العام والخاص في مجال إدارة المخاطر التي يتعرض لها الأمن السيبراني، بعد عملية تطوير طوعية على مدى سنة واحدة تخللتها مدخلات من أكثر من 3 000 من أصحاب المصلحة من الأوساط الصناعية والأكاديمية والحكومية والشركاء الدوليين.

ويستند الإطار إلى المعايير والمبادئ التوجيهية الدولية وأفضل الممارسات الصناعية الحالية التي أثبتت فعاليتها في حماية أنظمة تكنولوجيا المعلومات من التهديدات السيبرانية، وضمان سرية الأعمال، وحماية خصوصية الأفراد والحريات المدنية، بغية حماية البنية التحتية الحرجة من خلال إدارة المخاطر. وبالإضافة إلى ذلك، يوفر الإطار هيكلاً لتنظيم الممارسات، فضلاً عن أدوات لدعم استخدام المعايير والممارسات واعتمادها. وبما أن الإطار يستند إلى مرجعية المعايير المعترف بها عالمياً للأمن السيبراني، فهو يمتلك أيضاً المرونة اللازمة ليكون نموذجاً دولياً لإدارة المخاطر السيبرانية.

[42] الوثيقة SG2RGQ/272 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة
[43] الوثيقة SG2RGQ/151 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الولايات المتحدة

وبناءً على تعليقات أصحاب المصلحة، أجرى المعهد الوطني للمعايير والتكنولوجيا التحديثات التالية على الإصدار 1.1 من الإطار:

- إعلان قابلية تطبيق الإطار على "التكنولوجيا"، التي تتألف، كحد أدنى، من تكنولوجيا للمعلومات، وتكنولوجيا تشغيلية، وأنظمة سيبرانية مادية، وإنترنت الأشياء؛
- تعزيز توجيهات تطبيق الإطار على إدارة مخاطر سلسلة الإمداد؛
- تلخيص أهمية وفائدة القياسات المقدمة في الإطار بالنسبة للتقييم الذاتي للمنظمات؛
- توفير معلومات إضافية بشأن التقييم الذاتي لمخاطر الأمن السيبراني ؛
- إيلاء قدر أكبر من الاعتبار لمتطلبات التخويل والاستيقان وإثبات الهوية والكشف عن نقاط الضعف؛
- توفير تحديث إداري للمراجع الإعلامية بحيث تعكس التطورات في المعايير والمبادئ التوجيهية الصادرة عن المنظمات الخاصة والعامة.

بالإضافة إلى ذلك، أصدرت سلطة النقد الملكية (البنك المركزي) في بوتان توجيهاً يعزز تنفيذ إطار الأمن السيبراني للمؤسسات المالية من أجل تعزيز مرونة النظام المصرفي في مواجهة المخاطر السيبرانية غير المعروفة والمتقدمة.[44] ويغطي التوجيه المجالات التالية:

- يجب على جميع البنوك الأعضاء العمل من أجل الامتثال لمعيار أمن بيانات صناعة بطاقات الدفع، والذي يهدف إلى حماية بيئات بيانات حاملي البطاقات. علاوةً على ذلك، يجب على البنوك تطبيق المعيار ISO/IEC 27001:2013، بشأن أنظمة إدارة أمن المعلومات، لاستكمال تدابير الأمن السيبراني الخاصة بها.
- يحدد التوجيه ضرورة إنشاء فريق استجابة سيبرانية للمؤسسة المالية لتعزيز التعاون النشط والتبادل الفعال للمعلومات المتعلقة بالأمن السيبراني بين البنوك وسلطة النقد الملكية. وسيرصد الفريق بنشاط التهديدات السيبرانية، ويخطط وينسق تدابير مكافحة التهديدات لمنع مخاطر الأمن السيبراني، ويبلغ عن أي حوادث إلى المشرف ذي الصلة أو السلطات ذات الصلة في أقرب وقت ممكن. وقد تم تشكيل فريق سيبراني للبنوك مؤخراً، مع تولي سلطة النقد الملكية الدور القيادي فيه.
- يجب على البنوك الأعضاء أيضاً تنفيذ إطار مراقبة الأمن السيبراني ذي الصلة والإجراءات المشجعة كإجراء فوري لضمان أمن المعلومات الأساسية.

وفي مثال منفصل، استحدثت الصين مؤشر تقييم لقياس الرؤية الوطنية في تخطيط وتطوير وتنفيذ أمن الشبكات، باستخدام ثلاثة مستويات من المؤشرات شديدة التعقيد.[45] ويقيّم المستوى الأول خمسة مؤشرات:

- *السياسات العامة*: الاستراتيجيات والتشريعات الوطنية والوكالات الحكومية والتعاون الدولي.
- *الصناعة*: تنمية صناعة أمن الشبكات في بيئة قائمة على السوق، بما في ذلك بيئة التنمية والحجم والقدرات والاستدامة.
- *التكنولوجيا*: البحث والتطوير ومستوى تطبيق الأمن الوطني في التكنولوجيا، بما في ذلك المشاريع المحددة للبحث العلمي والاستثمار والمعايير التقنية وتدريب الموظفين.
- *القدرات*: مستوى حماية أمن الشبكات ومنع التهديدات، بما في ذلك تصور المخاطر والحماية الأمنية والاستجابة للطوارئ والدفاع الفعّال.
- *الموارد*: الموارد اللازمة لدعم بناء القدرات، بما في ذلك موارد البنية التحتية للشبكات والتوعية بالأمن والتأثير على المستوى الدولي.

ويتضمن المؤشر أيضاً 19 مؤشراً من المستوى الثاني و53 مؤشراً من المستوى الثالث. وفي ظل نظام التقييم للمؤشر، تبلغ درجة كل مؤشر بين 0 و1 نقطة، تحصل 53 منها على أعلى درجة ممكنة. وتستند حسابات كل مؤشر إلى المعلومات العامة الرسمية المنشورة على المواقع الإلكترونية الوطنية والدولية والمقدمة من المؤسسات البحثية.

---

[44] الوثيقة SG2RGQ/135 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان

[45] الوثيقة 2/155 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الصين

5.2 الشراكات بين القطاعين العام والخاص

لا تستطيع الكيانات الحكومية وحدها تحسين أوضاع الأمن السيبراني الوطنية. وتتطلب جهود ومشاريع الأمن السيبراني الناجحة شراكات قوية بين كيانات القطاعين العام والخاص.

وفي الولايات المتحدة، طور المعهد الوطني للمعايير والتكنولوجيا إطاره لتحسين الأمن السيبراني للبنية التحتية الحرجة من خلال عملية تعاونية في إطار شراكة بين القطاعين العام والخاص.[46] وكما هو موضح بمزيد من التفصيل في القسم 4.2، حرص المعهد على ضمان مشاركة جميع أصحاب المصلحة في إعداد التحديث من أجل تشجيع أقصى قدر من الامتثال للإطار. ومن خلال إشراك أصحاب المصلحة وإدماج تعليقاتهم في الإصدار 1.1 من الإطار، كان أصحاب المصلحة أكثر ميلاً لاتباع أفضل الممارسات والمبادئ التوجيهية والمعايير المتضمنة وتنفيذها.

وفي جمهورية كوريا، وضعت وزارة العلوم وتكنولوجيا المعلومات والاتصالات الخطة الوطنية الأساسية للأمن السيبراني لعام 2019 للقطاع الخاص بالتشاور مع أصحاب المصلحة المعنيين، بما في ذلك الأوساط الأكاديمية والصناعة ومنظمات القطاع العام.[47] وحددت الخطة هدفين: ضمان توفير فضاء سيبراني آمن وتطوير صناعة أمن المعلومات. وكانت المشاريع الاستراتيجية الرئيسية لتحقيق هذه الغاية تهدف إلى توسيع شبكة الأمن السيبراني، والنهوض بصناعة أمن المعلومات، وتعزيز البنية التحتية لأمن المعلومات.

ونظراً لبيئة تكنولوجيا المعلومات والاتصالات سريعة التغير، تعتزم الوزارة تحديث الخطة كل عام. كما يجتمع المجلس الاستشاري المشترك بين القطاعين العام والخاص في جمهورية كوريا مرتين سنوياً لرصد التقدم المحرز في تنفيذ الخطة وتحديد مجالات التحسين.

وكما هو موضح في القسم 1.2، تعد الإستراتيجية الوطنية للأمن السيبراني في البرازيل، E-Ciber، مثالاً آخر على أهمية الشراكات بين القطاعين العام والخاص (PPP) في تطوير استراتيجيات وطنية شاملة للأمن السيبراني. ويُسلط الضوء على الشراكات بين القطاعين العام والخاص في الإجراءات الاستراتيجية الرئيسية الواردة في الاستراتيجية E-Ciber، والتي تشمل تهيئة بيئة تعاونية وتشاركية وآمنة وجديرة بالثقة بين القطاعين العام والخاص والمجتمع المدني وتوسيع شراكات الأمن السيبراني بين القطاعين العام والخاص والأوساط الأكاديمية والمجتمع المدني.

وفي مثال جيد آخر على الشراكات بين القطاعين العام والخاص، قدمت البرازيل لمحة عامة عن تجربتها في تنظيم تدريب سيبراني وطني، يُعرف باسم تمرين الحارس الإلكتروني، في عام 2018، مع التركيز على البنية التحتية الحرجة الوطنية.[48] وفي عام 2019، نظمت البرازيل تمريناً للمتابعة، مما وسع نطاق المشاركين بشكل كبير ليشمل ممثلين عن وزارات الدفاع والعدل والشؤون الخارجية، ومكتب الأمن المؤسسي، والقوات المسلحة، والوكالات الحكومية الفيدرالية مثل Anatel ، والأفرقة CSIRT الوطنية، والبنك المركزي البرازيلي والبنوك العامة والخاصة وشركات الطاقة النووية والكهربائية وشركات الاتصالات والباحثين الأكاديميين والمراقبين الإقليميين والدوليين المدعوين.

ومن الأمثلة أخرى للشراكات بين القطاعين العام والخاص الأفرقة CERT/CSIRT/CIRT. تستطيع الوكالات العامة والقطاع الخاص العمل معاً، من خلال هذه الأفرقة للتعامل مع أحداث الأمن السيبراني. والتعاون والثقة ضروريان لضمان استمرار فعالية هذه الأفرقة.

6.2 التدابير/المبادرات الإضافية لبناء القدرات

1.6.2 إنشاء مؤسسات تعليمية للأمن السيبراني

بناءً على إدراك أن الاستثمار في التدريب والتعليم في مجال الأمن السيبراني ضروري لمكافحة تحديات الأمن السيبراني المتنامية، أنشأت العديد من الحكومات مؤسسات تعليمية لتدريب الجيل القادم من خبراء الأمن السيبراني. وأقرت العديد من المساهمات الواردة من الدول الأعضاء في الاتحاد خلال فترة الدراسة بضرورة بذل جهود في هذا المجال، بما في ذلك من خلال تعزيز العلاقات بين أصحاب المصلحة العامين والجامعات ومراكز البحوث.

[46] الوثيقة SG2RGQ/151 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الولايات المتحدة
[47] الوثيقة 2/168 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من جمهورية كوريا
[48] الوثيقة SG2RGQ/214 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من البرازيل

فعلى سبيل المثال، أنشأت تشاد في عام 2015 المدرسة الوطنية العليا لتكنولوجيا المعلومات والاتصالات (ENASTIC)، مما يدل بوضوح على الإرادة السياسية للسلطات العليا في البلاد لتوفير إطار للتعليم المتقدم في مجال تكنولوجيا المعلومات والاتصالات (بما في ذلك منح درجات علمية في مجال الأمن السيبراني والشبكات والاتصالات، وما إلى ذلك).[49]

وبالمثل، أنشأت السنغال المدرسة الوطنية للأمن السيبراني (ENC) ذات التركيز الإقليمي لبناء القدرات وزيادة الوعي بين صناع القرار وكبار موظفي الدفاع وغيرهم من المشاركين في النظام الإيكولوجي الرقمي للمنطقة.[50]

وتشمل المهام الرئيسية للمدرسة توفير ما يلي:

- التدريب وزيادة الوعي لمسؤولي الدولة والموظفين والطلاب السنغاليين والأجانب، والأفراد في قطاعي الأمن السيبراني العام والخاص من أجل تحسين فهم المخاطر والتهديدات؛
- التدريب المنتظم لمساعدة موظفي الأفرقة CERT/CSIRT المتخصصة على الاستجابة لأكثر الهجمات السيبرانية تعقيداً؛
- التدريب الدوري لموظفي المؤسسات الحكومية ودون الإقليمية لمنحهم القدرة والمعرفة للتأهب للحوادث والاحتراز منها والاستجابة لها والتعافي منها.

2.6.2 المبادرات الأخرى لبناء القدرات

قدمت جهة الاتصال المعنية بالأمن السيبراني بمكتب تنمية الاتصالات (BDT)، على مدار فترة الدراسة، تحديثات منتظمة عن برنامج عمل المكتب، بما في ذلك مبادراته المختلفة لبناء القدرات. ويعمل المكتب بشكل مشترك مع منظمات وكيانات مختلفة لتوفير التدريب على بناء القدرات للبلدان النامية، بما في ذلك إجراء تمارين التدريب السيبراني، والمساعدة في إنشاء الأفرقة CSIRT وإدارة الدورات التدريبية. كما سُلط الضوء على هذه الجهود في مساهمات الدول الأعضاء وأعضاء القطاع. انظر **الملحق 1** للاطلاع على مزيد من المعلومات.

[49] الوثيقة 2/136 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من تشاد
[50] الوثيقة SG2RGQ/146 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من السنغال

الفصل 3 - حماية الأطفال على الإنترنت (COP)

1.3 نظرة عامة

لم تعد الإنترنت في العصر الحديث مجرد بنك للمعرفة - "مكتبة ضخمة وفوضوية" - كما كان في عصر الويب 1.0. لقد أصبحت منصة للاتصالات يستخدمها الجميع، بما في ذلك الأطفال. وفي الواقع، يشكل الأطفال ثلث مستعملي الإنترنت في العالم، وفقاً لمنظمة الأمم المتحدة للطفولة (اليونيسف).[51]

ولقد تطورت طبيعة التهديدات على الخط التي يواجهها الأطفال. فبينما كانت التهديدات السابقة تقوم على المعلومات بصورة بحتة - على سبيل المثال، النفاذ إلى معلومات عن المخدرات أو المواد الإباحية أو الحركات المتطرفة - فإن التهديدات الحالية هي أيضاً ذات طبيعة سلوكية، مثل التفسخ الاجتماعي، وإدمان القمار، والإنفاق غير المنضبط، والتنمر الافتراضي، والكشف عن البيانات الشخصية والمعارف الخطيرة.

فعلى مدى السنوات العشر الماضية، كان المجتمع التكنولوجي يبتكر بنشاط أساليب لحماية الأطفال من المواقع التي تحتوي على معلومات غير ملائمة، لكن المطورين وأولياء الأمور يواجهون الآن تحدياً جديداً، وهو كيفية تعريف المستعملين الصغار بشكل سليم بالفضاء الرقمي وكيفية التحكم بسرعة وتصحيح السلوك الافتراضي. ومع التطور السريع لتكنولوجيا الإنترنت، امتدت مشكلة حماية الأطفال، التي يوجد إجماع عالمي عليها، بشكل طبيعي لتشمل الفضاء السيبراني. وتعتبر سلامة الفضاء السيبراني أمراً بالغ الأهمية عندما يتعلق الأمر بتعريف الأطفال بالأجهزة الرقمية والإنترنت.

وينص إعلان بوينس آيرس الذي اعتمده المؤتمر العالمي لتنمية الاتصالات لعام 2017 على *"أنه ينبغي استغلال الفرص التي توفرها الاتصالات/تكنولوجيا المعلومات والاتصالات استغلالاً تاماً بهدف كفالة توفير النفاذ المنصف إلى الاتصالات/تكنولوجيا المعلومات والاتصالات وإلى الابتكارات التي تعزز التنمية الاجتماعية والاقتصادية المستدامة والحد من الفقر وتوفير فرص العمل والمساواة بين الجنسين وحماية الأطفال على الإنترنت وريادة الأعمال وتعزيز الشمول الرقمي والتمكين للجميع"*.[52]

ويحدد القراران 179 (المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين للاتحاد و67 (المراجَع في بوينس آيرس، 2017) للمؤتمر العالمي لتنمية الاتصالات دور الاتحاد وقطاع تنمية الاتصالات في حماية الأطفال على الإنترنت.

وكما بينت جائحة COVID-19، تتطور أنماط سلوك المهاجمين والشبكات الإجرامية باستمرار، ويستغل الجناة حقيقة أن الكثير من الأطفال يقضون وقتاً أطول بكثير من المعتاد على الإنترنت. وفي هذه الظروف، يأتي المنشور الخاص بالمبادئ التوجيهية لعام 2020 بشأن حماية الأطفال على الإنترنت (COP)، في الوقت المناسب، والذي وضع لحماية رفاه الأطفال وأمانهم وسلامتهم.[53]

واشترك في إعداد المبادئ التوجيهية الاتحاد الدولي للاتصالات وفريق عمل مكون من مؤلفين من المؤسسات الرائدة النشطة في قطاع تكنولوجيا المعلومات والاتصالات، وكذلك في مسائل حماية الأطفال وحقوقهم (على الإنترنت). وتوفر المبادئ التوجيهية مجموعة شاملة من التوصيات لأصحاب المصلحة المعنيين كافة بشأن كيفية المساهمة في تهيئة بيئة آمنة وتمكينية على الإنترنت للأطفال والشباب. وتهدف المبادئ التوجيهية إلى زيادة الوعي بنطاق حماية الأطفال على الإنترنت وتوفر الموارد والأدوات اللازمة لمساعدة الأطفال وعائلاتهم في تطوير المهارات الرقمية، كما تهدف إلى مساعدة أصحاب المصلحة من الصناعة والهيئات الحكومية في وضع سياسات واستراتيجيات مؤسسية ووطنية لحماية الأطفال على الإنترنت. إن المبادئ التوجيهية، الموجهة للأطفال وأولياء الأمور والمعلمين والصناعات وواضعي السياسات، مصممة بحيث تعمل كمخطط يمكن تكييفه حسب الأعراف والقوانين الوطنية والمحلية.

وفي إطار الخطة الاستراتيجية للاتحاد المحددة في القرار 71 (المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين للاتحاد، فإن من بين أهداف قطاع تنمية الاتصالات *"دعم تطوير واستخدام الاتصالات/تكنولوجيا المعلومات والاتصالات وتطبيقاتها لتمكين الأشخاص والمجتمعات تحقيقاً للتنمية المستدامة"* (الفقرة 4.D). ويتعين على قطاع تنمية الاتصالات أن يوف، بشكل خاص، *"منتجات وخدمات بشأن الشمول الرقمي للنساء والفتيات*

---

51 منظمة الأمم المتحدة للطفولة (UNICEF)، تقرير حالة الأطفال في العالم لعام 2017. ديسمبر 2017.
52 الاتحاد الدولي للاتصالات. المؤتمر العالمي لتنمية الاتصالات (بوينس آيرس، 2017). إعلان بوينس آيرس. أكتوبر 2017.
53 الاتحاد الدولي للاتصالات. مبادئ توجيهية بشأن حماية الأطفال على الإنترنت.

والأشخاص ذوي الاحتياجات المحددة (كبار السن والشباب والأطفال والسكان الأصليين وغيرهم) مثل استراتيجيات وسياسات وممارسات زيادة الوعي بالشمول الرقمي ومجموعات أدوات تنمية المهارات الرقمية ومبادئ توجيهية ومنتديات نقاش لتبادل الممارسات والاستراتيجيات"، بغية تحقيق أهداف، من بينها، دعم حماية الأطفال على الإنترنت (الفقرة 3-4.D).

وتُغطى أنشطة حماية الأطفال على الإنترنت في قطاع تنمية الاتصالات وأعضائه في البند 2(د) من اختصاصات المسألة 3/2:

(د) مواصلة جمع التجارب الوطنية من الدول الأعضاء فيما يتصل بالأمن السيبراني وحماية الأطفال على الإنترنت، وتحديد المواضيع المشتركة ودراستها في إطار تلك التجارب، باستخدام هذه المعلومات لوضع مبادئ توجيهية تمكّن الدول الأعضاء من وضع آليات فعّالة لضمان الأمن في البيئة الرقمية.

2.3 أفضل الممارسات والاتجاهات المشتركة لدى الدول الأعضاء في الاتحاد

خلال فترة الدراسة، ركزت الأنشطة الرئيسية لحماية الأطفال على الإنترنت التي اضطلعت بها الدول الأعضاء على زيادة الوعي ووضع اللوائح وإجراء الاستقصاءات المواضيعية.

زيادة الوعي

هناك العديد من الجوانب لحماية الأطفال في الفضاء السيبراني، والتي لا تتطلب أدوات ومنصات فحسب، بل تتطلب أيضاً بيانات مناسبة. وينبغي استخدام البرامج الثقافية لنشر هذه الموارد في جميع أنحاء المجتمع.

فعلى سبيل المثال، طورت منظمة تكنولوجيا المعلومات الإيرانية مشروع الأطفال والإنترنت (KOVA) لحماية الأطفال في الفضاء السيبراني والذي تم اختياره كمشروع مرشح في مسابقة جوائز القمة العالمية لمجتمع المعلومات في عام 2018.

ونظراً للتطور السريع في البنية التحتية للإنترنت في السنوات الأخيرة والعدد الكبير من مستعملي الإنترنت الشباب، بما في ذلك الأطفال، أطلقت الحكومة الإيرانية في عام 2016 برنامجاً وطنياً لحماية الأطفال على الإنترنت. وأطلقت وزارة الاتصالات وتكنولوجيا المعلومات، في إطار البرنامج، مشروع KOVA لزيادة الوعي بين الأطفال وأولياء أمورهم فيما يتعلق بمخاطر الإنترنت وكيفية حماية الأطفال منها. والأهداف الرئيسية للمشروع هي:

- تحديد أهم التهديدات التي يتعرض لها الأطفال في الفضاء السيبراني وتقديم الحلول وخدمات الحماية القانونية؛
- بناء الوعي بين طلاب المدارس الابتدائية وطلاب المدارس الثانوية والمدرسين وأولياء الأمور حول التهديدات المختلفة التي يتعرض لها الأطفال بمختلف أعمارهم؛
- مساعدة الأطفال والمراهقين على استخدام وسائل التواصل الاجتماعي والإنترنت بشكل سليم وآمن؛
- الرد على الأسئلة التي يطرحها الأطفال والمراهقون والمعلمون وأولياء الأمور حول تحديات الأمن والسلامة في الفضاء السيبراني.

ولتحقيق أهداف المشروع، استُخدمت مجموعة متنوعة من الأدوات والأساليب (مثل المسرح والأفلام والرسوم المتحركة) لتعليم الأطفال السلامة على الإنترنت. وفي المرحلة الأولى من المشروع، تلقى أكثر من 200 000 تلميذ في 900 مدرسة تدريباً، والهدف الوصول في المرحلة الثانية إلى 000 4 مدرسة.[54]

في بوتان، زاد عدد مستعملي الإنترنت بأكثر من 28 في المائة منذ عام 2016، نتيجة لزيادة سهولة النفاذ، والقدرة على تحمل تكاليف التوصيل، وتوافر الهواتف الذكية الأرخص ثمناً. ويتمتع معظم أطفال المدارس بإمكانية الحصول إلى هاتف ذكي، مما يزيد من مخاطر التعرض لحوادث أمنية. ولا يوجد في بوتان حتى الآن منهج دراسي حول الأمن السيبراني، لأن زيادة استخدام الإنترنت والأجهزة المتنقلة هو اتجاه حديث. ومع ذلك، من الأهمية بمكان أن تتبنى الحكومات الأوقات المتغيرة من خلال تضمين الأمن السيبراني في المناهج الدراسية. وقد بدأت الكليات الخاصة في بوتان بالفعل في استكشاف كيفية توفير برامج الدرجات العلمية ذات الصلة، لا سيما في

[54] الوثيقة 82/2 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من جامعة إيران للعلوم والتكنولوجيا (جمهورية إيران الإسلامية)

مجال الأمن السيبراني. ويحتاج أطفال المدارس إلى أن يكونوا على دراية بمثل هذه المخاطر، لأنهم أكثر عرضة للهجمات التي تقع في شكل التصيد والألعاب على الخط.[55]

من خلال فحص عادات وسلوكيات الأطفال على الإنترنت عن طريق هذه الدراسة، تقوم بوتان بتطوير مقاطع فيديو بالرسوم المتحركة تغطي مواضيع مثل الاتجار بالأطفال والتنمر السيبراني والخصوصية وأمن الألعاب عبر الإنترنت، ستقوم ببثها عبر التلفزيون الوطني. وتقوم أيضاً بوضع ملصقات وكتيبات تشمل أفضل الممارسات في مجال الأمن السيبراني تستهدف الطلاب، سيجري توزيعها على مختلف المدارس في البلاد. كما تقوم بوتان بإنشاء فريق مهام على المستوى الوطني يضم ممثلين عن الوكالات المعنية لوضع المبادئ التوجيهية ذات الصلة بحماية الأطفال على الإنترنت في البلاد.[56]

وتنظم الصين أسبوعاً سنوياً وطنياً للدعاية لأمن الشبكات لزيادة الوعي بالأمن السيبراني وتحسين مهارات الحماية على الخط لجميع السكان من خلال المعارض والمنتديات والمسابقات والمحاضرات وأيام الدعاية المواضيعية والأنشطة الأخرى. فعلى سبيل المثال، تُقدم محاضرات حول أمن الشبكات لعرض المعارف والمهارات بما يتماشى مع احتياجات المجموعات المختلفة، مثل طلاب المدارس الابتدائية والثانوية وكبار السن والمجموعات الخاصة (مثل الأشخاص ذوي الإعاقة)، بناءً على مستوى مهاراتهم في مجال تكنولوجيا المعلومات.[57]

وتزود الولايات المتحدة الآباء والمعلمين بمعلومات عن ممارسات الأطفال والمراهقين، بما في ذلك: ما تنشره يمكن أن يستمر مدى الحياة! كن على علم بما يتم مشاركته! كن حذراً بشأن الكثير من المعلومات الشخصية! انشر فقط عن الآخرين ما تود منهم أن ينشروه عنك! امتلك تواجدك على الإنترنت من خلال تحديد من يمكنه رؤية المعلومات ومشاركتها! تعرف على البيانات التي يتم جمعها![58]

التنظيم

نظراً للتوافر الواسع لتكنولوجيا المعلومات، تتخذ الحكومات خطوات تنظيمية جادة لضمان سلامة جميع المواطنين الذين لديهم وسيلة للنفاذ إلى الإنترنت، ولا سيما القصر. وبينما تختلف تشريعات الأمن السيبراني اختلافاً طفيفاً حول العالم، تظل جذور المشكلة كما هي.

ومن الأسباب الرئيسية لظهور مثل هذه اللوائح هو الضعف الخاص للأطفال في سن ما قبل المدرسة والمدرسة الابتدائية على الإنترنت، الذين يقعون بسهولة ضحية للمتحرشين عبر الإنترنت (الأشخاص الذين يتحرشون جنسياً بالقصر عبر الإنترنت)، والإذلال والاستمالة عبر الإنترنت (التي يكتسب فيها شخص غريب ثقة الطفل لأغراضه الخاصة)، وإساءة استخدام البيانات الشخصية.

وقد تحول الأطفال تدريجياً إلى المجموعة الأكثر تعرضاً لخطر الكشف عن الخصوصية وسرقة الهوية. لذلك فإن حماية المعلومات الشخصية للأطفال أمر ملحّ للغاية.

فعلى سبيل المثال، أصدرت الصين لائحة خاصة بشأن الحماية السيبرانية للمعلومات الشخصية للأطفال، تنظم دورة الحياة الكاملة لجمع المعلومات الشخصية للأطفال وتخزينها واستخدامها ونقلها وكشفها.[59] وتوفر اللائحة أشكال الحماية الخاصة والمبادئ الواضحة والإدارة التعاونية، بغية تهيئة بيئة ملائمة ومفيدة على الخط للنمو الصحي للأطفال. وتشمل أشكال الحماية الخاصة عدة أمور من بينها الحق في الحذف وعدم الكشف عن المعلومات الشخصية للأطفال، بينما تغطي المبادئ الضرورة المشروعة والموافقة عن علم والغرض الواضح والأمن والاستخدام القانوني. وتنطبق اللائحة بشكل أساسي على حماية المعلومات الشخصية الخاصة بالأطفال دون 14 عاماً.

وفي ديسمبر 2010، سن الاتحاد الروسي قانوناً بشأن حماية الأطفال من المعلومات الضارة بصحتهم ونموهم يضمن أمن المعلومات الخاصة بالقصر، ويحدد شروط وإجراءات نشر المعلومات بين الأطفال.[60]

[55] الوثيقة SG2RGQ/79 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان
[56] الوثيقة 2/385 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان
[57] الوثيقة 2/286 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الصين
[58] الوثيقة 2/400 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الولايات المتحدة
[59] الوثيقة SG2RGQ/179 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الصين
[60] الوثيقة 2/264 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الاتحاد الروسي

وإلى جانب ذلك، يحظر قانون الإعلام بالاتحاد الروسي النشر عبر وسائل الإعلام أو عبر أي شبكة معلومات واتصالات (مثل الإنترنت) لمعلومات عن أي قاصر يقع ضحية أي فعل (أو إهمال) غير قانوني، بما في ذلك:

- اللقب أو الاسم الأول أو اسم الأب؛
- الصور الفوتوغرافية أو المقاطع الفيديوية للقاصر أو والديه أو الممثلين القانونيين الآخرين؛
- تاريخ ميلاد القاصر؛
- تسجيل صوتي لصوت القاصر؛
- مكان إقامة القاصر أو عنوانه المؤقت؛
- المكان الذي يدرس أو يعمل فيه القاصر؛
- أي معلومات أخرى يمكن استخدامها لتحديد هوية القاصر بشكل مباشر أو غير مباشر.[61]

الاستقصاءات المواضيعية

قدم الاتحاد المساعدة التقنية في عملية الصياغة الجارية لاستراتيجية بوتان الوطنية للأمن السيبراني.[62] وأثناء هذه العملية، أجري استقصاء لعدد 126 طالباً (بمتوسط عمر 16 عاماً)، حيث تم استخدام أسئلة الاختيار من متعدد لتقييم استخدام الإنترنت، والحوادث الأمنية مثل التسلط السيبراني، وانتشار فيروسات الحاسوب أو الجرائم التي يرتكبها الطلاب.

وأظهر الاستقصاء أن الطلاب كانوا يستخدمون الإنترنت بشكل مكثف. واستخدم جميع الطلاب الذين شاركوا في الاستقصاء تقريباً الإنترنت، واستخدم أكثر من 40 في المائة الإنترنت لأكثر من ساعتين في اليوم. وكان الأمن السيبراني موضوعاً ملحاً للطلاب: ففي حين تعرض ما يقرب من 40 في المائة للإصابة بالبرمجيات الضارة، أفاد حوالي 10 في المائة فقط أنهم استخدموا برمجيات مكافحة الفيروسات.

وفيما يتعلق بتعليم الأمن السيبراني، لا تزال المدرسة مصدراً مهماً للمعرفة للطلاب. فقد أفاد ما يقرب من 40 في المائة من الطلاب أنهم علموا عن الأمن السيبراني من المدرسة.

كما تعرض الطلاب للجرائم السيبرانية وأنشطة ضارة أخرى. وبصرف النظر عن الفيروسات الحاسوبية، كان أكثر من 10 في المائة من الطلاب الذين شملهم الاستطلاع ضحايا للتسلط السيبراني، في حين تم الاتصال بنسبة 25 في المائة من قبل شخص غريب عبر الإنترنت. وتضمن الاستبيان أيضاً قسماً عن الأفعال غير القانونية أو غير اللائقة، والذي كشف أن حوالي 35 في المائة من الطلاب أرسلوا رسائل تنمر أو ضارة يمكن اعتبارها تسلطاً سيبرانياً. وحاول نفس العدد تقريباً من الطلاب اقتحام شبكة لاسلكية محمية أو نجحوا في ذلك.

ولما كانت الدراسة الاستقصائية الأولية محدودة، أجرت بوتان دراسة استقصائية أخرى بشأن سلامة وحماية الأطفال على الإنترنت على الصعيد الوطني. وكانت الدراسة الاستقصائية جزءاً من مشروع " التكنولوجيا الرقمية للأطفال في آسيا والمحيط الهادئ" (DKAP) الذي أطلقته اليونسكو (مكتب اليونيسكو في بانكوك) بدعم من الصناديق الاستئمانية الكورية (KFIT). وشملت الدراسة 381 2 طالباً تتراوح أعمارهم بين 12 و17 عاماً من 45 مدرسة في البلاد، يُوجه إليهم 112 سؤالاً من أجل التأكد من مستوى الوعي بالأمن السيبراني والتهديدات والتدابير الوقائية. وقد أظهرت الدراسة أن غالبية الطلاب (81 في المائة) لديهم إمكانية الوصول إلى الهواتف الذكية في المنزل. ويميل معظم الطلاب إلى قضاء ما متوسطه ساعة إلى ساعتين على الإنترنت يوميًا. علاوة على ذلك، يفتقر 54 في المائة من الطلاب إلى المعرفة اللازمة لفصل المعلومات الموثوقة عن المعلومات غير الموثوقة. ويخشى حوالي 49 في المائة من الطلاب أن يسيء شخص ما استخدام معلوماتهم الشخصية.

وهناك أيضاً عدد قليل من الطلاب (10 في المائة) الذين يتحايلون على التطبيقات المقيدة حسب العمر من خلال تقديم معلومات خاطئة، والتنمر على الآخرين وتسجيل الدخول إلى حسابات الآخرين. وبالإضافة إلى ذلك، فإن 85 في المائة من الطلاب يرغبون في تكوين صداقات جديدة على الإنترنت و68 في المائة من الطلاب لا يمانعون في التحدث إلى أشخاص من أماكن أو خلفيات مختلفة عنهم. وأثارت الدراسة مخاوف بخصوص السلامة،

---

[61] انظر المادة 4 من القانون الفيدرالي رقم 2124، https://digital.gov.ru/ru/documents/6406/ [بالروسية]. الوثيقة 2/264 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الاتحاد الروسي.

[62] الوثيقة SG2RGQ/135 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان

حيث إن 51 في المائة من الطلاب قد التقوا بغرباء قابلوهم عبر الإنترنت، وأن هناك أيضاً 22,8 في المائة من الطلاب المنفتحين على فكرة مقابلة الغرباء، حيث تميل الطالبات إلى مقابلة الغرباء أكثر من نظرائهن من الذكور.[63]

وفي كوت ديفوار، أجرت منصة مكافحة الجريمة السيبرانية استقصاءً شمل 200 شاب من ثلاث مدارس ثانوية في أبيدجان من أجل تحليل سلوك الأطفال على الإنترنت، وتحديد المخاطر واقتراح استراتيجيات أمنية فعالة لمكافحة إساءة الاستخدام على الخط.[64]

وفي المجمل، أفاد 83 في المائة من المستجيبين على الدراسة الاستقصائية أنهم استخدموا الإنترنت. وكان السبب الرئيسي لعدم استخدام النسبة المتبقية من المستجيبين للإنترنت هو تكلفة الهواتف الذكية والمطاريف. وبالنسبة للأطفال الذين تتراوح أعمارهم بين 15 و18 عاماً، تم تحويل التلفزيون إلى مستوى استخدام ثانوي، في حين كان لدى 86,3 في المائة حساب على وسائل التواصل الاجتماعي. وتفضل هذه الفئة العمرية النفاذ إلى الإنترنت من خلال الهواتف الذكية. وتم الإبلاغ عن الصور والأفلام العنيفة كمصدر أساسي للتجارب السلبية على الخط، تليها القرصنة، وأخيراً الإهانات والتهديدات. وأبلغ المستجيبون، بنسبة أقل، عن تجارب سلبية ذات دلالات جنسية. وأفاد بعض المستجيبين أنهم تعرضوا للابتزاز بسبب مقاطع فيديو جنسية صريحة.

ووفقاً للاستقصاء، كانت أكثر التجارب التي يُحتمل أن تكون ضارة للأطفال هي:

- الفيروسات أو الأعطال أو الرسائل الاقتحامية أو القرصنة (24 في المائة)
- مقاطع فيديو جنسية (7,5 في المائة)
- صور أو مقاطع فيديو عنيفة (28,6 في المائة)
- استخدام الصور دون موافقة مسبقة (7,5 بالمائة)
- الإهانات أو الحقد أو التهديدات (19,5 في المائة)
- سرقة الهوية (6,7 في المائة)
- التواصل مع شخص غريب (4,51 في المائة)
- عمليات الاحتيال (0,75 في المائة)
- الابتزاز الجنسي (0,75 في المائة).

دعم الاتحاد للدول الأعضاء فيما يتعلق بحماية الأطفال على الإنترنت

نظم الاتحاد، في الفترة من 4 إلى 6 أبريل 2018، بالتعاون مع أكاديمية A.S. Popov الوطنية للاتصالات في أوديسا، ورشة عمل إقليمية بشأن الأمن السيبراني وحماية الأطفال على الإنترنت لمنطقتي أوروبا وكومنولث الدول المستقلة (CIS) في أوديسا، أوكرانيا.[65] وقد نُشرت النسخ النهائية لجميع الوثائق (بما في ذلك جدول الأعمال والتقارير والاستنتاجات والتوصيات وقائمة المشاركين والعروض التقديمية والصور الفوتوغرافية) على الموقع الإلكتروني للأكاديمية[66] وعلى الموقع الإلكتروني للاتحاد.[67] وخلص المشاركون في ورشة العمل، الذين يمثلون 14 دولة عضواً، إلى أن منطقتي أوروبا وكومنولث الدول المستقلة بحاجة إلى زيادة التعاون فيما بينهما من أجل الاستخدام الأمثل للموارد المتاحة وتحقيق نتائج عملية، بما في ذلك من خلال ترجمة المواد التدريبية الخاصة بالأمن السيبراني وحماية الأطفال على الإنترنت. وترد الاستنتاجات والتوصيات التي وضعها المشاركون في ورشة العمل في الوثيقة الختامية.[68]

وتعد حماية الأطفال على الإنترنت أحد المجالات الرئيسية التي تركز عليها مبادرة الاتحاد الإقليمية لمنطقة أوروبا بشأن بناء الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات. واستجابة لطلبات الأعضاء

---

63 الوثيقة 2/385 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من بوتان

64 الوثيقة 2/201 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من كوت ديفوار

65 الوثيقة 2/75، للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من أكاديمية A.S. Popov الوطنية للاتصالات في أوديسا (أوكرانيا)

66 أكاديمية A.S. Popov الوطنية للاتصالات في أوديسا، ورشة العمل الإقليمية للاتحاد الدولي للاتصالات لمنطقتي أوروبا وكومنولث الدول المستقلة - الأمن السيبراني وحماية الأطفال على الإنترنت، أوديسا، أوكرانيا، 4-6 أبريل 2018.

67 الاتحاد الدولي للاتصالات. ورشة العمل الإقليمية للاتحاد الدولي للاتصالات لمنطقتي أوروبا وكومنولث الدول المستقلة - الأمن السيبراني وحماية الأطفال على الإنترنت، أوديسا، أوكرانيا، 4-6 أبريل 2018.

68 الاتحاد الدولي للاتصالات. الاستنتاجات والتوصيات. ورشة العمل الإقليمية للاتحاد الدولي للاتصالات لمنطقتي أوروبا وكومنولث الدول المستقلة بشأن الأمن السيبراني وحماية الأطفال على الإنترنت المنعقدة، أوديسا، أوكرانيا، 4-6 أبريل 2018.

لوضع خرائط طريق لمبادرات حماية الأطفال على الإنترنت، أجرى الاتحاد استقصاءً بين الحكومات الوطنية التي تغطيها المبادرة الإقليمية، تناول مجموعة واسعة من القضايا المتعلقة بالسياسات والممارسات المعاصرة عبر جميع المنصات التكنولوجية التي يستخدمها الأطفال والشباب في الفضاء الرقمي. وقد أُجري الاستقصاء للمرة الأولى بين جميع الدول الأعضاء في عام 2009، وأجريت نسخة معدلة في عام 2016 بين الدول الأعضاء من أوروبا الوسطى والشرقية والبلطيق والبلقان.

بناء على الردود على الاستقصاء، أصدر مكتب تنمية الاتصالات في عام 2017 استعراضاً إقليمياً للأنشطة الوطنية المتعلقة بحماية الأطفال على الإنترنت في أوروبا، أشار إلى موقف البلدان المشاركة من حيث وضع السياسات واعتمادها وتنفيذها ومتابعتها في مجال حماية الأطفال على الإنترنت.[69] كما قدم الاستعراض أمثلة على الممارسات الحالية في ألبانيا، والبوسنة والهرسك، وبلغاريا، وقبرص، وكرواتيا، وإستونيا، وفنلندا، واليونان، وهنغاريا، ولاتفيا، وليختنشتاين، وليتوانيا، ومقدونيا الشمالية، وموناكو، والجبل الأسود، وبولندا، وسلوفاكيا، والجمهورية التشيكية، ورومانيا، وصربيا، وسلوفينيا، وتركيا.

ويقوم فريق العمل التابع لمجلس الاتحاد والمعني بحماية الأطفال على الإنترنت (CWG-COP) بعمله بما يتماشى مع القرار 1306 الصادر عن مجلس الاتحاد في دورته لعام 2009، بالإضافة إلى القرار 179 (المراجَع في دبي، 2018)، الذي قرر فيه مؤتمر المندوبين المفوضين أن يستمر الاتحاد في مبادرة حماية الطفل على الإنترنت كمنصة لزيادة الوعي بقضايا سلامة الأطفال على الإنترنت؛ ومواصلة تقديم المساعدة والدعم للدول الأعضاء، ولا سيما البلدان النامية، في وضع وتنفيذ خرائط طريق للمبادرة؛ ومواصلة تنسيق المبادرة، بالتعاون مع أصحاب المصلحة المعنيين.[70]

وقدمت معلومات عن الاجتماعات الخامس عشر والسادس عشر والسابع عشر للفريقCWG-COP، والتي عقدت في 26 سبتمبر 2019 و4 فبراير 2020 و26 يناير 2021، على التوالي في جنيف عن بُعد، كي تنظر فيها المسألة 3/2.[71]،[72]

وقد عُرضت الوثائق التالية في الاجتماع:

- تحديث عن مبادئ الاتحاد التوجيهية بشأن حماية الأطفال على الإنترنت (COP).[73]
- عرض بشأن نتائج مشاورة الشباب على الخط.[74]
- عرض بشأن عمل الاتحاد وأنشطته في مجال حماية الأطفال على الإنترنت.[75]
- عرض لعملية استعراض المبادئ التوجيهية بشأن حماية الأطفال على الإنترنت للفترة 2019-2020.[76]
- عرض بشأن مبادرة الاتحاد لحماية الأطفال على الإنترنت وتنفيذ المبادئ التوجيهية بشأن حماية الأطفال على الإنترنت لعام 2020.[77]

وكانت إحدى النتائج الرئيسية للاجتماعات هي الاعتراف بالحاجة إلى تقديم إرشادات حول كيفية تحسين عدد الردود من الشباب وزيادة إشراك ومشاركة أصحاب المصلحة في الفريق CWG-COP، نظراً لأهمية تقييم فعالية البرنامج.

---

69 قطاع تنمية الاتصالات في الاتحاد. استعراض إقليمي للأنشطة الوطنية المتعلقة بحماية الأطفال على الإنترنت في أوروبا، 2017.

70 الاتحاد الدولي للاتصالات. القرار 179 (المراجَع في دبي، 2018) لمؤتمر المندوبين المفوضين، بشأن دور الاتحاد الدولي للاتصالات في حماية الأطفال على الإنترنت.

71 الوثيقة SG2RGQ/242 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من فريق العمل التابع للمجلس المعني بحماية الأطفال على الإنترنت (CWG-COP).

72 يمكن الاطلاع على المساهمات المقدمة من الأعضاء ومن خبراء من الخارج على الروابط التالية: الاجتماع الخامس عشر، والاجتماع السادس عشر، والاجتماع السابع عشر.

73 الاتحاد الدولي للاتصالات. فريق العمل التابع للمجلس المعني بحماية الأطفال على الإنترنت، الوثيقة CWG-COP-14/2: تحديث بشأن مبادرة حماية الأطفال على الإنترنت (COP).

74 الاتحاد الدولي للاتصالات. فريق العمل التابع للمجلس المعني بحماية الأطفال على الإنترنت. الوثيقة CWG-COP-15/INF/3: مشاورة الشباب على الخط.

75 الاتحاد الدولي للاتصالات، الوثيقة CWG-COP-16/5: عمل الاتحاد وأنشطته في مجال حماية الأطفال على الإنترنت.

76 الاتحاد الدولي للاتصالات. فريق العمل التابع للمجلس المعني بحماية الأطفال على الإنترنت. الوثيقة CWG-COP-16/4: مبادرة الاتحاد لحماية الأطفال على الإنترنت: عملية استعراض المبادئ التوجيهية بشأن حماية الأطفال على الإنترنت للفترة 2019-2020.

77 الاتحاد الدولي للاتصالات. فريق العمل التابع للمجلس المعني بحماية الأطفال على الإنترنت. الوثيقة CWG-COP-17/2(Rev.1): مبادرة الاتحاد لحماية الأطفال على الإنترنت لعام 2020، حماية الأطفال وتمكينهم على الإنترنت.

وعقد الاتحاد في عام 2020 سلسلة من المنتديات المواضيعية لتبادل الخبرات[78] بشأن حماية الأطفال على الإنترنت بين مختلف أصحاب المصلحة وللترويج للمبادئ التوجيهية لحماية الأطفال على الإنترنت وتسهيل ترويجها وتكييفها ووضعها في سياقها على الصعيدين الوطني والإقليمي:

- إفريقيا: 30 أكتوبر 2020 [79]
- الأمريكتان: 19 أكتوبر 2020 [80]
- الدول العربية: 23 نوفمبر 2020 [81]
- آسيا والمحيط الهادئ: 3 نوفمبر 2020 [82]
- كومنولث الدول المستقلة: 27 أكتوبر 2020 [83]
- أوروبا: 26-27 نوفمبر 2020 [84]

3.3 الدروس المستفادة، والخطوات والإجراءات المستقبلية، والاستنتاجات

أصبحت الحاجة إلى حماية الأطفال على الإنترنت ماسة بشكل خاص خلال جائحة COVID-19.

ويمكن استخلاص عدد من الدروس من أنشطة الدول الأعضاء بشأن القضايا المتعلقة بحماية الأطفال على الإنترنت، مثل:

- ينبغي لكل بلد أن يقر بمسؤوليته عن ضمان أن تكون الإنترنت والتكنولوجيات المرتبطة بها آمنة للأطفال والشباب؛
- تعمل البلدان بشكل متزايد على دمج الوعي بالمخاطر على الخط في برنامج أوسع لحماية الأطفال وتربيتهم؛
- بينما تترسخ الفكرة القائلة بأن الإنترنت يمكن أن تكون أيضاً عاملاً إيجابياً في تعزيز المواطنة والتعلم، يبدو في كثير من الحالات أن نقص الموارد والخبرات المتاحة محلياً يعمل كعائق أمام التنمية؛
- في حين أن الأطر التشريعية في العديد من البلدان تتماشى على نطاق واسع مع الصكوك القانونية الدولية والإقليمية، فمن المهم للغاية لكل بلد أن يضمن أن تدابيره القانونية وإطاره التشريعي يتماشى مع التطورات التكنولوجية والتغيرات في السلوكيات؛
- جهات الاتصال الوطنية هي عنصر أساسي في الحماية الفعالة على الخط، ويجب أن يكون لدى جميع البلدان جهة اتصال وطنية مزودة جيداً بالموارد تشارك في المبادرات الإقليمية والدولية.[85]

وهناك أيضاً العديد من المجالات التي يمكن للدول الأعضاء فيها زيادة تسهيل أنشطة حماية الأطفال على الإنترنت، مثل:

- زيادة الوعي وتوفير التدريب على محو الأمية الرقمية لكل من المتخصصين المحترفين في الأمن السيبراني وللأطفال والآباء والمعلمين؛
- وضع القوانين واللوائح لحماية الأطفال على الإنترنت؛

---

78 الاتحاد الدولي للاتصالات. إصدارات إقليمية: المبادئ التوجيهية لحماية الأطفال على الإنترنت لعام 2020

79 قطاع تنمية الاتصالات. إصدار إقليمي للمبادئ التوجيهية لحماية الأطفال على الإنترنت لمنطقة إفريقيا. 30 أكتوبر 2020.

80 قطاع تنمية الاتصالات. المبادئ التوجيهية لحماية الأطفال على الإنترنت لمنطقة الأمريكتين. 19 أكتوبر 2020.

81 قطاع تنمية الاتصالات. حوار إقليمي على الإنترنت بشأن المبادئ التوجيهية لحماية الأطفال على الإنترنت لعام 2020 وفرص التنفيذ في المنطقة العربية. 23 نوفمبر 2020.

82 قطاع تنمية الاتصالات. المنتدى الإقليمي للتنمية لمنطقة آسيا والمحيط الهادئ (RDF ASP). جلسة المنتدى بشأن السلامة السيبرانية – إصدار المبادئ التوجيهية لحماية الأطفال على الإنترنت لعام 2020 لمنطقة آسيا والمحيط الهادئ. 3 نوفمبر 2020.

83 منتدى الاتحاد الدولي للاتصالات. معهد تكنولوجيا المعلومات في مجال التعليم التابع لليونيسكو بشأن حماية الأطفال على الإنترنت لمنطقة كومنولث الدول المستقلة. 27 أكتوبر 2020.

84 قطاع تنمية الاتصالات. منتدى الاتحاد لمنطقة أوروبا بشأن حماية الأطفال على الإنترنت. 26-27 نوفمبر 2020.

85 الوثيقة SG2RGQ/47 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من مسؤول الاتصال بمكتب تنمية الاتصالات المعني بالمسألة 3/2

- إجراء استقصاءات تمثيلية لتحسين مواءمة السياسات والمبادرات والإجراءات الحالية المتعلقة بحماية الأطفال على الإنترنت.

قد ترغب الجمعيات والمنظمات المجتمعية غير الربحية في اتخاذ خطوات لزيادة الوعي وتنمية المهارات بين الأطفال لمساعدتهم على استخدام الإنترنت بشكل أفضل في بيئة آمنة، مثل:

- الحد من درامية المنع التي قد تسهم في نشر ثقافة الخوف بين الآباء فيما يتعلق باستخدام أطفالهم للإنترنت، وبالتالي تجنب نهج يؤدي إلى زيادة القلق بين الآباء القلقين بطبعهم بشأن التكنولوجيا التي لا يفهمونها جيداً، وبالتالي تخريب أداة التعلم غير العادية، ألا وهي الإنترنت؛
- تشجيع البرامج التعليمية لتطوير أفضل الممارسات في إدارة المحتوى، وزيادة وعي الأطفال بكيفية استخدام الإنترنت بشكل مسؤول؛
- إنشاء بوابة على الإنترنت لتزويد الأطفال والمراهقين والآباء والمعلمين بقاعدة تعليمية؛
- إشراك جميع أصحاب المصلحة في أنشطة التوعية المجتمعية، بما في ذلك الوكالات الحكومية وقطاع الإنترنت الخاص والمنظمات غير الحكومية ومجموعات المجتمع وعامة الناس.[86]

ويمكن بشكل عام استنتاج ما يلي:

- يعتبر دور التعاون الدولي ودعم الدولة في ضمان الأمن السيبراني وحماية الأطفال على الإنترنت أمراً أساسياً؛
- ينبغي استخدام الأدوات السياساتية الوطنية لوضع استراتيجيات الأمن السيبراني في البلدان النامية؛
- تعد الشراكات بين القطاعين العام والخاص مهمة لزيادة فعالية الأدوات التنظيمية والتقنية للأمن السيبراني؛
- وصل عملية وضع آليات استراتيجية وتنظيمية جديدة لحماية الأطفال على الإنترنت، وتقييم الآليات القائمة، إلى ذروتها؛
- ينبغي إشراك المؤسسات التعليمية والشركات الخاصة في تنفيذ مشاريع لاستحداث أدوات تنظيمية وتقنية لحماية الأطفال على الإنترنت، بما في ذلك في إطار مبادرات الاتحاد الإقليمية؛
- يجب تطوير برامج وأدوات تعليمية لحماية الأطفال على الإنترنت تأخذ في الاعتبار احتياجات الأطفال ذوي الإعاقة؛
- ينبغي للدول الأعضاء أن تراجع التزاماتها بشأن الرقم القياسي العالمي للأمن السيبراني (GCI) وأن تشرع في اتخاذ مزيد من الإجراءات؛
- ينبغي أن تشارك المؤسسات التعليمية وكيانات القطاع الخاص والمنظمات غير الحكومية في أنشطة قطاع تنمية الاتصالات، بما في ذلك أعمال لجان دراسات الاتحاد ومراكز التميز التي تقدم دورات تدريبية في مجال الأمن السيبراني.

إذا ما تحتم تطوير حلول أكثر فعالية، فمن الأهمية بمكان أن يتم تبادل المعلومات بين جميع أصحاب المصلحة حول الأدوات المتاحة في مجال الأمن السيبراني وحماية الأطفال على الإنترنت، نظراً للأهمية المتزايدة لحماية الأطفال على الإنترنت في جميع أنحاء العالم والحاجة إلى بذل جهود تعاونية في هذا المجال، ولا سيما في إطار أنشطة قطاع تنمية الاتصالات.[87]

[86] الوثيقة 2/201 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من كوت ديفوار

[87] الوثيقة 2/75 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من أكاديمية A.S. Popov الوطنية للاتصالات في أوديسا (أوكرانيا)

الفصل 4 - تحديات الأمن السيبراني التي يواجهها الأشخاص ذوو الإعاقة

1.4 مقدمة

بالنسبة للمهاجمين السيبرانيين، لا يُعتبر أي شخص محصن. ولا ينبغي ترك الأشخاص ذوي الإعاقة يواجهون مخاطر سيبرانية أكبر لمجرد نقص المعلومات أو الوعي.

وخلال فترة الدراسة 2014-2017، أجرت لجنة الدراسات 2 لقطاع تنمية الاتصالات استقصاء بخصوص الوعي بالأمن السيبراني، ونشرت نتائجه في التقرير النهائي.[88] وأظهرت النتائج أن كبار السن والأشخاص ذوي الإعاقة هما المجموعتان الأقل استهدافاً من قبل حملات التوعية بالأمن السيبراني. بالإضافة إلى ذلك، فإن 69 في المائة من الدول الأعضاء المشاركة في الاستقصاء لم تدرج الأشخاص ذوي الإعاقة بين فئاتها المستهدفة فيما يتعلق بزيادة الوعي بالأمن السيبراني.

وتشير النتائج بوضوح إلى أنه يلزم القيام بالمزيد من العمل في هذا المجال. ولزيادة الوعي باحتياجات الأمن السيبراني المحددة لدى الأشخاص ذوي الإعاقة وأصحاب المصلحة الآخرين، بما في ذلك الحكومات والمنظمات الخاصة، استمرت المسألة 3/2 في دراسة الاعتبارات الأمنية المحددة ونقاط الضعف السيبرانية بناءً على حالات الاستعمال. وتُقدم في هذا الفصل حالات الاستعمال والدروس المستفادة والمعلومات المفيدة الأخرى.

2.4 حالات الاستعمال

1.2.4 مرسلو الرسائل الاقتحامية والمتصيدون الذين يستهدفون الأشخاص ذوي الإعاقة

نظرة عامة

أصبح مرسلو الرسائل الاقتحامية وخاطفو البريد الإلكتروني أكثر تعقيداً، حيث طوروا القدرة على تحديد ما إذا كان الهدف المحتمل لديه إعاقة واستخدام هذه الإعاقة لتكون هدفاً. ويواجه الأشخاص ذوو الإعاقة أيضاً تحديات في الحصول على المساعدة من إدارات الأمن والاحتيال لدى موردي خدمات البريد الإلكتروني الخاصة بهم.

ويتم استهداف الأشخاص ذوي الإعاقة من قبل مرسلي الرسائل الاقتحامية والمتصيدين، الذين يمثلون هدفاً باستخدام إعاقة الشخص كمعرف للهوية. وفي إحدى الحوادث، تم اختطاف حساب البريد الإلكتروني لشخص أصم يستخدم لغة الإشارة. وفي هذه الحادثة، كان للضحية حساب Gmail، لكن ربما كان الحساب يخص أي مورد حساب بريد إلكتروني. ولسوء الحظ، لم يقدم مكتب مساعدة Gmail إلا القليل من الدعم. وبمجرد نقر الضحية على رابط التصيد الاحتيالي واختراق حسابه، تمكن مرسل الرسائل الاقتحامية من النفاذ إلى دفتر عناوين الضحية، وربما إلى ملفات أخرى على جهاز حاسوب الضحية.

وأخبر مكتب المساعدة الضحية أن الحل الوحيد هو تغيير مورد البريد الإلكتروني الخاص به وعنوان بريده الإلكتروني. وفي حين أن الإعاقة في هذا المثال كانت الصمم، فليس من المستبعد أن يتم استخدام أي إعاقة بهذا الشكل من سرقة الهوية.

ومن المهم أن يدرك مستعملو البريد الإلكتروني، بمن فيهم المستعملون ذوو الإعاقة، أهمية التحقق من جميع الروابط المرسلة إليهم، حتى من الأصدقاء، قبل النقر على الرابط. ويتعين على مكاتب مساعدة موردي خدمات البريد الإلكتروني أيضاً الاهتمام بشكل فعال بهذا النوع من إساءة الاستخدام، خاصةً عندما يتم استهداف المجتمعات الضعيفة. وفي هذه الحادثة، اتصل الضحية برقم هاتف مكتب المساعدة عبر صديق أو خدمة ترحيل هاتف للصم؛ وينبغي أن يتعامل موردو الخدمات مع مثل هذه المكالمات بجدية أكبر أو ينبغي أن يوفروا رقم هاتف خاصاً يديره شخص ما بحيث يمكن للمستعملين الصم الاتصال به مباشرة باستخدام آلة الطباعة عن بُعد. والأفضل من ذلك، ينبغي لموردي الخدمات تعيين موظفين في مكتب المساعدة يجيدون لغة الإشارة. وفي الولايات المتحدة، اتخذت شركة أمازون خطوات لتقديم هذه الخدمة، على سبيل المثال.

[88] الاتحاد الدولي للاتصالات. التقرير النهائي للمسألة 3/2 التابعة للجنة الدراسات 2 لقطاع تنمية الاتصالات لفترة الدراسة 2014-2017. تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني. الاتحاد الدولي للاتصالات، 2017.

أمثلة عن البريد الإلكتروني

فيما يلي مثالان على نوع البريد الإلكتروني الذي أرسله مرسل الرسائل الاقتحامية في المثال أعلاه إلى قائمة جهات اتصال الضحية. ونتيجة لذلك، قام الضحية بتغيير مورد خدمة البريد الإلكتروني الخاص به بعد إبلاغ جهات اتصاله بأنه قد تعرض للقرصنة.

المثال 1: يتظاهر مرسل الرسائل الاقتحامية بأنه الشخص ذو الإعاقة.

من: Person with disability personwithdisability@gmail.com
تاريخ الإرسال: 23 مارس 2018 الساعة 13:00
الموضوع: **رائع!! البلد X يزيد العلاوة الشهرية للصم** بنسبة 70 في المائة

رائع! فكر البلد X في جميع الأشخاص الصم وضعاف السمع وقرر قائد البلد X زيادة إعانات الإدارات SSA وSSI وSSDI بنسبة 70 في المائة وهذه أخبار جيدة لجميع الصم وضعاف السمع في البلد X

ولقراءة المزيد ومعرفة مقدار الزيادة التي ستحصل عليها من إعانات الإدارات SSA وSSI وSSDI،

انقر هنا http://noisecancel.net/js/ggg/G/G/us/index.php

[ملاحظة: تم تغيير رابط الاحتيال الأصلي.]

مع تسجيل الدخول باستخدام حساب بريدك الإلكتروني وتأكد من صحة جميع البيانات

أخبار الصم

المثال 2: من الضحية لإبلاغ جهات اتصاله بأنه قد تعرض للقرصنة.

مرحبا بالجميع!

كما قلت سابقاً، نتيجة لإغرائي لمشاهدة مقطع فيديو بلغة ASL قبل ثلاثة أسابيع، تم اختراق حساب gmail الخاص بي!

[ملاحظة: ASL تعني لغة الإشارة الأمريكية.]

يواصل القرصان إرسال رسائل بريد إلكتروني **مزيفة** باستخدام حساب Gmail الخاص بي. والأمر المخيف هو أن المحتويات تبدو واقعية ومرتبطة بأنشطتي المتعلقة بالصم.

وبعد ساعات من المرور عبر شبكة Google الروبوتية، وجدت رقم هاتف، 836-3987 (855)، للوصول إلى إنسان.

خمن ماذا حدث؟ بدلاً من محاولة مساعدتي، قالوا "سيئ للغاية".

هل حساب Gmail الخاص بك آمن؟

والآن، أرجو حذف **أي** رسائل بريد إلكتروني.

<from personwithdisability@gmail.com>

عذراً

Person with disability

الدروس المستفادة وأفضل الممارسات المقترحة

- ينبغي تثقيف مجتمع ذوي الإعاقة بمشكلات الرسائل الاقتحامية والبرمجيات الضارة المعروفة.
- ينبغي لموردي الخدمات توفير موظفين مدربين للتعامل مع استفسارات العملاء من مجتمع ذوي الإعاقة.
- ينبغي ألا يقوم مستعملو البريد الإلكتروني بالنقر على أي عناوين ويب ما لم يتم التحقق من المصدر.
- ينبغي لضحايا اختطاف البريد الإلكتروني:
  - إخطار مورد خدمة البريد الإلكتروني الخاص بهم؛
  - إعادة توجيه البريد الإلكتروني المشبوه إلى قسم الاحتيال لدى مورد خدمة البريد الإلكتروني؛
  - طلب حجب عنوان البريد الإلكتروني المختطف؛
  - تغيير عنوان البريد الالكتروني؛
  - إبلاغ جميع جهات الاتصال بأن عنوان البريد الإلكتروني قد تم اختطافه وتزويدهم بالعنوان الجديد.

2.2.4 المخاطر السيبرانية المرتبطة بالتكنولوجيات المساعدة الممكنة بإنترنت الأشياء

خلفية

وفقاً لمنظمة الصحة العالمية (WHO)، يعاني أكثر من مليارى شخص من شكل ما من أشكال الإعاقة، وهو ما يمثل 37,5 في المائة من سكان العالم.[89] كما تلاحظ إدارة الشؤون الاقتصادية والاجتماعية بالأمم المتحدة، أن البلدان لا تشترك في تعريف موحد بشأن "الأشخاص ذوي الإعاقة"، وبالتالي اعتمدت تصنيفات وعتبات مختلفة.[90] وطبقاً لتعريف منظمة الصحة العالمية المعتمد دولياً، فإن الشخص ذا الإعاقة هو أي شخص لديه مشكلة في وظيفة من وظائف الجسم أو هيكله، أو وجود قيود على النشاط، أو صعوبة في تنفيذ مهمة أو عمل ما.[91]

وكما يوحي هذا التعريف، هناك أنواع عديدة من الإعاقات. وتمثل كل إعاقة حاجزاً يؤثر على حياة هؤلاء الأشخاص. ومع ذلك، تقوم التكنولوجيا بدور مهم في كسر هذه الحواجز ومساعدة الأشخاص ذوي الإعاقة على التمتع بظروف معيشية أفضل.

وفي الوقت الحاضر، تنتشر التكنولوجيا على نطاق واسع، وتؤثر على الحياة اليومية لكل من لأفراد والمجتمع ككل. وعلى مدى العقد الماضي، أثبتت إنترنت الأشياء إمكانية تغيير حياة الأشخاص ذوي الإعاقة إلى الأفضل.[92] لذلك تُستخدم التكنولوجيا المساعدة الممكنة بإنترنت الأشياء بشكل متزايد للتغلب على القيود الناشئة عن الإعاقات.[93]

وتحدد اتفاقية حقوق الأشخاص ذوي الإعاقة تكنولوجيا المعلومات والاتصالات كعنصر أساسي لمساعدة الأشخاص ذوي الإعاقة. وتؤكد المادة 9، على وجه الخصوص، المتعلقة بإمكانية النفاذ، على دور تكنولوجيا المعلومات والاتصالات في تعزيز الاستقلال والمشاركة الكاملة للأشخاص ذوي الإعاقة في مختلف المجالات، وتفوض الدول الأطراف ببذل جهود مشتركة واعية لتعزيز النفاذ إلى تكنولوجيا المعلومات والاتصالات.[94]

وتعمل كل من تكنولوجيا المعلومات والاتصالات وإنترنت الأشياء على زيادة السلامة والتنقل والاستقلالية؛ من الأطراف الصناعية الموصولة بالإنترنت إلى الأحذية الذكية التي تهتز لتوجيه مرتديها، تم تصميم العديد من أجهزة وخدمات إنترنت الأشياء لتحسين ظروف المعيشة وتقليل اعتماد الأشخاص ذوي الإعاقة على الآخرين.[95] فعلى سبيل المثال، يمكن للأفراد المكفوفين أو الذين يعانون من إعاقة بصرية استخدام التكنولوجيا لمساعدتهم على التنقل في محيطهم والنفاذ إلى المعلومات المكتوبة. وعلاوةً على ذلك، تسمح تكنولوجيات المنازل الذكية للأفراد

---

89 منظمة الصحة العالمية، التقرير العالمي حول الإعاقة لعام 2011. منظمة الصحة العالمية، 2011.

90 إدارة الشؤون الاقتصادية والاجتماعية بالأمم المتحدة (UNDESA). تقرير الإعاقة والتنمية: تحقيق أهداف التنمية المستدامة من قبل الأشخاص ذوي الإعاقة ومن أجلهم وبالتعاون معهم. الأمم المتحدة، نيويورك، 2018.

91 منظمة الصحة العالمية. المرجع السابق، الفصل 1.

92 منتدى مستقبل الخصوصية، إنترنت الأشياء (IoT) والأشخاص ذوي الإعاقة: استكشاف الفوائد والتحديات وضغوط الخصوصية. يناير 2019.

93 منظمة الصحة العالمية. موضوعات صحية. التكنولوجيا المساعدة.

94 إدارة الشؤون الاقتصادية والاجتماعية بالأمم المتحدة. اتفاقية الأمم المتحدة بشأن حقوق الأشخاص ذوي الإعاقة (CPRD). المادة 9 – إمكانية النفاذ.

95 منتدى مستقبل الخصوصية. المرجع السابق.

بالتحكم في الأجهزة والأشياء الأخرى الموجودة في منازلهم والتي قد يصعب الوصول إليها، مثل مفاتيح الإضاءة وأقفال الأبواب وأنظمة الأمن.

التكنولوجيا: سيف ذو حدين

برغم توفير العديد من الفوائد، تعمل التكنولوجيات المساعدة الممكنة بإنترنت الأشياء أيضاً على زيادة تعرض المستعملين للمخاطر السيبرانية بشكل كبير. ونظراً للاعتماد المتزايد على التكنولوجيات المساعدة، فإن أي تعطيل أو تعديل في هذه التكنولوجيات يمكن أن يؤدي إلى زيادة مواطن الضعف.

وغالباً ما تتميز أجهزة وخدمات إنترنت الأشياء بمستويات أمان أقل من المستوى الأمثل. فعلى سبيل المثال، قد لا تستخدم التجفير المناسب لنقل البيانات، مما قد يؤدي إلى الكشف غير المناسب عن البيانات وتسربها. وبالنسبة للأشخاص ذوي الإعاقة، على وجه الخصوص، قد تكون البيانات الشخصية ذات طبيعة حساسة، حيث يمكن أن تكشف عن تفاصيل الظروف الطبية للفرد.

ونظراً لأهمية التكنولوجيات المساعدة للأشخاص ذوي الإعاقة، يمكن أن يكون التأثير السلبي للمخاطر السيبرانية كارثياً. فعلى سبيل المثال، يعتمد بعض الأشخاص ذوي الإعاقات الجسدية على الأطراف الاصطناعية الميكانيكية الحيوية لاستعادة الحركة الكاملة أو الجزئية. وتستخدم هذه الأطراف الاصطناعية أجهزة استشعار محددة لقراءة وتحليل معاملات تقلص العضلات من أجل إعادة إنتاج الحركات من خلال الأجهزة (مثل تحريك أصابع الذراع الاصطناعية). وترسل الأطراف الاصطناعية البيانات بشكل روتيني إلى الحيز السحابي للإبلاغ بتحليلها الحسابي وتحسين فعاليتها. وتؤدي هذه التوصيلية إلى أن تكون هذه الأجهزة عرضة للهجمات التي تهدف إلى النفاذ إلى البيانات الموجودة في الحيز السحابي أو معالجتها أو حذفها أو النفاذ إلى البيانات الشخصية للمستعملين. وعلاوةً على ذلك، يمكن للمهاجمين السيطرة على الأطراف الاصطناعية عن بُعد. وإذا تم توصيل الطرف الاصطناعي بمغروسة دماغية، فقد تكون العواقب أسوأ.[96]

وكمثال آخر، يعتمد بعض الأشخاص الذين يعانون من إعاقات سمعية على مغروسات قوقعة الأذن، والتي تعتبر أكثر توغلاً من مساعدات السمع العادية. وتعتمد هذه التقنية على ثلاثة مكونات أساسية، وهي ميكروفون ومعالج كلام ومحفز مستقبل مغروس. وتتّحب بعض مغروسات قوقعة الأذن الحديثة بأجهزة تحكم عن بُعد تمكن المستعملين من التحكم في إعدادات المغروسة عبر تطبيق متنقل. وعلى المستوى الأساسي، يمكن للمهاجمين محاولة إيقاف تشغيل المغروسة، مما يصيب الضحية بالصمم. ويمكن للهجمات الأكثر تعقيدًا أن تمنع معالج الكلام من تلقي المدخلات من الميكروفون أو تغيير جهاز الاستقبال لنقل الأصوات التي ينتجها المهاجم. وقد يكون من الصعب اكتشاف هذه الهجمات الأكثر تعقيداً، خاصةً عندما لا يكون لدى مستخدمي مغروسات قوقعة الأذن طريقة أخرى للتحقق مما يسمعونه.

بالإضافة إلى الهجمات المصممة للتكنولوجيات المساعدة، يمكن للمهاجمين أيضاً استهداف التكنولوجيات التي يشيع استخدامها من قبل الأشخاص ذوي الإعاقة. فعلى سبيل المثال، قد يفقد الأشخاص ضعاف البصر جميع وسائل الملاحة الموثوقة إذا كانت أدوات النظام العالمي لتحديد الموقع (GPS) التي يستخدمونها معيبة أو تم اختراقها عن عمد من قبل المهاجمين. ففي هجمات انتحال النظام GPS، يُستخدم جهاز إرسال راديوي يقع بالقرب من الهدف للتداخل مع إشارة النظام GPS الحقيقية.[97] ويمكن للمهاجم بعد ذلك إرسال إحداثيات غير دقيقة أو قطع إرسال البيانات، مما قد يؤدي إلى ضرر مادي وعواقب خطيرة أخرى.

وبالرغم من أن هذه ليست سوى أمثلة قليلة للهجمات السيبرانية المحتملة التي تستهدف التكنولوجيات المساعدة الرقمية، فإنها تسلط الضوء على أهمية الأمن السيبراني في ضمان سلامة الأشخاص ذوي الإعاقة الذين يعتمدون على هذه التكنولوجيات.

الخطوات المقبلة للنظر فيها

يمكن للإنترنت وإنترنت الأشياء تسهيل المشاركة الاجتماعية والاقتصادية والمدنية للأشخاص ذوي الإعاقة. فبالرغم من أن إمكانات هاتين التكنولوجيتين واضحة، يلزم بذل جهود مستمرة لمواءمة العوامل المجتمعية والتشريعية والشخصية والعوامل المتعلقة بالبنية التحتية داخل النظام الإيكولوجي لإنترنت الأشياء بطريقة

[96] Vladimir Dashchenko، كيف تهاجم الذراع الاصطناعية وتدافع عنها. Securelist (Kaspersky)، 26 فبراير 2019.
[97] Maria Korolov، ماذا يعني انتحال النظام العالمي لتحديد الموقع (GPS) وكيف يمكنك الدفاع ضده. موقع *CSO* على الويب، فريق البيانات الدولية (IDG)، 7 مايو 2019.

تعطي الأولوية لأمن أجهزة إنترنت الأشياء. وهناك إجراءات ملموسة يمكن أن تتخذها الحكومات لتحسين أمن التكنولوجيات المساعدة، ومن ثم اعتماديتها.

يمكن للحكومات اتخاذ خطوات لتحسين التشريعات والسياسات المتعلقة بإمكانية النفاذ إلى إنترنت الأشياء وأمنها، وتطوير آليات لتعزيز وإنفاذ تطبيقها. ويجب أن تبدأ هذه الأطر بتقييم احتياجات الأشخاص ذوي الإعاقة وينبغي أن تحدد الأدوار والمسؤوليات بوضوح. ونظراً لأنه من المحتمل أن يشمل الموضوع ممثلين من مجموعة متنوعة من المجالات الحكومية (مثل التكنولوجيا والاتصالات والرفاهية والطب)، فإن التعاون أمر أساسي ويجب تعزيزه في كل مبادرة.

يمكن طرح مبادرات محددة. فعلى سبيل المثال، يمكن للحكومات وضع خطط اعتماد الأمن السيبراني للتكنولوجيات المساعدة، والتي يمكن أن تشمل فحوصات واختبارات أمنية دورية والالتزام بإجراء تحديثات منتظمة للنظام للتكيف مع التطورات التكنولوجية. كما يمكن للحكومات أن تدعم المصنّعين من خلال تقديم الحوافز، وتعزيز الشراكات بين القطاعين العام والخاص، وتقديم التمويل الأولي ومنح البحث والتطوير.

وبالمثل، هناك حاجة للترويج لثقافة أمنية تستجيب للمخاطر التي تنطوي عليها هذه التكنولوجيات. وينبغي للحكومات أن تعمل مع القطاع الخاص لإجراء حملات توعية سيبرانية بين السكان.

وفي الختام، بالرغم من أن التكنولوجيا المساعدة الممكنة بإنترنت الأشياء هي عنصر أساسي في دعم الأشخاص ذوي الإعاقة، فإنها يمكن أن تشكل أيضاً عدداً من المخاطر التي، إذا لم تُعالج بشكل صحيح، يمكن أن يكون لها عواقب وخيمة. لذلك ينبغي أن تلبي التكنولوجيات المساعدة أعلى معايير الأمن وينبغي أن تستجيب للتطورات التكنولوجية.

الدروس المستفادة وأفضل الممارسات المقترحة

كما هو موضح أعلاه، ينبغي تنفيذ تدابير الأمن السيبراني للأشخاص ذوي الإعاقة، خاصة أولئك الذين يعانون من صعوبات في السمع، مثل خدمات ترحيل الاتصالات والعرض النصي عن بُعد، من أجل تعزيز إمكانية الوصول إلى خدمات المعلومات والاتصالات.

3.2.4 النظر في القضايا الأمنية لخدمات إمكانية النفاذ إلى تكنولوجيا المعلومات والاتصالات

مقدمة

خدمات إمكانية النفاذ إلى تكنولوجيا المعلومات والاتصالات، مثل خدمات ترحيل الاتصالات والعرض النصي عن بُعد، تمكّن الأشخاص ذوي الإعاقة من التواصل والنفاذ إلى المعلومات. وتتطلب هذه الخدمات بطبيعة الحال اتخاذ تدابير أمنية لحماية سلامة وخصوصية الأشخاص ذوي الإعاقة والتخفيف من الضعف السيبراني لهذه المجموعات وغيرها من المجموعات ذات الاحتياجات المحددة، مثل الأطفال وكبار السن.

الجوانب الأمنية للعرض النصي عن بُعد

العرض النصي عن بُعد خدمة يتم فيها نسخ الكلمات المنطوقة في اجتماع أو مؤتمر في موقع مختلف عن الموقع الذي تم فيه الاجتماع.[98] وتُستخدم خدمات تكنولوجيا المعلومات والاتصالات، مثل الهواتف أو الهواتف الخلوية أو ميكروفونات الحواسيب، لإرسال صوت المتحدث إلى الشخص القائم بالعرض النصي الذي يقوم بنسخ الصوت إلى نص. ثم يتم إرسال النص المكتوب في الوقت الفعلي إلى مكان الاجتماع، حيث يمكن قراءة النص. وغالباً ما يتم عرض النص المنسوخ عن بُعد على شاشة عامة أو شاشة عرض في غرفة الاجتماعات أو على شاشة عرض شخصية. ولا تعد خدمات العرض النصي عن بُعد ضرورية فقط من أجل تمكين الأشخاص الصم أو ضعاف السمع من المشاركة في الاجتماعات، ولكنها مفيدة أيضاً للأفراد الذين تختلف لغتهم الأولى عن تلك المستخدمة في الاجتماع أو في المواقف التي يشارك فيها المتحدثون بأصوات ولهجات مختلفة في مجموعات مختلفة (على سبيل المثال في العمل أو في الفصل الدراسي أو في القاعات المجتمعية). ويجب أن يكون الشخص الذي يقدم النسخ المكتوبة لخدمة العرض النصي عن بُعد، والذي يُطلق عليه اسم "المُعلق"، مؤهلاً كمُراسل حرفي. وغالبًا ما يُعرف المعلق أيضاً باسم "محرر الكلام إلى نص".

[98] قطاع تقييس الاتصالات في الاتحاد (ITU-T)، الورقة التقنية FSTP-ACC-RCS، "نظرة عامة على خدمات العرض النصي عن بُعد"، 17 أكتوبر 2019.

وخدمات العرض النصي عن بُعد مطلوبة بموجب قوانين الممارسة الوطنية أو المحلية المختلفة. ويجب على المورد اتخاذ جميع التدابير الاحترازية المعقولة لتأمين خصوصية الاجتماع، حيث قد تكون هناك معلومات سرية.

أنواع المعلومات السرية

فيما يلي قائمة غير حصرية بالمعلومات التي يُحتمل أن تكون سرية:

- المعلومات الحساسة التي تناقش في الاجتماعات و/أو المؤتمرات
- المعلومات الطبية للمرضى
- المعلومات القانونية المتعلقة بالأفراد
- جلسات الاستشارة
- معلومات عن الامتثال للوائح حماية البيانات.

يجب على موردي خدمة العرض النصي عن بُعد اتباع قوانين ولوائح حماية البيانات والخصوصية المعمول بها، مثل تلك المنصوص عليها في الاتحاد الأوروبي.[99]

تجفير محتوى العرض النصي

ينبغي أن يكون النص الذي يتم بثه إلى شاشة عرض أو جهاز مطرافي شخصي محمياً بكلمة مرور. ويعتبر مورد خدمة العرض النصي عن بُعد مسؤولاً عن أمن النص ويجب عليه اتباع متطلبات حماية البيانات ذات الصلة. ويوصى بتجفير النص والعنوان URL لمصدر النص، إن أمكن، باستخدام بروتوكول طبقة المقابس المؤمنة أو أي تكنولوجيا أخرى ذات صلة.

تجفير الصوت

تجب حماية البيانات الصوتية الأصلية المستمدة من الحدث بشكل آمن.

الاعتبارات الأمنية لخدمات ترحيل الاتصالات

التكافؤ الوظيفي

يُعرَّف التكافؤ الوظيفي بأنه *"القدرة التي يستطيع بها الأشخاص الذين لديهم مجموعة مختلفة من القدرات (خاصة الأشخاص ذوي الإعاقة والأشخاص ذوي الاحتياجات المحددة) استخدام خدمة أو نظام اتصالات بمستوى من الوظائف وسهولة الاستخدام المعروضة تشابه تلك المعروضة لمجموعة أوسع من المستعملين في مجتمع ما [...] ويشمل ذلك الاعتبارات التقنية والاقتصادية على حد سواء مع عدم فرض أي تمييز مالي على مستعملي خدمة الترحيل."*[100]

ويشمل التكافؤ الوظيفي الالتزامات الأمنية المطبقة على موردي خدمات الاتصالات في أي ولاية قضائية معينة. ويعني التكافؤ الوظيفي أن مستعملي خدمات الترحيل يجب أن يكونوا على قدم المساواة مع المستعملين الآخرين في المجتمع، لا سيما فيما يتعلق بأنواع المكالمات التي تسمح بها خدمات الترحيل، والتي قد يكون لها تداعيات بالنسبة للأمن.

المتطلبات الأمنية للتكافؤ الوظيفي

لتحقيق التكافؤ الوظيفي، يجب ضمان سرية وخصوصية وأمن خدمات الترحيل الهاتفية والتكنولوجيات المستخدمة من قبل هذه الخدمات ومساعدي الاتصالات من البشر الذين يعملون عليها.

ويجب أن تكون متطلبات خدمات الترحيل الهاتفية فيما يتعلق بالسرية وأمن المكالمات، بما في ذلك التجفير، متوافقة مع تلك المطبقة على خدمات الاتصالات العامة في البلد المعني أو المنطقة المعنية.

---

[99] الاتحاد الأوروبي. اللائحة 679/2016 (EU) الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات والتي تلغي التوجيه 95/46/EC (لائحة حماية البيانات العامة).

[100] قطاع تقييس الاتصالات في الاتحاد، التوصية ITU-T F.930 خدمات ترحيل الاتصالات متعددة الوسائط.

اعتبارات الضعف السيبراني للأشخاص ذوي الاحتياجات المحددة

يعد ضمان الاستخدام المؤمن للإنترنت أمراً مهماً بشكل خاص للأشخاص ذوي الإعاقة وللمجموعات ذات الاحتياجات المحددة، مثل كبار السن والأطفال. ويعد الحد من الضعف السيبراني لهذه المجموعات قضية ملحة وهامة، وتتطلب وضع مبادئ توجيهية والالتزام بتطبيقها.

3.4 معلومات مفيدة

المسألة 7/1 التابعة للجنة الدراسات 1 لقطاع تنمية الاتصالات مسؤولة عن دراسة "نفاذ الأشخاص ذوي الإعاقة وذوي الاحتياجات المحددة إلى خدمات الاتصالات/تكنولوجيا المعلومات والاتصالات" وتناقش موضوعات مختلفة في هذا المجال.[101]

وينشر منتدى مستقبل الخصوصية تقريراً بعنوان "إنترنت الأشياء (IoT) والأشخاص ذوو الإعاقة: استكشاف الفوائد والتحديات وضغوط الخصوصية".[102]

ويمكن الاطلاع على مزيد من المعلومات من هذين المصدرين.

[101] لجنة الدراسات 1 لقطاع تنمية الاتصالات. المسألة 7/1.
[102] منتدى مستقبل الخصوصية. المرجع السابق.

الفصل 5 - حالة تحديات الأمن السيبراني، بما فيها التحديات التي تواجه التكنولوجيات الناشئة مثل إنترنت الأشياء والحوسبة السحابية

1.5 مقدمة

أدى النمو الهائل في القدرات التكنولوجية إلى عالم يتزايد فيه الطابع الرقمي يتسم بالتوصيل والتوصيل البيني. ووفقاً للمنتدى الاقتصادي العالمي، بدأت بالفعل فترة تُعرف باسم "العولمة 4.0"، حيث تشكل الأصول والخدمات الرقمية العمود الفقري للاقتصاد والصادرات.[103]

ويعمل الابتكار على تغيير المشهد التكنولوجي لتلبية الاحتياجات التجارية والعملية الجديدة. وقد أصبحت أجهزة إنترنت الأشياء، جنباً إلى جنب مع تكنولوجيا الجيل الخامس، منتشرة بشكل متزايد، مع ما يقدر بنحو 41,6 مليار جهاز موصول حول العالم بحلول عام 2025.[104] وأصبحت الحلول السحابية بالغة الأهمية للعمليات، مع اعتماد 94 في المائة من الشركات في جميع أنحاء العالم عليها.[105] ونظراً للزيادة في توفر البيانات ودقتها، يواصل الذكاء الاصطناعي أيضاً استنباط تطبيقات أوسع.

بيد أن ظهور تكنولوجيات جديدة يفرز الحاجة المتزايدة للأمن السيبراني. ولقد أدخل الابتكار الرقمي المزيد من المنتجات، فضلاً عن مزيد من التعقيد، مما زاد من احتمالية مواطن التعرض والضعف التي يمكن استغلالها.

وتتزايد التهديدات السيبرانية باستمرار. ففي عام 2018، كان هناك 80 000 هجمة سيبرانية يومياً، وهو ما يمثل أكثر من 30 مليون هجمة سنوياً.[106] وفي عام 2019، تم تسجيل أكثر من 90 مليار محاولة يومياً لاختراق معلومات حساسة.[107] كما ازدادت التهديدات السيبرانية تعقيداً، مما يهدد العالم والاقتصاد اللذين تم تمكينهما رقمياً بالكامل، بما في ذلك الأنظمة المادية السيبرانية في المنازل والمدن الذكية والمركبات وأنظمة الإنتاج والبنية التحتية الحرجة. وأثبت الخبراء أن من الممكن حتى قرصنة الأجهزة الطبية المغروسة في جسم الانسان، مثل أجهزة تنظيم ضربات القلب ومضخات الأنسولين.[108]

وترجع هذه الزيادة في الهجمات أيضاً إلى انتشار القرصنة كخدمة، عبر شبكة الويب الخفية، بسعر مناسب غالباً. ويتم تسويق الجريمة السيبرانية تجارياً بشكل متزايد وتحولت إلى قطاع كبير، حيث يبيع فيه القراصنة مجموعة واسعة من الأدوات والخدمات الضارة، بدءاً من سرقة كلمات المرور الضعيفة إلى مجموعات الاستغلال وتكنولوجيات الهجوم شديدة التعقيد، مثل رفض الخدمة الموزع والبرمجيات الضارة وبرمجيات طلب الفدية وبرمجيات التجسس.[109] علاوةً على ذلك، يمكن استخدام التكنولوجيات الناشئة، التي تُستخدم غالبًا لتحسين حلول الدفاع السيبراني، بشكل ضار لزيادة كفاءة أدوات القرصنة ومدى وصولها.[110] ويُستخدم الذكاء الاصطناعي والبرمجيات الروبوتية المؤتمتة وإنترنت الأشياء والحلول السحابية بشكل متزايد في الهجمات السيبرانية واسعة النطاق، وقد أدى الجمع بين تقنيات القرصنة الجديدة - مثل أدوات التصيد الآلي - مع التكنولوجيات الناشئة إلى توسيع نطاق المخاطر السيبرانية.

---

103 Klaus Schwab. العولمة 4.0 – ما المقصود بها؟ *المنتدى الاقتصادي العالمي*، 5 نوفمبر 2018.

104 شركة Business Wire. من المتوقع أن يولد النمو في أجهزة إنترنت الأشياء الموصولة 79,4 ZB من البيانات في عام 2025، طبقاً للتوقعات الجديدة لشركة IDC، 18 يونيو 2019.

105 Kim Weins. اتجاهات الحوسبة السحابية: تقرير حالة الحوسبة السحابية لعام 2019. مدونة *Flexera Blog*، 21 مايو 2020.

106 شركة PurpleSec. اتجاهات وبيانات إحصاءات الأمن السيبراني لعام 2019: القائمة النهائية لإحصاءات الأمن السيبراني. (مدونة *شركة PurpleSec*، تم الدخول إليها في 27 أبريل 2020.

107 شركة Check Point. الاستعداد لحرب سيبرانية باردة جديدة في 2020، إنذار لشركة Check Point. نشرة صحفية، 24 أكتوبر 2019.

108 Lily Hay Newman. ابتكر هؤلاء القراصنة تطبيقاً يقتل لإثبات نظرية ما. مجلة *Wired*، 16 يوليو 2019؛ وDan Gooding. يؤدي اختراق مضخة الأنسولين إلى إعطاء جرعة قاتلة عبر الموجات الراديوية. *The Register*، 27 أكتوبر 2011.

109 Armor. تقرير عن السوق الخفية: الاقتصاد الجديد، 28 سبتمبر 2020.

110 Deloitte، الحماية من عالم مخاطر الأمن السيبراني المتغير: مستقبل المخاطر في العصر الرقمي. Deloitte & Touche LLC، 2019.

يتمثل أحد التحديات الرئيسية للأمن السيبراني في النقص العام في المهارات المهنية ونقص وعي الموظفين. ومع زيادة تعقيد التهديدات السيبرانية، تسعى المنظمات لتوظيف خبراء مهرة في مجال الأمن السيبراني قادرين على حماية أنظمتها.[111] ففي عام 2017، أفاد 82 في المائة من أرباب العمل أن موظفيهم لا يتمتعون بمهارات كافية في مجال الأمن السيبراني. وبحلول عام 2021، ستكون هناك 4 مليون وظيفة مهنية في مجال الأمن السيبراني شاغرة.[112] علاوةً على ذلك، يُظهر الموظفون العموميون القليل من الوعي بالتهديدات السيبرانية. وللعامل البشري دور رئيسي في الأمن السيبراني وقد ثبت أنه يمثل جانباً كبيراً. وفي عام 2018، توصلت إحدى الدراسات إلى أن 99 في المائة من الحوادث الرقمية تم البدء فيها عن غير قصد من قبل موظفين وقعوا ضحية للهندسة الاجتماعية، في حين أن 1 في المائة فقط من الحوادث نتجت حصرياً عن الفشل التكنولوجي أو عمليات الاستغلال.[113]

يعد الأمن السيبراني مجالاً دينامياً، ويجب على المؤسسات إعادة النظر باستمرار في وضعها بالنسبة للأمن السيبراني للدفاع ضد التهديدات الناشئة. ومن أجل تهيئة بيئة أكثر أمناً، من المهم إشراك أصحاب المصلحة في حوار حول الأمن السيبراني وإدارة مخاطر الخصوصية؛ والتحقق من عمليات إدارة مخاطر الخصوصية والأمن السيبراني الحالية واستكمالها وتمحيصها؛ وتحديد اعتبارات الأمن السيبراني والخصوصية الرئيسية التي قد تتعلق تحديداً بحلول وبيئات تكنولوجية معينة. ويناقش هذا الفصل العديد من تهديدات الأمن السيبراني المرتبطة بالتكنولوجيات الناشئة، بما في ذلك إنترنت الأشياء، والحوسبة السحابية، وتكنولوجيا الجيل الخامس، والذكاء الاصطناعي، والثورة الصناعية الرابعة (المعروفة باسم "الصناعة 4.0"). كما يفرد الاتجاهات والتحديات الحالية والحلول المحتملة لمواجهة التهديدات التي يمكن أن تجور على المكاسب التي تحققت من خلال الابتكار الرقمي.

2.5 التهديدات والأطراف الفاعلة والدوافع فيما يتعلق بالأمن السيبراني

الهدف من التهديدات السيبرانية هو تقويض الأهداف التقليدية الثلاثة للأمن السيبراني، وهي السرية والسلامة والتيسر. وتحمي السرية المعلومات ضد الجميع باستثناء المصرح لهم بالنفاذ إليها. وتضمن السلامة دقة المعلومات وموثوقيتها وتمنع التعديلات غير المصرح بها للبيانات. ويشير التيسر إلى القدرة على النفاذ إلى البيانات والمعلومات عند الحاجة.

وعالم التهديدات السيبرانية عبارة عن بيئة غير متجانسة تسكنها جهات فاعلة مختلفة تسعى لتحقيق أهداف مختلفة ولديها قدرات مختلفة. وبشكل عام، يمكن تصنيف الجهات الفاعلة ذات الأغراض الخبيثة على النحو التالي:

- ***العاملون الداخليون:*** وفقاً للتقارير الأخيرة، فإن حوالي 40 في المائة من الحوادث يرتكبها موظفون داخليون، غالباً ما يكونون موظفين ساخطين يسعون إلى الانتقام من أرباب أعمالهم.[114] وقد يكون العاملون الداخليون خطرين بشكل خاص لأنهم يتمتعون بالنفاذ المباشر إلى البيانات والمعلومات والأصول الرقمية.
- ***القراصنة:*** هم أفراد تحركهم دوافع سياسية واجتماعية. وهم يسرقون عادةً المعلومات الحساسة وينشرونها بهدف إحراج القادة السياسيين أو المشاهير، ويكشفون عن بيانات الملكية والسرية بذريعة حرية التعبير. وغالباً ما يشوهون مواقع الويب ويقومون بهجمات رفض الخدمة الموزع ضد خدمات أو مواقع ويب معينة.[115]
- ***المجرمون السيبرانيون:*** هؤلاء مجرمون بدافع الكسب المالي. وهم يستهدفون المعلومات المتعلقة بالأفراد والشركات والمؤسسات بهدف تسييلها. وعادة ما يبتزون الأهداف ويسرقون ويبيعون البيانات وحقوق الملكية الفكرية في السوق السوداء وينفذون هجمات برمجيات طلب الفدية. وكما نوقش أعلاه، تطورت الجريمة السيبرانية لتصبح خدمة تبيع فيها مجموعات مختلفة سلعاً وخدمات إجرامية، بدءاً من عمليات استغلال النظام إلى دورات حياة الهجمات الكاملة.

---

111 William Crumpler وJames A. Lewis. الفجوة في القوة العاملة في مجال الأمن السيبراني. مركز الدراسات الاستراتيجية والدولية، 29 يناير 2019.

112 Rob Saunders. 134 إحصائية واتجاه بشأن الأمن السيبراني لعام 2021. شركة Varonis. حُدثت في 16 مارس 2021.

113 شركة Proofpoint. التقرير السنوي لشركة Proofpoint بشأن العامل البشري، تفاصيل اتجاهات كبار المجرمين السيبرانيين: تحتاج 99 في المائة من الهجمات السيبرانية إلى البشر للنقر على الزر، 9 سبتمبر 2019.

114 شركة Verizon. تقرير التحقيقات في خرق البيانات لعام 2019. شركة Verizon، 2019.

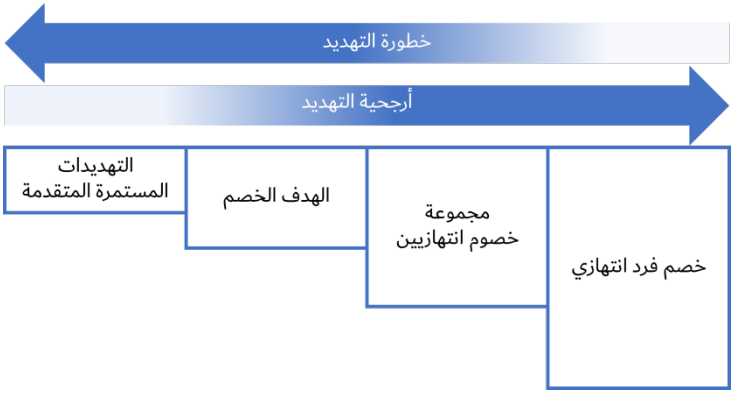
115 Lillian Ablon. لصوص البيانات: دوافع الأطراف الفاعلة فيما يتعلق بالتهديدات السيبرانية واستخدامها للبيانات المسروقة وتسييلها. مؤسسة RAND، 2018.

- ***التهديدات المستمرة المتقدمة (APT):*** كما حددها المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST)، هي عدائيات متطورة للغاية ولديها حيل قادرة على إنشاء موطئ قدم في شبكة الهدف لأغراض مثل تهريب المعلومات أو تقويض أو إعاقة الجوانب الحرجة لمهمة الهدف أو إضعاف أصوله الرقمية.[116] وتتكيف التهديدات المستمرة المتقدمة مع أنظمة دفاع الضحايا باستخدام نواقل هجوم متعددة، فهي قادرة على متابعة أهدافها خلسة لفترات طويلة من الزمن. وهذه العدائيات هي الأكثر تطوراً من حيث المهارات التقنية والتمويل والموارد التنظيمية، وغالباً تتولى رعايتها الدول التي تسعى إلى تحقيق مصالحها الجيوسياسية.

بينما تستهدف جميع الأطراف الفاعلة ذات النوايا الخبيثة سرية وسلامة وتيسر المعلومات والأصول، هناك مجموعة واسعة من النتائج المحتملة لاقتحام الشبكات. ويغطي التعبير الشامل "الهجوم السيبراني" مجموعة متنوعة من الأعمال، تتراوح من الإزعاج، مثل تشويه موقع الويب أو هجمات رفض الخدمة، إلى التدمير الخطير للبيانات والأنظمة من خلال الهجمات المسلحة.

تختلف الأطراف الفاعلة ذات النوايا الخبيثة وهجماتها من حيث التعقيد والمدة والضرر. ففي حين أنه من المستحيل الدفاع ضد جميع التهديدات، يمكن للمنظمات تطبيق نماذج التهديد لتحديد التهديدات ذات الصلة وفقاً لمواصفاتها الشخصية ومخاطرها وسياقها. ويوضح **الشكل 1** نموذجاً عاماً للتهديد السيبراني، يوضح أن غالبية المنظمات تواجه عادةً تهديدات انتهازية وأقل تعقيدًا، وبالتالي تتطلب أوضاع دفاعية أقل تحديداً.

الشكل 1: نموذج تهديد



على النقيض من ذلك، فإن الشركات الكبيرة والمنظمات التي تعمل في القطاعات الحرجة والاستراتيجية والجهات التي تدير المعلومات والأصول القيمة تكون أكثر احتمالاً للهجوم من خلال التهديدات المستهدفة أو التهديدات المستمرة المتقدمة.

ويقدم هذا القسم لمحة عامة عن تهديدات الفضاء السيبراني. وسيوفر الجزء المتبقي من الفصل معلومات عن كيفية تطبيق هذه التهديدات على التكنولوجيات الناشئة وما هي الاستراتيجيات والأطر والحلول العملية المتاحة للدفاع ضدها.

1.2.5 التهديدات من منظور تكنولوجي

تقوم التكنولوجيات الناشئة بجمع وتبادل وتخزين وتحليل كميات هائلة من البيانات، غالباً بسرعة غير مسبوقة. ومع ذلك، فإن الخصائص المحددة، مثل زيادة التوصيلية وتعقد البيئات التي تتفاعل فيها هذه الأدوات، يمكن أن تثير عدداً من التحديات التكنولوجية والتنظيمية للأمن.

[116] المعهد الوطني الأمريكي للمعايير والتكنولوجيا. المبادرة التحويلية لفريق المهام المشترك، المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا 39-800: إدارة المخاطر الأمنية للمعلومات، الرسالة ومنظور نظام المعلومات، مارس 2011.

التمثيل الافتراضي

يشكل التمثيل الافتراضي ركيزة أساسية للبيئات التكنولوجية الحديثة، لأنه يمكن المطورين من تكييف البنى التحتية لتلبية احتياجات التطبيقات الشبكية ودعم تطوير معماريات وبروتوكولات جديدة في بيئة مثالية.[117] ومع ذلك، فإن التشارك في قنوات الاتصالات وأجهزة التسيير في حالات تعدد الشاغلين يمثل عدداً من المخاطر الأمنية:[118]

- يتفاقم خطر الكشف غير المصرح به عن البيانات، سواء عن قصد أو عن غير قصد، في البيئات الافتراضية التي يتم فيها التشارك في الموارد المادية بين العديد من العملاء أو المستعملين. ويمكن تنفيذ الأنشطة الضارة، مثل الاعتراض والكسح (البحث عن بقايا البيانات في شبكة ما من أجل الحصول على المعلومات) بسهولة أكبر إذا كان النظام يسمح بالتفتيش المتبادل لمختلف المستعملين.
- قد يؤدي تعدد الشاغلين إلى زيادة المخاطر التي تنشأ عن سلسلة الإمداد ويجعل من الصعب الدفاع ضد عمليات الاقتحام. ويمكن للخصوم الحصول على امتيازات واقتحام شبكة الهدف باستخدام موارد ذات مستوى حماية أقل تشترك في نفس الطبقة المادية كناقل.
- في البيئات الافتراضية، تكون نتائج تداول الهوية معقدة بشكل خاص، بسبب الأنظمة ذات التراتبية العالية لإدارة الامتيازات. ويوفر هذا السياق مساحة للأطراف الفاعلة ذات النوايا الخبيثة لارتكاب الاحتيال جرائم تزوير الهوية ومضاعفة الامتيازات.
- قد يؤدي التشارك في الموارد أيضاً إلى تضخيم مخاطر الانقطاعات الخبيثة أو غير الطوعية في الأنظمة التي يمكن أن تؤثر سلباً على توريد الخدمات. فعلى سبيل المثال، يمكن للتحميل الزائد للموارد المادية أن يؤدي إلى تدهور أداء الشبكات الافتراضية، مع ما يترتب على ذلك من انقطاع في الاتصالات.

أمن الحوسبة السحابية

في الحلول السحابية، تتم الاستعانة بمصادر خارجية لتقديم خدمات وموارد تكنولوجيا المعلومات، بما في ذلك وظائف ومسؤوليات الأمن ذات الصلة، إلى مورد الخدمة السحابية. من ناحية أخرى، يمكن أن يسمح ذلك للتكنولوجيات الجديدة بالتوسع بسرعة وتعزيز الأمن، نظراً لأن المورد، بناءً على وفورات الحجم، يمكن أن يوفر تدابير وضوابط وقائية متقدمة. ومع ذلك، يمكن أن تكون مواطن الضعف السحابية مغرية للمهاجمين السيبرانيين، نظراً إلى أن اختراقاً واحداً ناجحاً يمكن أن يعرض العديد من العملاء للخطر. تتكون الحلول السحابية من عدة طبقات من التجريد (وهي التطبيق ونظام التشغيل والمعمارية والشبكة)، مما يعني أنه يمكن للخصوم استهدافها من خلال نواقل متعددة:

- يمكن استغلال مواطن الضعف في البرمجيات من خلال حقن لغة الاستعلام البنيوية وأنماط الهجوم الأخرى. وفي هذا السيناريو، من المهم لعملاء الحوسبة السحابية أن يكونوا على دراية بمن هو المسؤول عن أنشطة التصحيح (أي مزود الحلول السحابية لحلول البرمجيات كخدمة، وعميل حلول البنية التحتية كخدمة والمنصة كخدمة).
- يقدم موردو الحلول السحابية مجموعة واسعة من الخدمات والسطوح البينية لبرمجة التطبيقات الموصولة بالإنترنت للسماح للعملاء بإدارة أصولهم ومراقبتها. وتجعل هذه التوصيلية الحلول السحابية هدفاً محتملاً لهجمات الشبكة، مثل التلصص/التنصت على حركة الشبكة وهجمات رفض الخدمة وهجمات الاعتراض.
- إذا تسنى للمهاجم الحصول بشكل غير قانوني على إثباتات المستعملين، فقد يتمكن من النفاذ إلى السطح البيني للإدارة الذي يستخدمه المدراء لإدارة عدد كبير من الأصول. لذلك يجب إنشاء آليات استيقان وتخويل قوية، خاصة للموظفين ذوي الامتيازات الكبيرة.
- يزيد تعدد الشاغلين من مخاطر انتهاك البيانات وتسربها إذا أخفقت ضوابط الفصل أو تم خرقها (تعطل العزل).
- عند الانتقال إلى الحلول السحابية، يكون لدى العملاء عادةً رؤية أقل وتحكماً أقل في بياناتهم وأصولهم. ويؤدي ذلك إلى زيادة المخاطر المرتبطة بالحذف المأمون للبيانات المخزنة على عدد من الأجهزة داخل

---

[117] Leonardo Richter Bays et al. أمن الشبكات الافتراضية: التهديدات والتدابير المضادة والتحديات. *جريدة خدمات وتطبيقات الإنترنت*، العدد 6، المقالة رقم 1 (2015).

[118] وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA). الجوانب الأمنية للتمثيل الافتراضي، 10 فبراير 2017.

البنية التحتية لمورد الحلول السحابية. ومن المهم التحقق من حذف البيانات بشكل مأمون وكامل. وتتفاقم هذه المشكلة بسبب الحلول متعددة الأوساط السحابية.

- قد تؤدي تقييدات البائعين، حيث يواجه العملاء صعوبات في الانتقال إلى مورد حلول سحابية آخر، إلى مخاطر أمنية خطيرة. وينبغي للمستعملين تضمين خطط لتغيير موردي الخدمة في استراتيجيات استمرارية الأعمال الخاصة بهم وتخزين جميع البيانات بنسق قياسي يمكن نقله بسهولة.
- وفقًا لهيئة تنظيم الاتصالات في ناميبيا، يعد تخزين بيانات العملاء في مراكز بيانات الخدمات السحابية الموجودة خارج الحدود الوطنية مشكلة ملحة. وفي البلدان التي تتم فيها استضافة مخدمات البيانات، لا تتمتع هيئات التنظيم بأي ولاية قضائية ولا حتى قدر ضئيل من الرقابة للتعامل مع مسائل حماية العملاء والأمن السيبراني عند حدوث هجمات إلكترونية، مما يؤدي إلى سرقة الهوية الشخصية، وتسرب المعلومات الشخصية، وفي بعض الحالات، خسارة محتملة في الإيرادات. وعلاوةً على ذلك، يمكن أن تختلف التشريعات في البلدان المضيفة فيما يتعلق بالنفاذ إلى المعلومات وحماية البيانات والاعتراض القانوني، مما قد يعرض العملاء للنفاذ غير المصرح به إلى البيانات الشخصية.[119]

إنترنت الأشياء

مع انتشار ثقافة الأمن حسب التصميم التي لا تزال في مهدها، تعد زيادة التوصيلية واحدة من أكثر الاتجاهات إثارة للقلق من حيث المخاطر، وتشكل تحديات أمنية كبيرة:[120]

- الأشياء الذكية - التي تتراوح من الكاميرات والأبواب وأجهزة التبريد إلى أنظمة تكييف الهواء والأجهزة القابلة للارتداء - تجمع قدراً هائلاً من المعلومات (كل من البيانات والبيانات الشرحية). ويمكن للمهاجمين معرفة الكثير عن حياة هدفهم من خلال التنصت على البيانات التي تستشعرها الأشياء الذكية للهدف.
- من بين التهديدات الناشئة لإنترنت الأشياء برمجيات طلب الفدية. وتوفر الأجهزة الذكية عالماً جذاباً للابتزاز للمهاجمين، ليس فقط بسبب العدد الهائل من الأهداف المتاحة في المتناول، ولكن أيضاً لأن الهجمات بهذه الطريقة يمكن أن تعطل وظائف الأجهزة، وبالتالي إزعاج الهدف وإجباره على دفع الفدية.[121]
- أجهزة إنترنت الأشياء معرضة بشكل خاص لهجمات رفض الخدمة ورفض الخدمة الموزع، لأن معظمها يتمتع بقدرات تقنية محدودة (الذاكرة والتخزين ووحدة المعالجة المركزية وما إلى ذلك). ويمكن للمهاجمين إغراق مواردهم المحدودة بسهولة، مما يتسبب في انقطاع الخدمة.
- تشكل محدودية الموارد في أجهزة إنترنت الأشياء تحدياً خطيراً عندما يتعلق الأمر بتضمين تدابير أمنية، يمكن أن تكون ثقيلة من الناحية الحاسوبية.[122]
- تكمن إحدى القضايا الأمنية الرئيسية لإنترنت الأشياء في مستوى تعقيدها. وتدمج الأجهزة تكنولوجيات مختلفة، مثل التمثيل الافتراضي والحوسبة السحابية وأجهزة الاستشعار والشبكات، والتي تحمل نقاط الضعف الخاصة بها. ويعني تأمين إنترنت الأشياء تأمين سلسلة هذه المكونات بأكملها. وبالمثل، لإنترنت الأشياء تطبيقات في عدة مجالات (أتمتة المنازل، والرعاية الصحية، والأجهزة القابلة للارتداء، وما إلى ذلك)، والتي لها احتياجات أمنية مختلفة وتتعرض لتهديدات مختلفة.
- على الرغم من أن الهجمات المستندة إلى الإنترنت هي الأكثر شيوعاً، يمكن أيضاً استهداف أجهزة إنترنت الأشياء من خلال الهجمات المادية. ويمكن للمهاجمين الوصول بسهولة إلى أجهزة إنترنت الأشياء والعبث بها في المناطق التي تعاني من انخفاض المراقبة أو انعدامها.
- يمكن أيضاً استخدام أجهزة إنترنت الأشياء كنواقل لإطلاق هجمات رفض الخدمة الموزع. ففي عام 2016، على سبيل المثال، وقع مورد أنظمة أسماء ميادين شهير ضحية لهجوم لرفض الخدمة الموزع صدر عن عشرات الملايين من عناوين بروتوكول الإنترنت، بحيث تأتي غالبية الحركة الضارة من أجهزة إنترنت الأشياء مثل الطابعات والمسيرات والكاميرات.[123]

---

119 الوثيقة SG2RGQ/75 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من ناميبيا

120 Amit Ashbel. ظهور إنترنت الأشياء وما يرتبط بها من مخاطر أمنية. 7 يوليو 2016.

121 Mohammad Ahsan Chishti وSyed Rameem Zahra، برمجيات طلب الفدية وإنترنت الأشياء: كابوس أمني جديد. *إجراءات المؤتمر الدولي التاسع بشأن الحوسبة السحابية وهندسة علوم البيانات (الحشد)*. Uttar Pradesh، الهند، 10-11 يناير 2019.

122 Ammar Rayes وSamer Salam. إنترنت الأشياء من الضجيج إلى الواقع: الطريق إلى الرقمنة، Springer International Publishing، 2019.

123 Nicole Perlroth. يستخدم القراصنة أسلحة جديدة لاختراق المواقع الإلكترونية الرئيسية في الولايات المتحدة. جريدة *نيويورك تايمز*، 21 أكتوبر 2016.

تكنولوجيا الجيل الخامس (5G)

سيوفر الجيل الخامس من تكنولوجيا الاتصالات، المعروف باسم 5G، توصيلاً أكثر موثوقية وعالي الجودة يعتمد على السرعات العالية والكمون المنخفض، مما يعظم من نتاج تطبيقات التكنولوجيات الناشئة في مجالات مثل الطاقة والصحة والتصنيع. وتُعد هذه الأصول هدفًا جذاباً للمهاجمين، كما أن نقاط الضعف المتأصلة فيها تجعل الأمن السيبراني صعباً من الناحية العملية. وعلاوةً على ذلك، ولأن حلول 5G لا تزال في المرحلة التجريبية، فهناك ندرة في المعلومات والبيانات حول حوادث الهجمات السيبرانية، مما يجعل من الصعب فهم التهديد المحتمل:[124]

- مشهد تهديدات شبكات الجيل الخامس (5G) واسع وغير متجانس؛ فبالجمع بين التكنولوجيات المتنوعة، فإنها ترث أيضاً نقاط الضعف والتهديدات الخاصة بها. وعلى وجه الخصوص، يمكن استهداف شبكات وأصول تكنولوجيا الجيل الخامس من خلال الاستفادة من أوجه انعدام الأمن التقليدية من تكنولوجيات الأجيال الثاني والثالث والرابع، ونقاط الضعف التقليدية القائمة على بروتوكول الإنترنت، والتدفقات التي أدخلتها تكنولوجيا التمثيل الافتراضي. ويمكن للمهاجمين أيضاً استهداف الأصول الخاصة بتكنولوجيا الجيل الخامس تحديداً، مثل الشبكة الأساسية ونقطة النفاذ وعناصر الحواف.
- يمكن أن تشمل الهجمات ضد تكنولوجيات الجيل الخامس محاولات لسرقة البيانات أو التلاعب بها أو تدميرها أو اعتراض الاتصالات أو تشويشها أو إتلاف الأصول المادية أو تعطيل توفير الخدمات. وستعمل تكنولوجيا الجيل الخامس على توصيل مجموعة واسعة من القطاعات والقطاعات الرأسية، مما سيؤدي على الأرجح إلى تغيير مشهد الأمن السيبراني، وبالتالي ظهور نقاط ضعف جديدة.
- ينبع عامل التهديد الحاسم من سلسلة الإمداد، ولا سيما البائعين وموردي الخدمات المخترقين. ويكمن الخطر في أن البائع قد يدمج بشكل خبيث في منتجاته أبواب خلفية مخفية أو برمجيات أو عيوباً خطيرة. ويؤدي تنفيذ التحديثات الأوتوماتية (وغير المتحكم فيها) والتلاعب في الوظائف أيضًا إلى مشكلات تتعلق بالأمن. والعلاقة بين تكنولوجيا الجيل الخامس والأمن القومي واضحة، وينبغي اختيار موردي الخدمات بعناية بناءً على نهج يراعي المخاطر.

الذكاء الاصطناعي

سيؤثر انتشار حلول الذكاء الاصطناعي في مختلف قطاعات المجتمع على مشهد الأمن السيبراني بعدة طرق. ويمكن استهداف هذه الأصول من قبل الأطراف الفاعلة ذات النوايا الخبيثة أو استخدامها من قبل الخصوم والمدافعين:

- يمكن التلاعب بأصول الذكاء الاصطناعي من خلال تغيير القرارات والسلوكيات المؤتمتة، لا سيما من خلال تسميم البيانات، والعبث بنماذج التصنيف، والأبواب الخلفية.[125] وتستفيد كل هذه الطرق من القدرة التعليمية للنظام من أجل تغيير المخرجات سلباً عن طريق تغذية النظام ببيانات ومعلومات خاطئة.[126]
- يلجأ القراصنة إلى حلول الذكاء الاصطناعي لتحسين مدى وصولهم وقدراتهم. ويمكن استخدام الذكاء الاصطناعي لتوفير برمجيات ضارة قادرة على تجاوز الإجراءات الدفاعية بشكل مستقل، وتكييف استراتيجياتها على أساس النجاحات وتحسين عملياتها باستمرار.
- الذكاء الاصطناعي هو أيضاً مورد دفاعي مهم. فهو يمكنه أن يزيد بشكل كبير من قدرة النظام على الصمود من خلال تعزيز الأنشطة الدفاعية النموذجية، مثل الكشف عن التهديدات والحالات غير الطبيعية، والاستجابة للحوادث وتحليل التهديدات.

2.2.5 التهديدات من منظور نموذج الصناعة 4.0

يستلزم نموذج الصناعة 4.0 تطبيق الأتمتة، جنباً إلى جنب مع إنترنت الأشياء، وحلول التمثيل الافتراضي، والتحليلات والذكاء الاصطناعي، على قطاعات رأسية مختلفة. وتسمح هذه التكنولوجيات بجمع كميات هائلة من البيانات وتخزينها وتبادلها وتفسيرها ويمكن أن تحقق تحسينات كبيرة من حيث السرعة والكفاءة والفعالية من حيث التكلفة والإمداد بالخدمات. ويمكن تطبيق نموذج الصناعة 4.0 على قطاعات مختلفة، كل منها عرضة لتهديدات ومخاطر أمنية محددة.

---

[124] وكالة الاتحاد الأوروبي للأمن السيبراني. مشهد تهديدات شبكات الجيل الخامس في وكالة الاتحاد الأوروبي للأمن السيبراني. نوفمبر 2019.

[125] Fabio Roli وBattista Biggio. الأنماط الضارية: بعد عشر سنوات من ظهور تعلم الآلة العدائي. *التعرف على النماذج*، المجلد 84، ديسمبر 2018، الصفحات 317-331

[126] Matthew Jagielski وآخرون. التلاعب في تعلم الآلة: هجمات التسمم والتدابير المضادة لتعلم الانحدار. *ندوة معهد مهندسي الكهرباء والإلكترونيات بشأن الأمن والخصوصية (SP)، 2018*

المنازل الذكية

تعد المنازل الذكية واحدة من القطاعات العديدة التي يمكن فيها تطبيق نموذج الصناعة 4.0، لا سيما في الاستهلاك الذكي للطاقة والإضاءة والتدفئة. وتحتوي المنازل الذكية على مجموعة متنوعة من الأشياء الذكية التي تستخدم أجهزة استشعار والمفعلات وتتم إدارتها عن بُعد عبر الإنترنت.[127] ويؤدي توصيل الأجهزة بالإنترنت إلى حدوث عدد من المخاطر الأمنية:

- تولد المنازل الذكية كميات ضخمة من البيانات التي تكون عرضة للهجمات. وكما أشارت وزارة البريد وتكنولوجيا المعلومات والاتصالات الجديدة في تشاد، فإن الأشياء الموصولة (بما في ذلك التلفزيونات الذكية) تكون عرضة لتهديدات أمن نظام المعلومات. فعلى سبيل المثال، يمكن أن يؤدي استعمال التلفزيونات الموصولة إلى نفاذ أشخاص غير مصرح لهم إلى بيانات خصوصية عن طريق الإنترنت، وتسهيل سرقة الهوية عبر الإنترنت. والأشياء الموصولة معرضة للهجوم مثلها مثل أي حاسوب شخصي موصول بشبكة حاسوبية، وهي معرضة بالمثل لتهديدات البرمجيات الضارة.[128]
- تتمتع الأجهزة الذكية بأمن ضعيف ويمكن بسهولة اختراقها. ويمكن للمهاجمين الذين يتسنى لهم التحكم في الجهاز التحرك بشكل جانبي داخل الشبكة المحلية من أجل السيطرة على عقد أخرى.
- عادةً ما تحتوي الأجهزة الذكية على موارد حاسوبية ضعيفة، مما يجعلها عرضة بشكل خاص لهجمات رفض الخدمة ورفض الخدمة الموزع، مما يجعل الجهاز أو الشبكة غير متاحين للمستعمل المقصود بصفة مؤقتة.

المدن الذكية

تجمع المدن الذكية بين التكنولوجيات الناشئة وتكامل البيانات وأتمتة المهام لاستمثال تنظيم المدن وتقديم خدمات أفضل. وتعتمد المدن الذكية على تدفقات البيانات المكثفة المشتركة بين الخدمات الحرجة، مثل النقل وإمدادات الطاقة والرعاية الصحية، والتي أصبحت مترابطة بينياً بشكل متزايد. وينتج عن حجم البيانات المنتجة والدور الذي تؤديه البيانات في إدارة المدن الذكية حاجة ماسة للأمن السيبراني من أجل حماية خصوصية المعلومات وسلامة الأصول الرقمية ضد التهديدات الأمنية المختلفة:

- ***الصحة الإلكترونية***: مع تزايد الاعتماد على التكنولوجيا وكم البيانات الصحية، لا بد لموردي خدمات الرعاية الصحية حماية المعلومات الحساسة وضمان تقديم الخدمات. وعلى الرغم من عدم وقوع حوادث معروفة حتى الآن، فقد أثبتت عمليات المحاكاة أن من الممكن إيقاف تشغيل أجهزة تنظيم ضربات القلب المغروسة لاسلكياً،[129] واختراق مضخات الأنسولين لإطلاق جرعات قاتلة[130] وحتى اختراق أنظمة مراقبة المريض لتعديل العلامات الحيوية للمرضى في الوقت الفعلي.[131]
- ***الشبكات الذكية***: هي عنصر أساسي في المدن الذكية. وهي تستخدم أجهزة ثنائية الاتجاه، مثل أجهزة الاستشعار والمفعلات والعدادات، تسمح بالحفاظ على التوازن والإشراف باستمرار على تدفقات الطاقة من المنتجين إلى المستهلكين.[132] ونظراً لأن الشبكات الذكية تعتمد على بروتوكولات تكنولوجيا المعلومات والاتصالات وتوصيلات الإنترنت، فهي عرضة للهجمات السيبرانية.[133] وتمثل الشبكات الذكية هدفاً مغرياً للهجمات؛ ومع ذلك، فإن للشبكات الذكية معمارية معقدة، ويتطلب التسبب في ضرر واسع النطاق موارد تقنية وتنظيمية عالية المستوى. وحتى الآن، لم تُسجل إلا حالتان معروفتان فقط من حالات انقطاع التيار

---

127 Ado Adamou Abba Ari وآخرون. تمكين الخصوصية والأمن في الحوسبة السحابية للأشياء: المعمارية والتطبيقات وتحديات الأمن والخصوصية. *الحوسبة والمعلوماتية التطبيقية*، 31 يوليو 2020

128 الوثيقة 2/140 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من تشاد

129 Daniel Halperin وآخرون. أجهزة توليد ضربات القلب وأجهزة تنظيم ضربات القلب المغروسة: الهجمات الراديوية البرمجية والدفاعات الصفرية. *ندوة معهد مهندسي الكهرباء والإلكترونيات بشأن الأمن والخصوصية (SP)، 2008*.

130 Arundhati Parmar. القراصنة يكشفون نقاط الضعف في مضخات الأنسولين اللاسلكية. *MedCityNews*، 1 مارس 2012. David Klonoff. الأمن السيبراني لأجهزة مرض السكري الموصولة. *مجلة علوم وتكنولوجيا مرض السكري 9*، المجلد 9، العدد 5، 16 أبريل 2015.

131 Douglas McKee. من 80 إلى 0 في أقل من 5 ثوان: تزوير البيانات الحيوية الطبية للمرضى. McAfee، 11 أغسطس 2018.

132 Luay A. Wahsheh وLindah Kotut. استقصاء تحديات وحلول الأمن السيبراني في الشبكات الذكية. *ندوة الأمن السيبراني لعام 2016 (CYBERSEC)*.

133 Resul Das وMuhammed Zekeriya Gunduz. الأمن السيبراني في الشبكات الذكية: التهديدات والحلول المحتملة. *مجلة Computer Networks*، المجلد 169، 14 مارس 2020.

الكهربي بسبب الهجمات السيبرانية، وهما هجوما BlackEnergy3 وCrashoverride، ويُعتقد أن كلاهما نفذتهما جهات فاعلة من دول.[134]

- ***النقل الذكي***: يمكن تطبيق الأصول الرقمية والأنظمة المادية وشبكات الاتصالات والأتمتة على البنية التحتية للنقل لاستمثال الجودة والكفاءة. ومن خلال تغيير البيانات والمعلومات، يمكن للمهاجمين عرقلة حركة المرور وحتى التسبب في وقوع حوادث. وعلاوةً على ذلك، تتضمن أنظمة النقل الذكية تدفقاً كبيراً للمعلومات الشخصية والحساسة التي يجب تأمينها.

إنترنت الأشياء الصناعية

تكيف إنترنت الأشياء الصناعية (IIoT) نموذج إنترنت الأشياء حسب المشهد الصناعي. فعند دمجها مع الروبوتات والأتمتة، يمكن أن تحقق فوائد قيّمة للشركات الصناعية، بما في ذلك عن طريق تحسين الجودة والفعالية من حيث التكلفة والصيانة للعملية الإنتاجية. وتتمتع هذه الأنظمة السيبرانية المادية بخصائص ومتطلبات محددة تجعل نقل تدابير الأمن السيبراني التقليدية صعبة إلى حد ما.

الأنظمة السيبرانية المادية هي بيئات شديدة في الوقت الفعلي بمستوى عالٍ من التركيز، حيث يسود فيها تيسر البيانات فيما يتعلق بالسلامة والسرية.[135] وفي مثل هذه الأنظمة، تعمل المكونات الرقمية مع العمليات المادية، مثل حركات الأشياء، والتفاعلات الكيميائية، وإطلاق المواد وعمليات التبريد، وتعمل تدفقات البيانات كمدخلات لتنفيذ المهام. وفي مثل هذه السياقات، قد يؤدي اعتماد ضوابط أمنية شائعة، مثل برامج مكافحة الفيروسات أو التجفير أو جدران الحماية، إلى إبطاء تدفق البيانات والتداخل مع تنفيذ الأنشطة، مما يؤدي إلى تأخيرات قد تؤثر بشكل كبير على العمليات، على الرغم من عدم أهميتها من الناحية الكمية.[136]

بالإضافة إلى ذلك، لا تستطيع معظم المعدات في الأنظمة السيبرانية المادية التعامل مع الإجراءات الأمنية أو التحديثات المعقدة، مما يؤدي إلى إمكانية تعرض الأصول الموصولة بالإنترنت للخطر. ويمكن للهجمات السيبرانية ضد الأنظمة السيبرانية المادية الصناعية أن تتسبب في أضرار اقتصادية خطيرة من خلال تعطيل العمليات، وبالتالي، الإنتاج في أي مصنع.

ومع ذلك، فإن الشاغل الرئيسي هو أنه من خلال التلاعب بتدفق البيانات، يمكن للمهاجمين السيبرانيين تعديل تشغيل النظام حتى يصل إلى نقطة توقف ميكانيكية، مما يؤدي إلى تأثير حركي قد يكون له عواقب وخيمة على السلامة العامة. فعلى سبيل المثال، إذا قام أحد المهاجمين بتزويد النظام بأرقام معدلة تخبر وحدة التحكم أن درجة الحرارة تتناقص بسرعة كبيرة، فستقوم وحدة التحكم بالتعويض أوتوماتياً عن طريق زيادة التسخين، مما يؤدي إلى إفراط غير مكتشف في التسخين.[137] فمثلًا، تم في عام 2014 اختراق مصنع صلب ألماني بنجاح، وتمكن المهاجمون، من خلال منع الفرن من الإغلاق بشكل صحيح، من التسبب في أضرار مادية جسيمة للمكونات الحرجة.[138]

والعمليات السيبرانية العدائية ذات التأثيرات المادية معقدة للغاية، ولا تتطلب فقط فهماً جيداً للأصول الرقمية المستخدمة، ولكن أيضاً معرفة واسعة بالعملية المادية المستهدفة وفهماً تفصيلياً للمتغيرات المختلفة. ولهذه الأسباب، فإن التهديدات المستمرة المتقدمة والوكلاء الذين ترعاهم الدول من المرجح أن يكون لديهم الموارد التقنية والتنظيمية اللازمة لتنفيذ عمليات من هذا النوع.

3.5 الحلول الحالية والناشئة

لا تحتوي نسبة كبيرة من أجهزة إنترنت الأشياء على ميزات متأصلة أساسية للأمن السيبراني. وفي أكتوبر 2018، بعد 18 شهراً من التعاون مع ممثلي الصناعة والخبراء في المركز الوطني للأمن السيبراني، نشرت وزارة التكنولوجيا

---

134 شركة Dragos, Inc.. CRASHOVERRIDE: تحليل البرمجيات الضارة التي تهاجم شبكات الطاقة. 12 يونيو 2017.

135 Roberto Setola وآخرون. التهديدات السيبرانية للتكنولوجيات التشغيلية. *الجريدة الدولية للأنظمة وهندسة الأنظمة*، المجلد 10، العدد 2، 2020.

136 Roberto Setola وآخرون. لمحة عن الهجمات السيبرانية على أنظمة التحكم الصناعية، *معاملات الهندسة الكيميائية*، المجلد 77، 2019.

137 Stephen McLaughlin وآخرون. مشهد الأمن السيبراني في أنظمة التحكم الصناعية. *وقائع معهد مهندسي الكهرباء والإلكترونيات*، المجلد 104، الإصدار 5، مايو 2016.

138 Robert Lee وآخرون. هجوم سيبراني على مصنع صلب ألماني. حالة استعمال للدفاع عن أنظمة التحكم الصناعية، 30 ديسمبر، 2014.

الرقمية والثقافة والإعلام والرياضة في المملكة المتحدة مدونة ممارسات لأمن إنترنت الأشياء الاستهلاكية.[139] وتوفر المبادئ التوجيهية الطوعية البالغ عددها 13 في المدونة خط الأساس لأجهزة إنترنت الأشياء التي يجب على المصنّعين تضمينها في منتجاتهم لجعلها "آمنة حسب التصميم". وساهم المدونة في تطوير أول معيار قابل للتطبيق عالمياً بشأن أمن إنترنت الأشياء، المعيار ETSI TS 103 645.[140]

كما أكدت شركة Algérie Télécom على أهمية توفير أدلة وتوصيات بشأن تأمين التكنولوجيات الناشئة، مثل الحوسبة السحابية وإنترنت الأشياء، والتي من المتوقع أن تصبح المحرك الأساسي في تنمية نظام المعلومات والاقتصاد الرقمي.[141]

ويقدم **الجدولان 1** و**2** قائمة بتوصيات قطاع تقييس الاتصالات ذات الصلة بحماية الحوسبة السحابية وإنترنت الأشياء على التوالي، من حيث البنية التحتية والتطبيقات والبيانات والخصوصية.

الجدول 1: المعمارية الأمنية من أجل حماية البنية التحتية والتطبيقات والبيانات والخصوصية للحوسبة السحابية

العنوان	الموضوع	المؤسسة	الرابط الإلكتروني
نظرة عامة على أمن الحوسبة السحابية			
ITU-T X.1601	الإطار الأمني للحوسبة السحابية	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12613
تصميم أمن الحوسبة السحابية			
ITU-T X.1602	متطلبات الأمن من أجل بيئات تطبيقات البرمجية كخدمة	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12615
ITU-T X.1603	متطلبات أمن البيانات لخدمة مراقبة الحوسبة السحابية	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13406
ITU-T X.1604	متطلبات أمن الشبكة كخدمة (NaaS) في الحوسبة السحابية	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14093
ITU-T X.1605	متطلبات أمن البنية التحتية كخدمة (NaaS) عمومية في الحوسبة السحابية	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14094
ITU-T X.1631	تكنولوجيا المعلومات - تقنيات الأمن - مدونة ممارسات بشأن ضوابط أمن المعلومات استناداً إلى المعيار ISO/IEC 27002 من أجل الخدمات السحابية	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12490
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية			
ITU-T X.1641	مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12853
ITU-T X.1642	مبادئ توجيهية من أجل الأمن التشغيلي للحوسبة السحابية	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12616

[139] المملكة المتحدة، وزارة التكنولوجيا الرقمية والثقافة والإعلام والرياضة. مدونة ممارسات لأمن إنترنت الأشياء الاستهلاكية. أكتوبر 2018.

[140] المعهد الأوروبي لمعايير الاتصالات. الإصدار V1.1.1 من المعيار ETSI TS 103 645 (2019-02). الأمن السيبراني لإنترنت الأشياء الاستهلاكية.

[141] الوثيقة 2/66، للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من شركة Algérie Télécom SPA (الجزائر)

الجدول 2: المعمارية الأمنية من أجل حماية البنية التحتية والتطبيقات والبيانات والخصوصية لإنترنت الأشياء

العنوان	الموضوع	المؤسسة	الرابط الإلكتروني
أمن إنترنت الأشياء			
ITU-T X.1361	الإطار الأمني لإنترنت الأشياء القائم على نموذج البوابة	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13607
ITU-T X.1362	إجراء تجفير بسيط من أجل بيئات إنترنت الأشياء (IoT)	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13196
ITU-T X.1364	متطلبات الأمن وإطار من أجل إنترنت الأشياء ضيقة النطاق	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14088
ITU-T X.1365	منهجية أمنية من أجل استخدام التجفير القائم على الهوية لدعم خدمات إنترنت الأشياء (IoT) على شبكات الاتصالات	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14089
ITU-T X Suppl. 31	إضافة للتوصية ITU-T X.660 بشأن مبادئ توجيهية لاستخدام معرّفات الأشياء في إنترنت الأشياء	الاتحاد الدولي للاتصالات	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13411

التقنيات والأطر الأمنية الناشئة الأخرى

- يمكن لتطبيقات الذكاء الاصطناعي، بما في ذلك تعلم الآلة والتعلم العميق، أن تفيد بشكل كبير استراتيجيات الأمن السيبراني من حيث الكفاءة والفعالية من حيث التكلفة. وتستخدم هذه الحلول الانحدار والتصنيف والتكتل لاكتشاف الحالات الشاذة وتحديد طوبولوجيات مختلفة من الهجمات وتطوير استجابات علاجية محتملة. ويمكن لأنظمة الذكاء الاصطناعي أيضاً تعزيز أنشطة الاستجابة للحوادث من خلال اقتراح إجراءات محددة استجابةً لحوادث معينة. ويمكنها أيضاً تحسين أنشطة إدارة المخاطر من خلال التخصيص الأوتوماتي لقيم المخاطر لنقاط الضعف وأخطاء التشكيل الجديدة استناداً إلى أوصافها ومنع الهجمات بشكل استباقي عن طريق التعجيل بشكل كبير في استخراج وتفصيل وتطبيق البيانات المتعلقة بالتهديدات والجهات الفاعلة والهجمات والبرمجيات الضارة ونقاط الضعف ومؤشرات الاختراق.[142]
- تظهر أيضاً الميزات المحددة لتكنولوجيا السجلات الموزعة (DLT) إمكانات واعدة لتطبيقات الأمن.[143] أولاً، التخزين المستند إلى التكنولوجيا DLT يكون لا مركزياً، مما يقلل بشكل كبير من مخاطر خروقات البيانات واسعة النطاق، حيث لا يتسنى للمهاجمين النفاذ إلى جميع البيانات المخزنة من خلال نقطة نفاذ واحدة. وبالمثل، تجلب اللامركزية مزايا أمنية أساسية لشبكات إنترنت الأشياء، التي تُنظم عادة طبقاً لمنطق نموذج مخدم العميل، حيث تدير سلطة مركزية البيانات والأجهزة داخل الشبكة. وباستخدام تطبيقات التكنولوجيا DLT، يمكن لأجهزة إنترنت الأشياء تحديد الحالات الشاذة وعزل العقد التي تتصرف بشكل غير عادي. وكذلك، يمكن للتكنولوجيا DLT توليد الثقة في شبكات إنترنت الأشياء، من خلال ضمان أن يستمر ثبات التيسر وقابلية التدقيق والمساءلة والسلامة والسرية بالنسبة للبيانات المتبادلة.[144]
- تستلزم طريقة تنسيق الأمن والأتمتة والاستجابة (SOAR) حلولاً توصل أدوات وأنظمة الأمن من أجل تنفيذ أنشطة مثل إدارة نقاط الضعف والاستجابة للحوادث وأتمتة العمليات الأمنية بطريقة متكاملة وعضوية. وتسمح أتمتة العمليات الأمنية للنظام بتنفيذ التدابير العلاجية وأنشطة الصيانة (مسح نقاط الضعف، ومراقبة النفاذ والسجل) دون تدخل بشري.
- هناك خيار آخر هو نماذج عدم الثقة، حيث تكون بيئات الشبكة مجزأة داخلياً وتتم إدارة عمليات النفاذ وفقاً لمبدأ الامتياز الأقل. وهذا يعني أن كل وحدة نمطية، بما في ذلك المستعملون والأجهزة والسطوح البينية لبرمجة التطبيقات وأجهزة إنترنت الأشياء، لا تستطيع النفاذ إلا إلى الموارد والبيانات والأصول

---

142 Padmavathi Ganapathi وD. Shanmugapriya. كتيب البحث في تطبيقات تعلم الآلة والتعلم العميق للأمن السيبراني. *IGI Global*، 2019؛ وDave Shackleford. من يستخدم معلومات التهديدات السيبرانية وكيف؟ *SANS*، 12 فبراير 2015.

143 Nir Kshetri. دور سلسلة الكتل في تعزيز الأمن السيبراني وحماية الخصوصية. *سياسات الاتصالات*، المجلد 41، الإصدار 10، نوفمبر 2017.

144 Ben Cole. سلسلة إمداد الثقة" المتأصلة في أمن بيانات إنترنت الأشياء"، *برنامج إنترنت الأشياء*، 28 نوفمبر 2016.

الضرورية لوظيفتها المشروعة. وتعمل نماذج عدم الثقة على زيادة الأمن الداخلي بشكل كبير، حيث إنها تجعل الحركة الجانبية وزيادة الامتيازات أكثر صعوبة للمهاجمين الذين سيتعين عليهم، من أجل التمكن من النفاذ إلى الشبكة بأكملها، استهداف أجهزة متعددة.

- وسطاء أمن النفاذ إلى الخدمات السحابية هم نقاط إنفاذ سياساتية تعمل بين المستعملين وموردي الخدمات السحابية. فعلى سبيل المثال، يمكن أن تتضمن سياسات الأمن المفروضة الاستيقان، وتسجيل الدخول الوحيد، والتخويل، ومقابلة الإثباتات، وتحديد سمات الأجهزة، والتجفير، والترميز، والتسجيل، والتنبيه، والاكتشاف/المنع فيما يخص البرمجيات الضارة.[145]
- تشير إدارة النفاذ المتميز إلى مجموعة من الأدوات والحلول لمراقبة الحسابات المميزة وحمايتها، مثل حسابات المدير المستخدمة للنفاذ إلى الأصول والبيانات والموارد الحرجة. وتعزل هذه الحلول الحسابات الحرجة في مستودع آمن وخاضع للمراقبة، مما يقلل من مخاطر سرقة الإثباتات.
- ينبغي للمنظمات الانتقال من نهج التطوير والعمليات (DevOps) إلى نهج التطوير والأمن والعمليات (DevSecOps)، الذي يدمج الأمن كجزء متأصل من التطوير والعمليات. وداخل أطر عمل وأدوات نهج التطوير والأمن والعمليات، فإنه بدلاً من تثبيت الأمن في المنتجات النهائية (مثل البرمجيات والتطبيقات)، يعتبر الأمن ميزة لا غنى عنها وأساسية منذ المرحلة الأولى من التطوير. ويجعل هذا النهج الأمن أكثر صلابة ويخفف من المخاطر ويقلل من تكاليف الامتثال.
- ويقترح إطار Gartner للتقييم المستمر للمخاطر التكيفية والثقة (CARTA) نهجاً تكيفياً للأمن، حيث تستند القرارات إلى المخاطر والكفاءة.[146] وينطوي الإطار CARTA على ثلاث مراحل: "التشغيل"، والتي تركز على تحليل التهديدات الرئيسية؛ و"البناء"، التي تشير إلى التهديدات ونقاط الضعف التي تم تحديدها أثناء تطوير المنتجات والعمليات؛ و"التخطيط"، حيث تُستخدم التحليلات لتحديد المخاطر الأمنية وتقييم ما إذا كان التخفيف منها سيؤثر سلباً على الإنتاجية.[147]

الحلول الفعالة من حيث التكلفة

- وفقاً لوزارة التكنولوجيا الرقمية والثقافة والإعلام والرياضة في المملكة المتحدة، فإنه من خلال التركيز على التأثير على العائد على الاستثمارات من الهجمات الأقل تعقيداً والأكثر شيوعاً، يمكن البدء في معالجة تأثير الهجمات السيبرانية على نطاق واسع، مع تحقيق منافع كبيرة شاملة. وقد تم تطوير مخطط الدفاع السيبراني النشط (ACD) لزيادة تكلفة ومخاطر تصعيد الهجمات السيبرانية على السلع ضد المملكة المتحدة، وبالتالي تقليل العائد على الاستثمار بالنسبة للمجرمين.[148] وفي عام 2018، كان للمخطط التأثير الأكبر من خلال خدمة الإزالة الخاصة به، والتي تقوم بتحديد المواقع الضارة (إما الهجمات أو البنية التحتية الداعمة للهجمات) وإخطار المضيف أو المالك بضرورة إزالتها من الإنترنت: تمت إزالة 256 192 موقعاً احتيالياً بهذه الطريقة، تمت إزالة 64 في المائة منها في غضون 24 ساعة. بالإضافة إلى ذلك، تمت إزالة 133 22 حملة تصيد احتيالي في فضاء IP مخصص للمملكة المتحدة (بإجمالي 203 142 هجمة فردية)، وتمت إزالة 124 14 موقعاً من مواقع التصيد الاحتيالي ذات صلة بالحكومة.[149]
- وفقاً للشركة الليتوانية NRD Cyber Security، فإنه من أجل تحقيق تأثير إيجابي كبير على أمن البيئة الرقمية الوطنية، ينبغي أن تعمل الأفرقة CSIRT الوطنية والقطاعية ليس فقط كجهات اتصال وكجهات تنسيق وتحليل للاستجابة للحوادث، ولكن أيضاً كجهات تيسير ملهمة في تطوير قدرات إضافية مستقلة للأمن السيبراني داخل الصناعات والمجتمعات المهنية ومراكز التعليم والبحوث والأحداث والاجتماعات والمؤتمرات وأفرقة CSIRT الخاصة والداخلية.[150]

---

145 Gartner. مسرد Gartner. وسطاء أمن النفاذ إلى الخدمات السحابية (CASB).
146 Gartner. نهج Gartner لأمن تكنولوجيا المعلومات من أجل العصر الرقمي. 12 يونيو 2017.
147 Gartner. عرض Gartner: الاستفادة من الأتمتة في الأمن العصري. 17 يونيو 2019.
148 Ian Levy و Maddy S.. الدفاع السيبراني النشط (ACD) – العام الثاني. المركز الوطني للأمن السيبراني بالمملكة المتحدة. 15 يوليو 2019.
149 الوثيقة SG2RGQ/175 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من المملكة المتحدة
150 الوثيقة 2/172 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من شركة NRD Cyber Security (CS) (ليتوانيا)

- وفقًا لشركة Guardtime الإستونية، تعتبر التمارين السيبرانية ضرورية لتحقيق المرونة السيبرانية المستدامة لأنها تساعد الأفرقة على فهم العمليات اللازمة للتخفيف من حدة الأزمات السيبرانية. وتوصي إستونيا بتطوير برنامج لإدارة المرونة السيبرانية يغطي التعليم والتدريب والتمارين السيبرانية، بدءاً من الأحداث المحلية وصولاً إلى التدريبات المنتظمة على المستوى الوطني. وينبغي أن تأخذ هذه البرامج في الاعتبار الجوانب المختلفة للهيكل التنظيمي الوطني والوضع الاجتماعي والاقتصادي، وأدوار ومسؤوليات مختلف أصحاب المصلحة، والبيئة التنظيمية الوطنية، والشراكات الإقليمية والدولية للبلاد، والمخاطر المختلفة التي يواجهها البلد في إطار مشهد التهديدات السيبرانية الذي يتسم بالتطور.[151]

[151] الوثيقة SG2RGQ/32 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من شركة Guardtime AS (إستونيا)

الفصل 6 - كيفية دعم الأمن السيبراني لحماية البيانات الشخصية

1.6 مقدمة

مع ظهور تكنولوجيا المعلومات الجديدة، يظهر معها العديد من الخدمات الجديدة والمريحة بشكل متزايد للاستخدام اليومي. ومع ذلك، فإن ظهور تكنولوجيا المعلومات الجديدة يغير أيضاً بشكل ثنائي من مخاطر حماية الخصوصية والبيانات التي يواجهها الأفراد. فعلى الرغم من استمرار ظهور مخاطر جديدة على البيانات الشخصية، يمكن استخدام تقنيات مختلفة لتدنية أو تجنب هذه المخاطر. ولهذا السبب، يجب التركيز بشكل أكبر على الأمن السيبراني وتكنولوجيات تعزيز الخصوصية التي يمكن أن تدعم حماية البيانات الشخصية، مثل إخفاء الهوية والخصوصية حسب التصميم.

وإخفاء الهوية هو إجراء لإدارة البيانات وإلغاء تحديد الهوية يتم من خلاله استبدال حقول المعلومات المحددة لهوية الأشخاص في سجل البيانات بواحد أو أكثر من معرفات الهوية الاصطناعية، أو "أسماء مستعارة". والاسم المستعار الواحد لكل حقل يتم استبداله أو مجموعة من الحقول المستبدلة يجعل سجل البيانات أقل قابلية للتحديد، بينما يظل مناسباً لتحليل البيانات ومعالجتها.[152] ويمكن لإخفاء الهوية أن يساعد في حماية المعلومات المحددة لهوية الأشخاص وقد يقلل العبء على الكيانات التي تقوم بجمع هذه البيانات والاحتفاظ بها.

في الخصوصية حسب التصميم، لا ينتظر المرء إلى ما بعد الخرق لاتخاذ الإجراءات الأمنية. فبدلاً من ذلك، يتوقع المطورون أو يتنبأون بتهديدات الخصوصية أو يمنعونها من الحدوث من خلال تدابير وقائية، مثل تخطيط الخدمة أو تصميمها.[153] ويتمثل الاختلاف بين النهجين في أنه بينما يتطلب إخفاء الهوية إجراءات تقنية معينة، فإن الخصوصية حسب التصميم تمنح مراقبي البيانات المرونة في تحديد التدابير التقنية الإضافية التي يمكن أن تضمن أمن البيانات وخصوصيتها بشكل أفضل.

2.6 المشهد القانوني وأفضل الممارسات لدى الدول الأعضاء

في البرازيل، يشمل القانون الذي أُعتمد مؤخراً لحماية البيانات العامة، تعاريف الأنماط المختلفة للبيانات الشخصية وبيانات المعالجة ويوفر الأذونات القانونية من أجل المعالجة المحلية والدولية، والحقوق الأساسية لموضوعات البيانات، وإنشاء هيئة لحماية البيانات الوطنية.[154] ويحدد القانون مبادئ تقليل البيانات إلى الحد الأدنى ومنع خرق البيانات وأمن البيانات وينص على قواعد محددة للتحكم في تلك المجالات. ويتبنى القانون أيضاً مفهوم الأمن حسب التصميم، وينص على ضرورة تنفيذ التدابير الأمنية لحماية البيانات الشخصية بدءاً من مرحلة تصور المنتج أو الخدمة وحتى تنفيذها.

وفي عام 2017، أصدرت الصين رسمياً مجموعة من المعايير الوطنية بشأن مواصفات أمن المعلومات الشخصية في تكنولوجيا أمن المعلومات، والتي تكمل متطلبات أمن المعلومات الشخصية المنصوص عليها في قانون الأمن السيبراني. وتوفر المعايير مبادئ توجيهية وتعليمات تشغيلية. وتواصل الصين أعمال البحث والتطوير لمعايير حماية المعلومات الشخصية.[155]

وفي الصين، تدأب الشركات المحلية لأمن البيانات أيضاً في بحث وتطوير المنتجات والخدمات الأمنية، بما في ذلك في مجالات منع فقدان البيانات، وتدقيق سلامة قواعد البيانات، والمسح الكاشف عن التسرب في قواعد البيانات، وكذلك تجفير قواعد البيانات، وتقنيع البيانات، بغية توفير الدعم التقني لحماية البيانات الشخصية.

وأدخلت جمهورية كوريا تعديلاً رئيسياً على قانون حماية المعلومات الشخصية الخاص لديها لتوفير تدابير تقنية لحماية البيانات الشخصية.[156] وأدخل التعديل تغييرات لتبسيط الإشراف التنظيمي وإدخال مفهوم "البيانات

---

152 Wikipedia. https://en.wikipedia.org/wiki/Pseudonymization

153 استخدم مفهوم الخصوصية حسب التصميم في مجال المعمارية الحالية، بيد أن المفهوم كان ثانوياً. وقد بدأ يكتسب زخماً بعد أن أشار إليه Dr. Ann Cavoukian، مفوض المعلومات والخصوصية في أونتاريو، كندا، في أواسط تسعينات القرن الماضي.

154 الوثيقة SG2RGQ/143 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من البرازيل

155 الوثيقة 2/156 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من الصين

156 الوثيقة 2/342 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من جمهورية كوريا

المخفاة"، بما يسمح لأجهزة مراقبة البيانات ومعالجاتها بمعالجة البيانات بشكل أكثر أماناً، مع تدنية مخاطر إساءة استخدام البيانات وخرقها من خلال التدابير التكنولوجية والتنظيمية الأخرى مثل حماية البيانات حسب التصميم وبالتغيب.

بالإضافة إلى ذلك، نشرت حكومة جمهورية كوريا مبادئ توجيهية للحماية بشأن المعالجة الأوتوماتية للبيانات الشخصية. وفي حين أن التكنولوجيات الجديدة، مثل تحليل البيانات الضخمة المستند إلى الذكاء الاصطناعي وأجهزة الاستشعار المستخدمة في أجهزة إنترنت الأشياء لجمع البيانات، تجعل الخدمات المبتكرة ممكنة، فإن هناك صعوبات في فهم تدفق عمليات معالجة البيانات الشخصية والقيود في إجراءات المتابعة. وفي المعالجة الأوتوماتية للبيانات الشخصية من أجهزة إنترنت الأشياء، تشجع البيانات التوجيهية على تطبيق مفهوم الخصوصية حسب التصميم، حيث يتم النظر بشكل شامل في احتمالية حدوث انتهاكات للبيانات الشخصية من خطوات التخطيط المبكرة جداً وطوال دورة حياة البيانات.

وقواعد الحماية العشرة للمعالجة الأوتوماتية للبيانات الشخصية المدرجة في المبادئ التوجيهية هي:

- مرحلة التخطيط
  - القاعدة 1: تأكيد البيانات الشخصية اللازمة للخدمات
  - القاعدة 2: تأكيد الالتزام القانوني عند جمع البيانات الشخصية
- مرحلة التصميم
  - القاعدة 3: تقليل البيانات إلى الحد الأدنى ومعالجة البيانات الشخصية اللازمة فقط
  - القاعدة 4: تطبيق تدابير السلامة المناسبة في كل خطوة من خطوات معالجة البيانات الشخصية
  - القاعدة 5: نشر إجراءات وأساليب معالجة البيانات الشخصية بشفافية
  - القاعدة 6: ضمان أن أصحاب البيانات يمكنهم بسهولة ممارسة حقوقهم
  - القاعدة 7: تعليمات واضحة لأصحاب البيانات عند توفير البيانات الشخصية وتخويلها لطرف ثالث
  - القاعدة 8: إتلاف البيانات الشخصية ومنع الاستمرار في جمعها عند إنهاء الخدمة بواسطة صاحب البيانات
  - القاعدة 9: خطط لضمان حقوق أصحاب البيانات عند إنهاء العمل
- مرحلة الفحص
  - القاعدة 10: فحص عوامل المخاطر المتعلقة بانتهاكات البيانات الشخصية قبل إطلاق الخدمة.

نظراً للحاجة التي طرأت مؤخراً لتتبع الحالات المؤكدة لمرض COVID-19 حول العالم، اتخذت جمهورية كوريا تدابير مؤسسية وتقنية مختلفة لحماية البيانات الشخصية. فبالإضافة إلى توفير الأساس القانوني لتتبع المرضى المؤكدين من خلال تنقيح اللوائح ذات الصلة، يتم اتخاذ تدابير تقنية لفصل وإدارة معلومات تحديد الهوية لمنع الانتهاكات المحتملة للمعلومات الشخصية. وتُستخدم المعلومات المنفصلة في التحقيقات الوبائية عند حدوث حالات مؤكدة فقط، وتتم إدارة معلومات المستعمل والزائر بأمان، مثل التدمير التلقائي بعد أربعة أسابيع من التوليد.[157]

وطورت شركة إيطالية منهجية خاصة تستحوذ على ملكيتها يمكن للمنظمات استخدامها بسهولة لوضع قائمة بالأنشطة التقنية لتحقيق امتثال البنية التحتية السحابية (الخاصة أو العامة أو المختلطة) للوائح الخصوصية.[158] وتتضمن المنهجية مقترحاً بتحديد المبادئ التوجيهية العامة التي يمكن أن تستخدمها الدول الأعضاء لبناء أدوات التشكيل الوطنية الخاصة بها من أجل توحيد الامتثال متعدد البلدان بشكل أكثر كفاءة وأقل تكلفة، باستخدام الحوسبة السحابية كمنصة قوية لتسهيل تحقيق الطفرة في مجال الاقتصاد الرقمي.

وفي حالة أخرى من حالات أفضل الممارسات، تعترف المادة 25، المتعلقة بحماية البيانات حسب التصميم وبالتغيب، من لائحة حماية البيانات العامة للاتحاد الأوروبي (GDPR)، بمفهوم الخصوصية حسب التصميم باعتباره الطريقة الأنسب لمنع مخاطر حماية البيانات الشخصية التي تفرزها أجهزة إنترنت الأشياء، والبيانات

[157] الوثيقة SG2RGQ/268 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من جمهورية كوريا
[158] الوثيقة SG2RGQ/25 للجنة الدراسات 2 لقطاع تنمية الاتصالات المقدمة من شركة Prog-Software (إيطاليا)

الضخمة، الذكاء الاصطناعي والتكنولوجيات الجديدة الأخرى. وبتبني مفهوم الخصوصية حسب التصميم، يتم دمج التدابير التنظيمية والتقنية المناسبة اللازمة لضمان أمن وخصوصية البيانات الشخصية في دورة الحياة الكاملة لمنتجات المنظمة وخدماتها وتطبيقاتها وأعمالها وإجراءاتها والتقنية. ويمكن أن تشمل التدابير التقنية، على سبيل المثال لا الحصر، إخفاء الهوية وتقليل البيانات إلى أدنى حد.[159]

قدمت وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) ثماني استراتيجيات رئيسية لمساعدة الشركات على تطبيق مفهوم الخصوصية حسب التصميم بهدف دراسة الطرق المختلفة لإمكانية الوصول والاستراتيجيات والعوامل التقنية لحماية البيانات الشخصية.[160]

الجدول 3: الاستراتيجيات الرئيسية الثماني لتطبيق مفهوم الخصوصية حسب التصميم

	المبدأ	المضمون
1	التقليل للحد الأدنى	التقليل للحد الأدنى لكمية البيانات الشخصية المعالجة عن طريق المعالجة وفقاً للأغراض الواضحة بهدف تقليل احتمال انتهاك الخصوصية
2	الإخفاء	إخفاء نقل النص العادي عند معالجة البيانات الشخصية من أجل منع النفاذ إليها من الخارج
3	الفصل	فصل وتخزين مجموعة متنوعة من البيانات الشخصية لمنع التمييز ضد فرد واحد في قاعدة البيانات
4	التجميع	تجميع كميات كبيرة البيانات الشخصية عند المعالجة لتقليل التمييز ضد الأفراد وتصنيف نتائج المعالجة لجعل التمييز مستحيلاً
5	الإبلاغ	إبلاغ أصحاب البيانات عن العملية الكاملة لمعالجة البيانات الشخصية من أجل توفير فهم شفاف للأغراض التي تستخدم من أجلها البيانات
6	التحكم	التحكم في استخدام البيانات الشخصية. ويجب أن يفهم أصحاب البيانات العملية الكاملة لمعالجة البيانات الشخصية وأن يكونوا قادرين على ممارسة حقوقهم فيما يتعلق بالاستخدام غير المشروع لبياناتهم الشخصية أو مستويات الأمن بناءً على الإستراتيجية الخامسة، "الإبلاغ"
7	الإنفاذ	يجب أن تعكس سياسات حماية البيانات الشخصية الداخلية الواجبات القانونية والنظامية ويجب إنفاذها
8	الإثبات	إثبات الامتثال للالتزامات القانونية، مثل التطبيق الفعال لسياسات حماية البيانات الشخصية واتخاذ إجراءات فورية ضد الحوادث التي تنطوي على تسرب البيانات للخارج

قدمت وكالة الاتحاد الأوروبي للأمن السيبراني أيضاً اقتراحات لأنشطة حماية الخصوصية والبيانات التي يتعين على أصحاب المصلحة القيام بها. وتوصي بأن يقوم واضعو السياسات بتعزيز ودعم تطوير حوافز جديدة للنهوض بخدمات حماية البيانات الشخصية وأن تقوم أفرقة البحث والتطوير بدراسة الأساليب الهندسية لحماية البيانات الشخصية من خلال نهج متعدد التخصصات ونشر نتائج البحوث عبر واضعي السياسات ووسائل الإعلام. وأخيراً، توصي الوكالة بأن يوفر مطورو البرمجيات تكنولوجيا يمكنها تفعيل خصائص الخصوصية بشكل بديهي وتدعم حماية البيانات الشخصية في مشاريع البنية التحتية العامة والمنشأة بشكل متبادل.

وفي الولايات المتحدة، تؤكد لجنة التجارة الفيدرالية (FTC) على المبادئ العملية والإجرائية لحماية الخصوصية، مثل الخصوصية حسب التصميم، والاختيار المبسط للمستهلك، والمبادئ الموضوعية والإجرائية مثل الشفافية المضمونة. كما تؤكد اللجنة على حماية خصوصية المستهلك في تنظيم الأعمال والمنتجات وجميع مراحل تطوير الخدمات.[161]

---

159 الاتحاد الأوروبي. اللائحة 679/2016 (EU) الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات والتي تلغي التوجيه 95/46/EC (لائحة حماية البيانات العامة).

160 وكالة الاتحاد الأوروبي المعنية بأمن الشبكات والمعلومات. حماية الخصوصية والبيانات حسب التصميم – من السياسات حتى الهندسة. ديسمبر 2014.

161 لجنة التجارة الفيدرالية الأمريكية. حماية خصوصية المستهلكين في عصر سريع التغير: توصيات للشركات وواضعي السياسات. مارس 2012.

ونشرت هيئة حماية البيانات الإسبانية (AEPD) دليلاً للخصوصية حسب التصميم تؤكد فيه ضرورة مراعاة الخصوصية ومبادئ حماية البيانات منذ بداية أي نوع من أنواع المعالجة. ويقدم الدليل أيضاً المبادئ والاستراتيجيات الأساسية لمعالجة البيانات الشخصية.[162]

الجدول 4: الربط بين أهداف الخصوصية واستراتيجيات تصميم الخصوصية

أهداف حماية الخصوصية	استراتيجيات حماية الخصوصية المتمحورة حول البيانات	استراتيجيات حماية الخصوصية المتمحورة حول العمليات
عدم الارتباط	التقليل للحد الأدنى، التجريد، الفصل، الإخفاء	
التحكم		التحكم، الإنفاذ، الإثبات
الشفافية		الإبلاغ

3.6 الدروس المستفادة والمضي قدماً

يتزايد معدل الهجمات السيبرانية وخروقات البيانات والاستخدام غير المصرح به للبيانات الشخصية بشكل كبير. ومن المهم أكثر من أي وقت مضى، خاصة بالنسبة للمنظمات التي تتعامل مع المعلومات المحددة لهوية الأشخاص، فهم حقوق والتزامات الأفراد والمنظمات فيما يتعلق بالمعلومات الشخصية.

وقد عرض هذا الفصل لمحة عامة عن التغييرات القانونية والتدابير التقنية للأمن السيبراني فيما يتعلق بحماية البيانات الشخصية المطبقة في الدول الأعضاء. كما تناول أفضل الممارسات لمساعدة الدول الأعضاء على الامتثال لمتطلبات خصوصية البيانات المتطورة وتطرق إلى دور تكنولوجيات الأمن السيبراني في التخفيف من المخاطر ودعم الامتثال.

ويمكن استخلاص الدروس التالية من دراسة مختلف تكنولوجيات الأمن السيبراني وأفضل الممارسات التي تستخدمها الدول الأعضاء في حماية المعلومات الشخصية:

- تساعد الترتيبات المؤسسية الخاصة بالإخفاء والخصوصية حسب التصميم والتدابير التكنولوجية الأخرى في تهيئة بيئة أكثر أمناً.
- تحتاج الشركات التي تجمع المعلومات الشخصية وتستخدمها إلى بذل جهود نشطة لإدخال تدابير تقنية لحماية المعلومات الشخصية على مستوى أساسي أكبر.
- يحتاج أصحاب المصلحة المختلفون، بما في ذلك أصحاب البيانات والمجتمع المدني والأكاديميون وممثلو الصناعة، إلى مناقشة استخدام التكنولوجيا بشكل جماعي وبذل الجهود لزيادة الوعي وتحسين الأمن.

[162] *هيئة حماية البيانات الإسبانية (AEPD)*. دليل بشأن الخصوصية حسب التصميم. أكتوبر 2019.

الفصل 7 - مستقبل المسألة

الأمن السيبراني قضية مهمة لجميع أصحاب المصلحة، بما في ذلك الحكومات والمستهلكون. ويساعد العمل الذي يقوم به قطاع تنمية الاتصالات في هذا الصدد على إذكاء الوعي بالمخاطر. ومع استمرار ارتفاع أسعار التوصيلية واستخدام الإنترنت في جميع أنحاء العالم، تظل الحاجة إلى حماية المستهلكين والأنظمة مهمة. ونظراً لاستمرار الحاجة العالمية إلى تبادل المعلومات بشأن ممارسات الأمن السيبراني، يرى فريق إدارة المسألة 3/2 للجنة الدراسات 2 التابعة لقطاع تنمية الاتصالات أن المسألة بشأن قضايا الأمن السيبراني ينبغي أن تستمر كما هي في فترة الدراسة المقبلة. ولا تزال الموضوعات التي تم تناولها خلال فترة الدراسة الحالية مناسبة وينبغي أن تشكل الأساس لمزيد من المساهمات والعمل خلال فترة الدراسة المقبلة. لذلك ينبغي أن يظل الإطار العام للمسألة كما هو دون تغيير: نظراً لأن القضايا الأمنية تتعلق بجميع التكنولوجيات، فإن المسألة 3/2 تستمر في التطبيق على جميع التكنولوجيات الجديدة والناشئة، والتي تكون بطبيعتها مدمجة في تصميمها.

Annexes

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions on Question 3/2

Web	Received	Source	Title
2/407	2021-03-03	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/400	2021-03-01	United States	Update on Cyber Awareness Campaigns
2/385	2021-01-28	Bhutan	Survey findings on National Child Online Safety and Protection
RGQ2/278	2020-09-22	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs
RGQ2/268	2020-09-22	Republic of Korea	Protecting personal data in responding COVID-19 pandemic (Korea's experience)
RGQ2/261	2020-08-19	Togo	Draft text for Chapter 1 of the Final Report for Question 3/2- Update on the status of spam and malware, including mitigation responses
RGQ2/241	2020-08-26	United Kingdom	Updated case study on securing consumer Internet of Things (IoT) devices in UK
RGQ2/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme
RGQ2/234	2020-08-20	United Kingdom	UK case study- reporting service for phishing emails
RGQ2/216	2020-07-27	Brazil	Brazilian National Cybersecurity Strategy (E-Ciber)
RGQ2/215	2020-07-27	Brazil	#SafeConnection (#ConexãoSegura) Awareness Campaigns
RGQ2/214	2020-07-27	Brazil	Brazilian National Cyberdrill- Cyber Guardian Exercise
2/344	2020-02-11	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/342	2020-02-11	Republic of Korea	Korea's major amendment to data protection law and its implication
2/341	2020-02-11	Republic of Korea	Implementation plan for strengthening national cybersecurity of Korea
2/338	2020-02-11	Co-Rapporteur for Question 3/2	Draft table of contents (V1) for the Final Report of Q3/2
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility
2/328	2020-02-08	Deloitte (United States)	People with disabilities and the Internet of Things

(تابع)

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo
2/322	2020-02-07	Welchman Keen (Singapore)	Enhancing capacity and capability for critical national infrastructure in the Pacific Island Nations
2/321	2020-01-08	Sudan	WSIS project for consideration by Question 3/2
2/305	2020-01-15	Mexico	Perception on security and trust from Mexican users on fixed and/or mobile Internet
2/287	2020-01-07	China	Forum on network security technology development and international cooperation
2/286	2020-01-07	China	National Network Security Publicity Week and network security industrial park
2/272	2020-01-02	Niger	Cybersecurity best practices: case study and recommendation
2/264	2019-12-27	Russian Federation	Protecting children from information harmful to their health and development. Experience of the Russian Federation
RGQ2/TD/13 +Ann.1 (Rev.1)	2019-10-08	Forum of Incident Response and Security Teams (FIRST)	Introduction to incident response for policy makers
RGQ2/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills
RGQ2/179	2019-09-23	China	China's practice in protecting children's personal information
RGQ2/175	2019-09-19	United Kingdom	Follow up to "case study for the use of Active Cyber Defence on UK Government networks"
RGQ2/156 +Ann.1-3	2019-09-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK
RGQ2/153 +Ann.1-2	2019-08-22	United States	Enhancing the resilience of the Internet and communications ecosystem against botnets and other automated, distributed threats
RGQ2/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1
RGQ2/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus
RGQ2/143	2019-08-23	Brazil	The adoption of the Brazilian General Data Protection Law
RGQ2/135	2019-07-30	Bhutan	Cybersecurity initiatives in Bhutan

(تابع)

Web	Received	Source	Title
RGQ2/134	2019-07-29	State of Palestine, which participates in ITU under Resolution 99 (Rev. Dubai, 2018)	Government Data Exchange
RGQ2/118	2019-06-21	Democratic Republic of the Congo	Securing information and communication networks: Best practices for developing a culture of cybersecurity
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire
2/199 (Rev.1)	2019-03-06	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combatting Cybercrime (PLCC)
2/172	2019-02-07	NRD Cyber Security (Lithuania)	National and sectorial CSIRT developments as means to strengthen cybersecurity environments, 2019 update
2/168	2019-02-07	Republic of Korea	2019 Comprehensive Cybersecurity Plan for the private sector
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies
2/165	2019-02-06	Mexico	Fixed and/or mobile Internet users' perception of cybersecurity
2/156	2019-02-05	China	Work experiences in personal information protection
2/155	2019-02-05	China	Design of evaluation index for network security capability
2/154	2019-02-05	China	Experience of Internet governance with the coordinated participation of the whole of society
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin
2/141	2019-01-15	Chad	Digital dividend
2/140	2019-01-15	Chad	Vulnerability of connected TVs
2/136	2019-01-15	Chad	Status of cybersecurity in the Republic of Chad
RGQ2/TD/1	2018-09-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for ITU members
RGQ2/79	2018-09-18	Bhutan	Challenges, issues and recommendations from Bhutan: developing country perspective
RGQ2/75	2018-09-18	Namibia	Enforcement of cyber security challenged by cloud services

(تابع)

Web	Received	Source	Title
RGQ2/55	2018-09-10	United Kingdom	Case study for the use of Active Cyber Defence on UK government networks
RGQ2/47	2018-08-31	BDT Focal Point for Question 3/2	Information on two publications issued in 2017: regional review of national activities on child online protection in Europe; and mobile identification: implementation, challenges, and opportunities
RGQ2/39 +Ann.1	2018-08-20	High-Tech Bridge SA (Switzerland)	Cybersecurity awareness and other educative activities to members
RGQ2/32	2018-08-16	Guardtime AS (Estonia)	Towards cyber resilience - the role of national cyber exercises
RGQ2/30	2018-08-15	Brazil	Survey proposal
RGQ2/26	2018-08-14	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means of strengthen cybersecurity environments
RGQ2/25	2018-08-14	Proge-Software (Italy)	Data Privacy and Cloud.be compliant
2/91	2018-04-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/84	2018-04-23	Japan	Proposal for workshops in 2018-2021 study period
2/82	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	KOVA Project: A best practice for COP implemented in Iran
2/75	2018-04-14	A.S. Popov Odessa National Academy of Telecommunications (Ukraine)	ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. Conclusions and Recommendations
2/74	2018-04-13	Korea Telecom (Republic of Korea)	Study topics for Question 3/2 in the current study period
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities
2/66	2018-04-08	Algérie Télécom SPA (Algeria)	Proposals on the content of the (Question 3/2) final report
2/49	2018-03-15	Burundi	Current situation with regard to the Burundian Penal Code in relation to efforts to combat cybercrime
2/41	2018-02-28	Burundi	Cybersecurity, Internet Exchange point and e-commerce in Burundi

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
RGQ2/242	2020-08-31	Council Working Group on Child Online Protection	Liaison statement from the Council Working Group on Child Online Protection (CWG-COP) to ITU-D SG2 on the outcome of the 15th and 16th Meetings of CWG-COP
RGQ2/174	2019-09-18	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on vulnerability of TVs
2/182 +Ann.1	2019-02-11	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D Study Group 2 Question 3/2 on Cybersecurity in Africa (overview and outlook), from Democratic Republic of Congo
RGQ2/62	2018-09-14	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison representative with ITU-D Question 3/2
RGQ2/43	2018-08-27	ITU-T Study Group 13	Liaison statement from ITU-T SG13 to ITU-D SG1 Q3/1 and ITU-D SG2 Q3/2 on inter-sector coordination
RGQ2/3	2018-05-11	ITU-T JCA-IMT2020	Liaison Statement from JCA-IMT2020 to ITU-D Study Groups 1 and 2 on invitation to update the information in the IMT2020 roadmap
2/73	2018-04-13	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF to ITU-D Study Group 1 Q7/1 and Study Group 2 Q3/2 on JCA-AHF recent meeting reports
2/69	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison relationship with ITU-D Study Group 2 Question 3/2
2/68	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on best practices in Benin and Senegal
2/67 (Rev.1)	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/62	2018-04-03	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/46	2018-03-05	ITU-T JCA-IMT2020	Liaison Statement from ITU-T JCA-IMT2020 to ITU-D study groups on invitation to update the information in the IMT2020 roadmap
2/23	2017-11-24	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on an ongoing work item on technical framework for countering telephone service scam
2/10	2017-11-22	ITU-T Study Group 20	Liaison Statement from ITU-T SG20 to ITU-D study groups on work on the combat of counterfeit ICT devices and mobile device theft

Annex 2: List of lessons learned received on Question 3/2

Web	Received	Source	Title
SG2RGQ/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs

The UK Government provides targeted support to small and medium-sized enterprises (SMEs) to help them navigate complicated standards to better understand how to mitigate cyberrisk. This support is designed specifically for organizations who are not aware of the cyberthreat and have limited resources, both financially and in terms of technical capability. Lessons learned include the following:

– Clear and consistent cyberrisk management messaging is crucial. Critically, **awareness campaigns** should not just explain ***what*** businesses need to do and ***how*** they can actually carry out the action by pointing to government advice, guidance and support, but should draw attention to ***why*** they should do it.

– **Advice and guidance** is most effective when it is non-technical, size-specific and easy to access. Government and law enforcement should use national, regional and local networks, and work in partnership with key industry bodies, to identify levers and business touchpoints that can be used to amplify messaging, and ensure advice and guidance reaching SMEs.

– The creation of a government-backed **certification scheme** can be an effective intervention to support SMEs to improve their cybersecurity. The certification scheme can:

  • be quickly and effectively delivered by a single supplier if the government can outline the technical controls and/or minimum standards that should be covered;

  • evolve to continue to meet the needs of SMEs and address the changing threat landscape;

  • better ensure organizations remain compliant through having a certification expiry date and requiring annual recertification.

Web	Received	Source	Title
SG2RGQ/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme

Challenges

A range of interconnected challenges face governments in relation to traditional approaches to public procurement of ICTs, which is typically:

– neither understanding nor meeting the needs of users

– task oriented, risk averse and inflexible

– isolated from what happens:

  • **'before' (strategic planning, investment appraisals, early market engagement)**

  • **'after' (service delivery, monitoring and evaluation, supplier relationship management)**

– hidden from public scrutiny due to the poor quality, inconsistency, incompleteness and poor availability of data.

User-centred design approaches

Since GDS was established in 2011, it has incubated, embedded and mainstreamed new standards-based approaches to government transformation.

These approaches were first conceptualized by the Government Design Principles,[163] published in April 2012.

Since then, GDS and the government and UK public sector more broadly have been incrementally applying these principles to redesign and improve services, organizational structures, governance approaches, etc. This includes public procurement.

Social Purpose Digital Commissioning

Focus on culture, mindset, collaboration and capability, by:

- understanding users' needs
- being clear about the problems you are trying to overcome (e.g. legacy ICT, system vulnerabilities, capability and capacity, governance and accountability, etc.) to meet users' needs
- being outcome-oriented (rather than solution-oriented), experimental and flexible, making small incremental investments to try out different approaches to address users' problems, learning quickly and iteratively
- being multidisciplinary and collaborative coalition builders, advocating for systemic change through communities of practice
- engaging throughout the end-to-end lifecycle of delivery- the 'before' and 'after' of procurement
- being open to public scrutiny through deliberative participation of civil society, enabled by structured, quality, consistent, complete and published open data.

Web	Received	Source	Title
SG2RGQ/215	2020-07-27	Brazil	*#ConexãoSegura* (#SafeConnection) Awareness Campaigns

The campaign around personal data protection on the Internet reinforced the importance of telling consumers how to protect themselves in the digital environment. The interactions of consumers on digital media and on the website revealed that many of them have a number of doubts about what is fraud or scam- especially when it involves cash prizes, in addition to not knowing what to do when they are victims of these situations. It is also important to advise people not to post or publish personal data (surprisingly many people do not know what can happen). In the next initiative, it would be interesting to expand the dissemination of materials further in order to reach a wider audience.

[163] UK Government. Guidance. Government Design Principles. April 2012.

Web	Received	Source	Title
SG2RGQ/214	2020-07-27	Brazil	Brazilian National Cyberdrill - Cyber Guardian Exercise

The exercise started with two national critical infrastructure (NCI) sectors and evolved in its second edition to a broader and more complex exercise process. The exercise continues to evolve, and for its third edition (cancelled due to the COVID-19 pandemic) it was planned to include six NCI sectors and to add an international cooperation component to the exercise.

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo

Turn cybersecurity in the Democratic Republic of the Congo into a lever for integration, protection, good governance, economic growth and social progress.

This vision will make a significant contribution to building the country's capacity in its digital transformation (circulation of information, data economy, growth economy, transparency and traceability, interoperability of information systems, etc.). It will allow digitalization to become a key driver for modernizing the State, promoting economic growth and fostering social progress.

Web	Received	Source	Title
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK

A significant proportion of IoT devices do not have basic cybersecurity features built into them. Following 18 months of collaboration with industry and experts at the UK's National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS) published the Code of Practice (CoP) for Consumer IoT Security in October 2018. The 13 voluntary guidelines, as outlined in the 2018 CoP, provide a much-needed baseline for IoT devices that manufacturers should embed into their products to make them 'secure by design'.

These include:

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data are protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data.

These guidelines are outcome-focused as opposed to being prescriptive, which gives companies the space to come up with innovative solutions and appropriate ways to secure their products. Some devices might require enhanced security that is not included on this list and, as such, retailers and manufacturers are encouraged to secure their devices accordingly and seek solutions beyond the 13 guidelines. Action on the first three guidelines will bring largest security benefits in the short term.

Web	Received	Source	Title
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility

This document describes the consideration and implementation of cybersecurity measures for persons with disabilities, especially those with hearing difficulties, such as telecommunication relay service and remote captioning, to enhance accessibility to information and communication services.

Web	Received	Source	Title
SG2RGQ/134	2019-07-29	State of Palestine	Government Data Exchange

The central server issues certificates to security servers and provides a list of authenticated certificates to the systems connected to the Government Data Exchange. In addition, the central security server maintains encrypted activity data (hash logs) from the security servers to enable a series of e-service uses to be built subsequently, if necessary. If one of the parties to the service denies sending or receiving certain information, the service provider and user logs are compared with the encrypted copy in the central server. This method allows the integrity of security server logs to be checked, as it is impossible to change the log without it subsequently being detected.

The terms of the data-sharing process are defined by a memorandum of understanding signed by the two parties sharing the data and the Ministry of Telecommunications and Information Technology (MTIT), as third-party system operator. The memorandum includes an annex on the obligations of the parties, an annex on controls, standards and the duties and rights of each party, and an annex on the data which the two parties agree to share.

The system allows a connected ministry to determine which other connected institutions may access and read its data and the level of data that may be accessed. This is done by means of a control window on the ministry's own security server, enabling it to grant access rights to any of its services to the institutions it wishes.

Encrypted data are shared directly through secure servers from one information system to another. They do not pass through the central system and cannot be displayed there. The central system only has statistical information on the data shared.

Using this approach, the system facilitates the secure sharing of data between institutions, enabling them to share data between one another. It has also made it easier for the public to access services currently available G2G, by only going to one institution where the service involves more than one. MTIT is currently working to develop this mechanism and to provide services to the public directly via applications being developed.

Web	Received	Source	Title
SG2RGQ/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus

- Enhancing international cooperation, particularly between developed and developing countries.
- The school's regional nature helps to enhance cooperation among African countries.
- Covering all aspects of cybersecurity in both initial and continuing training.
- As cybersecurity is a prerequisite for the Digital Senegal 2025 Strategy (SN2025), classes have begun at the offices of the National School of Administration (ENA) while construction of the school's own premises is being completed at Diamniadio, 20 km from Dakar.
- The school will be the final element in the system for information system security and cybersecurity already in place.
- Boosting the fight against cybercrime in Africa.

Web	Received	Source	Title
SG2RGQ/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1

The recent update process to develop Version 1.1 of the Framework demonstrates an example of a good process for stakeholder engagement to ensure the Framework remains a useful tool for managing cybersecurity risk.

Web	Received	Source	Title
SG2RGQ/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

A recent advisory on ransomware from the National Cyber Security Centre (NCSC) recommends the following risk-mitigation techniques:

- Keep devices and networks up to date (e.g. prompt updating and patching, and regular scans)
- Prevent and detect lateral movement in your enterprise network
- Segment networks
- Set up a security monitoring capability
- Whitelist applications
- Use antivirus
- Back up files.

The full advisory and detailed list of recommendations can be found at: https://www.ncsc.gov.uk/news/ongoing-threat-organisations-ransomware

Protecting your organization from ransomware: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Mitigating malware: https://www.ncsc.gov.uk/guidance/mitigating-malware

Unfortunately, it is not a question of 'if' but 'when' a cyberattack will occur. In the event an attack does take place, cooperation between the public and private sectors is key to understanding the threat and coordinating a quick and effective response to mitigate the impact of an attack. In the event of an attack, organizations are advised to contact the National Crime Agency, NCSC's Cyber Incident Response, or Cyber Security Information Sharing Partnership (CiSP). NCSC led the UK's response to the WannaCry attack and worked in collaboration with the National Crime Agency (NCA). Over the course of an incident, NCSC publishes statements and guidance for large organizations as well as home users and small businesses. Up-to-date information is announced via the NCSC Twitter account (@NCSC).

Web	Received	Source	Title
SG2RGQ/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills

This contribution recommends the use of cyberrange technology (cloud-based – public or private cloud) and competency frameworks in the development and delivery of new generation cyberdrills.

Web	Received	Source	Title
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire

(تابع)

Web	Received	Source	Title
- De-dramatize prevention by banishing the anxiety-provoking approach. Internet prevention can be part of a fear culture. However, this increases the anxiety of parents who are already worried about a technology they do not understand well, thereby undermining the extraordinary learning tool that is the Internet. - Encourage educational programmes aimed at developing best practices in content management and raising children's awareness of responsible use of the Internet. - Put an Internet portal online in order to provide children, adolescents, parents and teachers with an educational base. - Involve all stakeholders in community-awareness activities: government agencies, the private Internet sector, NGOs, community groups and the general public.			

Web	Received	Source	Title
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire
Statistics should be collected on complaints and damages (financial, moral).			

Web	Received	Source	Title
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combating Cybercrime (PLCC)
– Development of partnerships between bodies responsible for combating cybercrime and the police in developing countries – Awareness-raising in schools – Collaboration with equivalent organizations in other countries.			

Web	Received	Source	Title
SG2RGQ/26 2/172	2018-08-14 2019-02-07	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means to strengthen cybersecurity environments (2018 +2019 update)
For national digital security success, CSIRTs should focus substantial energy on broad facilitation for developing additional independent capabilities – in industries, professional communities, education centres, research, events, meet-ups and conferences, private and internal CSIRTs.			

Web	Received	Source	Title
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies
- Establish and adopt situation awareness and threat intelligence policies. - Develop incident analysis and response capabilities- establish CERTs. - Develop collaboration with the private sector and information-sharing policies (public-private partnerships).			

Web	Received	Source	Title
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin

Benin calls on ITU-D Study Group 2 to support:

- the establishment of a national CERT in Benin to enhance the level of trust in cyberspace;
- the building up of a common African security and defence policy;
- the creation of a panel of eminent personalities to reflect on Africa's role in regard to security;
- the establishment of a CERT-AFR (for Africa) along the lines of CERT-EU (for the European Union);
- a coordinated effort to avoid disparities between the strategies adopted and means deployed by Member States in terms of military cyberdefence capabilities;
- regulators and ICT authorities as they seek to:
  - **adopt measures designed to enhance the security of information systems and networks;**
  - **create reliable digital identities;**
  - **protect minors and vulnerable groups; and**
  - **foster transparency.**

Web	Received	Source	Title
SG2RGQ/25	2018-08-14	Proge-Software [*SME pilot*] (Italy)	Data Privacy and Cloud- be compliant

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) (EU) 2016/679 governs data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU. Superseding Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personally identifiable information (personal data) of individuals (formally called data subjects in the GDPR) inside the European Union, and applies to an enterprise that is established in the EU or – regardless of its location and the data subjects' citizenship – that is processing the personal data of people inside the EU. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data-protection principles. Severe penalties are applied to violators.

Cloud computing

In computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or how it is transported. Periodically they pay for what they have consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power or specially crafted development environments without having to worry how these work internally. Cloud computing is usually Internet-based computing. According to a paper published by IEEE Internet Computing in 2008, "***Cloud computing is a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include computers, laptops, handhelds, sensors, etc.***".

Web	Received	Source	Title
SG2RGQ/32	2018-08-16	Guardtime AS [*SME pilot*] (Estonia)	Towards cyber resilience – the role of national cyber exercises

Cyberexercises are essential to achieving sustainable cyberresilience. Cyberexercises are different from training, and must be customized, realistic and engaging. Governments should consider developing a programme to govern cyberresilience, covering education, training and cyberexercises ranging from localized events to customized national-scale exercises conducted on a regular basis.

Web	Received	Source	Title
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities

1. Contact the service provider to inform it of the highjacking of your e-mail address.
2. Try to give information on the spammer's/hacker's contact details with an example e-mail, e.g. by forwarding the suspect e-mail to its fraud section.
3. Ask to have your violated e-mail blocked.
4. Change your e-mail address.
5. Let your friends and contacts know you have been hacked and give them the new address.
6. Do not click on any web addresses unless you have verified it is in fact from a known source.

Web	Received	Source	Title
2/41	2018-02-28	Burundi	Cybersecurity, Internet exchange point and e-commerce in Burundi

Security of IT data and of communication networks in order to ensure high-quality services is the pillar of ICT-sector development. A legal and regulatory framework for cybersecurity in our country is an essential tool for implementing all aspects of data security. The introduction of an Internet exchange point facilitates local communications and reduces latency times and associated costs. Lastly, domain name management provides facilities for investors. Data security will thus enable us to ensure reliable e-transactions and retain our customers.

الاتحاد الدولي للاتصالات (ITU)
مكتب تنمية الاتصالات (BDT)
مكتب المدير

Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

مكتب نائب المدير ودائرة تنسيق العمليات الميدانية للحضور الإقليمي (DDR)

Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

دائرة الشبكات الرقمية والمجتمع الرقمي (DNS)

Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

دائرة محور المعارف الرقمية (DKH)

Email bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

دائرة الشراكات من أجل التنمية الرقمية (PDD)

Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

إفريقيا

إثيوبيا

المكتب الإقليمي للاتحاد

Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa - Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

الكاميرون

مكتب المنطقة للاتحاد

Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé - Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

السنغال

مكتب المنطقة للاتحاد

8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff - Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

زيمبابوي

مكتب المنطقة للاتحاد

TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare - Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

الأمريكتان

البرازيل

المكتب الإقليمي للاتحاد

SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF - Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

بربادوس

مكتب المنطقة للاتحاد

United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown - Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

شيلي

مكتب المنطقة للاتحاد

Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

هندوراس

مكتب المنطقة للاتحاد

Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa - Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

الدول العربية

مصر

المكتب الإقليمي للاتحاد

Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

آسيا – المحيط الهادئ

تايلاند

المكتب الإقليمي للاتحاد

Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi - Bangkok 10210 - Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

إندونيسيا

مكتب المنطقة للاتحاد

Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110 - Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

كومنولث الدول المستقلة

الاتحاد الروسي

المكتب الإقليمي للاتحاد

4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

أوروبا

سويسرا

الاتحاد الدولي للاتصالات (ITU)
مكتب أوروبا (EUR)

Place des Nations
CH-1211 Geneva 20 - Switzerland

Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

الاتحـاد الـدولي للاتصـالات
مكتب تنميـة الاتصـالات
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-34106-0
9 789261 341060

نُشرت في سويسرا
جنيف، 2021