ممارسات ضمان الأمن السيبراني

فترة الدراسة

2025-2022

المسألة 2/3

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

ناتج مؤقت لعام 2023

ملخص تنفيذي

استعرض المؤتمر العالمي لتنمية الاتصالات الذي عقد في كيغالي عام 2022 ولاية مسألة الدراسة 2/3 التي تركز على تبادل الخبرات بشأن ممارسات الأمن السيبراني. وتشكل تهديدات الأمن السيبراني مصدر قلق كبير على الصعيد العالمي، حيث يؤدي الاعتماد المتزايد على التكنولوجيا إلى تصعيد مخاطر الهجمات السيبرانية وعواقبها. وقد برزت ممارسات ضمان الأمن السيبراني كعنصر حاسم في حماية الشبكات والأنظمة والبيانات من الأنشطة الضارة.

ويبين هذا التقرير المساهمات والمناقشات التي دارت في اجتماعات فريق إدارة المسألة 2/3 وورشة عمل مخصصة بشأن ممارسات ضمان الأمن السيبراني. وترد أدناه ستة سيناريوهات رئيسية مستخلَصة من هذه المناقشات:

1 تتطلب المستويات المختلفة من الحراجة والمخاطر مستويات مختلفة من الضمان. ويمكن لتقييم المخاطر أن يساعد في تحديد مستوى الضمان المناسب الذي يراعي حساسية البيانات والأصول الجارية حمايتها، وعواقب الخرق، فضلاً عن بيئة التهديدات.

2 يمكن أن يكون التعاون مع المنظمات الشريكة ودوائر الصناعة وأصحاب المصلحة المتعددين وسيلة فعّالة لدفع عجلة ضمان الأمن السيبراني. ويمكن للتعاون بين صانعي السياسات ومنظمات المجتمع المدني ودوائر الصناعة أن يعزز الطلب على الأمن وأن يرشد التطوير السياساتي والتنظيمي.

3 النظر في نهج تنظيمي متطور، يستنير من خلال الحوار والمشاورات. ويمكن إدخال ممارسات ضمان الأمن السيبراني بصورة طوعية قبل أن تصبح إلزامية، تبعاً للحاجة إلى تدابير أقوى للحماية من الهجمات السيبرانية.

4 وفي ضوء مشهد التهديدات الدينامي ومخاطر الأمن السيبراني الناشئة، تنبغي إعادة النظر في ممارسات ضمان الأمن السيبراني وتكييفها على مر الزمن. وتعتبر المراجعات الداخلية المنتظمة والاشتراك في الاستخبارات عن التهديدات من الممارسات السليمة.

5 تُبذل جهود لتثقيف المستهلكين والمصنعين بشأن أهمية الأمن السيبراني وفوائد اختيار منتجات أكثر أمناً. ويمكن لمخططات وسم الأمن السيبراني وحملات التوعية أن تساعد في إعلام المستعملين بأمن منتجات التكنولوجيا.

6 يمكن لاتفاقات المعاملة بالمثل أن تساعد في تسهيل الالتزام للجهات الفاعلة الصناعية العاملة في أسواق متعددة، في حين أن تنسيق متطلبات الأمن الأساسي يقلل من الأعباء التنظيمية على مقدمي المنتجات والخدمات.

مقدمة

خلال المؤتمر العالمي الأخير لتنمية الاتصالات الذي عُقد في كيغالي، رواندا في يونيو 2022، استُعرضت ولاية مسألة الدراسة 2/3 - تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني، وشملت إحدى القضايا المحددة للدراسة "تبادل الخبرات بشأن ممارسات الأمن السيبراني"[1].

وتعترف الاختصاصات المعتمدة لمسألة الدراسة 2/3 بأن تهديدات الأمن السيبراني لا تزال تشكل مصدر قلق كبير للحكومات والمنظمات والأفراد في جميع أنحاء العالم. ومع تزايد الاعتماد على التكنولوجيا، تتصاعد أيضاً المخاطر والعواقب المحتملة للهجمات السيبرانية، مع تزايد ربحية الهجمات السيبرانية.[2] ويشغِّل المجرمون السيبرانيون أعمالاً مربحة تقدر تكلفتها بنحو 8 تريليون دولار أمريكي في جميع أنحاء العالم[3].

وقد برزت ممارسات ضمان الأمن السيبراني[4] كعنصر حاسم في حماية الشبكات والأنظمة والبيانات من الأنشطة الضارة. وهي تشير بوجه عام إلى الإجراءات المستخدمة لضمان وجود ضوابط ذات صلة لحماية سرية وسلامة وتيسر الأجهزة والأنظمة والشبكات والبيانات الإلكترونية. وبالرغم من أنها لا تمنع الهجمات السيبرانية مباشرةً، فإن هدفها، إذا نُفذت على الوجه الصحيح، هو تقليل خطر هذه الهجمات إلى أدنى حد. ويمكن التحقق من ممارسات ضمان الأمن السيبراني قياساً بضوابط ومبادئ توجيهية ومعايير أمنية محددة ويمكن أن تفرضها اللوائح أو تعتمدها دوائر الصناعة طواعية. ولكن لا يوجد نهج واحد يناسب الجميع، حيث تستخدم السلطات الوطنية وهيئات تنظيم القطاعات في كثير من الأحيان ممارسات مختلفة تتراوح بين التقييم الذاتي والمبادئ التوجيهية الطوعية وصولاً إلى مخططات الوسم وعمليات التحقق الصارمة من الالتزام.

وعلى الرغم من عدم وجود نهج واحد يوصى به، يتضح وجود تحول مستدام نحو اعتماد ممارسات ضمان الأمن السيبراني في جميع أنحاء العالم في السنوات والأشهر الماضية، بتطورات مختلفة في عدة بلدان ومناطق. وكمثال على هذا الزخم، أطلقت منظمة التعاون والتنمية في المجال الاقتصادي في ديسمبر 2022 توصية المجلس بشأن الأمن الرقمي للمنتجات والخدمات وهي توصي باعتماد سياسات لتعزيز الأمن الرقمي للمنتجات والخدمات بما يتناسب المخاطر، بدءاً بنهج خفيف يقوم على تدابير سياساتية طوعية، واستكشاف الحاجة إلى تدابير إلزامية[5].

ويبين هذا التقرير المساهمات والمناقشات التي دارت في اجتماعات فريق إدارة مسألة الدراسة 2/3 وورشة عمل مخصصة بشأن ممارسات ضمان الأمن السيبراني. وأتاحت ورشة العمل العامة، التي استمرت يوماً كاملاً والتي عُقدت في جنيف يوم 23 مايو 2023، فرصة لاستكشاف المشهد العالمي لضمان الأمن السيبراني في مختلف الميادين (إنترنت الأشياء (IoT) والاتصالات وغيرها) من خلال عرض مجموعة من الممارسات والأصوات المستمرة من جميع أنحاء العالم. وجمعت ورشة العمل بين دول أعضاء وممثلين عن دوائر الصناعة وسلطات تقنية فضلاً عن ممثلي المجتمع المدني.

ويود فريق إدارة المسألة 2/3 أن يغتنم هذه الفرصة ليشكر جميع المتحدثين والمساهمين على مساهماتهم القيمة بشأن هذا الموضوع. فما كان لهذا المسعى أن يتسنى بدون التزامهم.

وفي ضوء المساهمات القيمة المتلقاة، ينقل جل هذا التقرير التحديات التي اعترضتهم والتأثيرات التي قُيمت والدروس المستفادة حتى الآن عند النظر في ممارسات ضمان الأمن السيبراني وتنفيذها من خلال عرض ستة استنتاجات.

ويمكن أن تكون هذه الاستنتاجات بمثابة مدخلات هامة لأعضاء الاتحاد من أجل تقييم ممارساتهم القائمة وتقييم الحاجة إلى اعتماد نُهج إضافية أو مختلفة، مع مراعاة التجارب والدروس المستفادة من الإدارات والمنظمات الأخرى.

الاستنتاج 1: المستويات المختلفة من الحراجة والمخاطر تتطلب مستويات مختلفة من الضمان

عند النظر في تنفيذ ممارسات ضمان الأمن السيبراني، من الأهمية بمكان أولاً تحديد ما الذي يحاول كيان حمايته والمخاطر التي تواجهها الأصول المحددة. وينبغي للبلدان والشركات التي ترغب في الحماية من الهجمات السيبرانية، كأولوية، أن تحدد الأنظمة والأصول التي تحتاج إلى الحماية وأن تقيِّم مواطن ضعفها. وفي هذا الصدد، يعد وجود مخطط لإجراء تقييمات المخاطر أداة مؤازرة. ومن أشهر الأطر إطار الأمن السيبراني لدى المعهد الوطني للمعايير والتكنولوجيا (NIST)[6]، الذي يخضع حالياً للتحديث،[7] وهو يوفر نهجاً يستخدم على نطاق واسع للمساعدة في تحديد المخاطر التنظيمية وتقليلها إلى أدنى حد. وهو يضع مبادئ توجيهية غير تنظيمية تتيح للمنظمات على الصعيد العالمي تبيُّن مشهد المخاطر الخاصة بها وتطبيق ضوابط الأمن السيبراني المناسبة فيما يتعلق بذلك. ويعتمد الإطار المراجَع، بسبب أنه سيُستكمل في أوائل عام 2024، على التعامل الواسع وطويل الأجل مع مجتمع أصحاب المصلحة الذين يستخدمون هذه المبادئ التوجيهية، فضلاً عن المواءمة المستمرة مع المعايير الدولية الأخرى.

1 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/ToR/Q3-2.aspx#Question

2 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090023PDFE.pdf

3 https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023

4 يرتبط الأمن التشغيلي ارتباطاً وثيقاً بممارسات ضمان الأمن السيبراني، حيث يمكن للأمن التشغيلي أن يوفر أساساً جيداً لممارسات الضمان. وعرضت شركة Broadcom، في شخص نائب رئيس لجنة الدراسات 17 لقطاع تقييس الاتصالات، نموذج الظروف الجيدة مسلطة الضوء على أنها تتألف من أربعة عناصر رئيسية هي: الأشخاص والعمليات، والمعرفة، ومنتجات الأمن (الأمن الخارجي) والأمن في الأصول (الأمن الداخلي). انظر "تقليل المخاطر وحماية السمعة"، https://www.itu.int/md/T22-SG17-C-0214/en

5 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

6 https://www.nist.gov/cyberframework

7 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

وفي ورشة العمل، سلط ممثل المعهد الضوء على حقيقة أن الوضع المفيد للمنظمة بوصفها وكالة غير تنظيمية سمح بانخراط أعمق مع أصحاب المصلحة في دوائر الصناعة من جميع أنحاء العالم لفهم التحديات الحقيقية وتلقي التعقيبات التي أدرجت في المبادئ التوجيهية الجديدة.[8] والغرض منها أن تكون قابلة للتكيف ومرنة وقابلة للتطبيق على جميع المنظمات والقطاعات. وتحدثت شركة BitSight، وهي عضو من القطاع الخاص في قطاع تنمية الاتصالات، عن منصتها التي تتضمن إطار الأمن السيبراني لدى المعهد الوطني للمعايير والتكنولوجيا (NIST)، وقد استخدمتها مختلف الوكالات الحكومية المسؤولة عن الأمن السيبراني (مثل أفرقة الاستجابة للطوارئ الحاسوبية (CERT) والوكالات الوطنية للأمن السيبراني ومنظمي الاتصالات).[9] ومن خلال هذه المنصة، يمكن للبلدان إجراء تقييمات للمخاطر التي تهدد ما تعتبره بنيتها التحتية وأصولها الحرجة وقياس عوامل المخاطرة الخاصة بها.

ويمكن لتقييم المخاطر أن يساعد أيضاً في تحديد مستوى الضمان المناسب بمراعاة حساسية البيانات والأصول الجارية حمايتها، والعواقب المترتبة على الخرق وكذلك بيئة التهديد (أي ما إذا كان كيان ما معرضاً لهجمات سيبرانية). وفي بعض الحالات، ستملي المتطلبات التنظيمية مستويات الضمان. وكلما ارتفع مستوى الضمان، كانت الضوابط الأمنية أكثر صرامةً. فعلى سبيل المثال، قد يتطلب مستوى منخفض من الضمان كلمة مرور للنظام أو جدار حماية بينما يتطلب مستوى أعلى من الضمان إضافة ضوابط أكثر تقدماً مثل التجفير المتقدم والاستيقان المتعدد العوامل.

وبالرغم من أن ممارسات ضمان الأمن السيبراني تضيف إلى ميزانيات تكنولوجيا المعلومات، فإن التقاعس عن وضع ضوابط أمنية يمكن أن يكون أكثر تكلفةً. وخلال ورشة العمل، حث الممثلون الحضور على التفكير في تكاليف المعاناة من هجوم سيبراني ليس من مجرد الناحية المالية: إذ يمكن أن تكون التكلفة الإضافية للسمعة أشد ضرراً بكثير. فلفقدان ثقة العملاء والمواطنين تأثير طويل الأجل يمتد إلى ما هو أبعد من المال ويجب أن تكون المنظمات قادرة على فهم ذلك استراتيجياً. وبالمثل، بالنسبة للقطاع العام، قد تؤثر الهجمات الناجحة على تقديم الخدمات العامة والأنشطة الحرجة التي لا يمكن أيضاً تقييم تعطلها من مجرد الناحية المالية، لأنها تؤثر على حياة المواطنين.

الاستنتاج 2: يمكن أن يكون التعامل مع المنظمات الشريكة ودوائر الصناعة وأصحاب المصلحة المتعددين وسيلة فعّالة لدفع عجلة ضمان الأمن السيبراني

أولاً، من المهم مقارنة المبادرات بالمبادرات الأخرى لفهم أفضل الممارسات والتعلم من نجاح الآخرين وأخطائهم أثناء إعداد المبادرات. ثانياً، من المهم التعامل مع العديد من أصحاب المصلحة، بما في ذلك دوائر الصناعة، للحصول على رؤى هامة بشأن المبادرة نفسها كجزء من التطوير.

وبالرغم من أن ممارسات ضمان الأمن السيبراني أصبحت أكثر ضرورة في البلدان الأقل نمواً، فقد لايزال من الصعب تطبيقها. وأوضح ممثل شركة الدفاع السيبراني عن إفريقيا (CDA) في توغو التحديات التي تواجه السوق المحلية في تقديم ضمان الأمن السيبراني عبر مشغلي الخدمات الأساسية (ESO).[10] وقد استُشهد بالافتقار إلى التمويل، وانعدام الثقة في الحكومة كمقدم للخدمة، والافتقار إلى القدرات البشرية والمرافق المحلية، كبعض العوامل التي ووجهت. ولدعم مشغلي الخدمات الأساسية في الالتزام بضوابط الأمن السيبراني المنشورة حديثاً، أنشأت حكومة توغو شراكة بين القطاعين العام والخاص مع مقدم كبير مرموق للأمن السيبراني لتقديم خدمات الأمن السيبراني ضمن القطاعين العام والخاص. ومن خلال هذا النموذج، أنشأت توغو شركة الدفاع السيبراني عن إفريقيا (CDA) بوصفها مقدماً محلياً للأمن السيبراني مكتفياً ذاتياً وعالي الجودة لدعم مشغلي الخدمات الأساسية على أساس غير إلزامي. وسمح نموذج الاكتفاء الذاتي المستخدم لتوغو لمواجهة التحديات الكثيرة المذكورة أعلاه والبدء في تعزيز المواهب المحلية في مجال الأمن السيبراني، فضلاً عن تشجيع تنمية السوق المحلية. وأشار ممثل شركة الدفاع السيبراني عن إفريقيا (CDA) إلى أهميتها ككيان خاص في سوق تنافسية من أجل ضمان قابلية التكيف وعلو جودة الخدمات والتسعير التنافسي.

ومن المهم أيضاً تعزيز التعاون بين واضعي السياسات الذين قد يحددون البيئة التنظيمية ومنظمات المجتمع المدني التي يمكن أن تعزز الطلب على الأمن، وكذلك توجيه التطور السياساتي والتنظيمي على أساس الممارسات الإقليمية والدولية القائمة المحددة. فعلى سبيل المثال، شركة DiploFoundation هي منظمة دولية تقدم برامج تدريبية وبناء القدرات للحكومات والهيئات التنظيمية والأعمال التجارية والمجتمع المدني بشأن مسائل الساعة المتعلقة بالأمن السيبراني، وهي تشارك في حوار جنيف بشأن السلوك المسؤول في الفضاء السيبراني (حوار جنيف).[11] وفي عام 2020، أنتج حوار جنيف مجموعة من الممارسات الجيدة[12] التي تشمل التعاريف المقترحة للتصميم الآمن وإدارة مواطن الضعف، ونمذجة التهديدات، وأمن الطرف الثالث وسلسلة التوريد، والتنمية الآمنة، وإدارة مواطن الضعف والكشف عنها، فضلاً عن الثقافة التنظيمية. والمنتدى العالمي للخبرات السيبرانية (GFCE) هو منصة دولية تدعم تنسيق المشاريع وتعزيز تبادل المعارف والخبرات ومطابقة الطلبات مع عروض دعم بناء القدرات وتطوير المشاريع البحثية.[13] وأنشأ المنتدى أربعة محاور إقليمية في جزر المحيط الهادئ وإفريقيا والأمريكتين والبحر الكاريبي وجنوب شرق آسيا. ونظراً إلى رقعته العالمية، والدعم المتنوع الذي يقدمه في البلدان النامية،

[8] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090017PDFE
[9] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090024PDFE
[10] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090025PDFE
[11] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090020PDFE
[12] https://genevadialogue.ch/goodpractices/
[13] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090021PDFE

فإنه في وضع جيد لطرح وجهات نظر أكثر تنوعاً على الصعيد الإقليمي بشأن احتياجات بناء القدرات السيبرانية ومتطلباتها. ولدى المنتدى بوابة إلكترونية تستخدم كمستودع للمشاريع الجارية المنفَّذة في مجال بناء القدرات السيبرانية، على الصعيد العالمي، فضلاً عن الموارد والأدوات. وتساعد هذه البوابة أيضاً على تقليل ازدواجية الجهود وتساعد على تحديد بعض البرامج أو الثغرات والأنماط في تقديم بناء القدرات.

الاستنتاج 3: النظر في نهج تنظيمي متطور يستنير من خلال الحوار والمشاورات

في كثير من الحالات، ستُدخل ممارسات ضمان الأمن السيبراني بصورة طوعية قبل أن تصبح إلزامية. ويحدث التحول عادة عندما ترى الحكومات أن دوائر الصناعة لا تفعل ما يكفي لتأمين المنتجات وأن المستهلكين لا يملكون بالضرورة المعرفة اللازمة لتقييم ما إذا كانت المنتجات آمنة أم لا. ويمكن أن يؤدي ذلك بالحكومات والسلطات الوطنية إلى التصرف والنص على ممارسات الضمان التي تتوقع أن تلبيها دوائر الصناعة. ففي البرازيل، على سبيل المثال، أنشأت هيئة تنظيم الاتصالات، Anatel، نظاماً لهيئات إصدار الشهادات ومختبرات الاختبار داخل البلد لإصدار الشهادات لمعدات منشآت العملاء (CPE)، أو البوابات المنزلية). كان نهج الوكالة الوطنية للاتصالات (Anatel) تقليدياً يتمثل في تزويد قطاع الاتصالات بمبادئ توجيهية طوعية للأمن السيبراني. ولكن تبين من خلال إجراء تقييمات للمخاطر أن التوصيات ليست كافية لمعدات منشآت العملاء، بالنظر إلى مواطن الضعف والتهديدات المرتبطة بهذا النوع من المعدات، وأن الضرورة تقتضي وضع متطلبات إلزامية دنيا لسلامة هذه المنتجات. وقد نشرت هذه المتطلبات الإلزامية لمقدمي خدمات الاتصالات (CSP) في أوائل عام 2023 وهي تركز على مواطن الضعف مثل كلمات المرور غير الآمنة وأجزاء الخدمة الممكّنة بلا داع. وستصبح المتطلبات سارية في أوائل عام 2024 كجزء منّ الاختبارات المختبرية الإلزامية للموافقة على المنتجات[14]. وأوضحت الوكالة الوطنية للاتصالات أن التطور من نهج غير إلزامي إلى متطلبات الشهادة الإلزامية للأمن السيبراني لمجموعة محددة من المعدات ما كان ليتسنى إلا بعد مناقشة شاملة مع القطاع.

وبالمثل، عرضت الهيئة الوطنية للأمن السيبراني (NCA) بالمملكة العربية السعودية مبادرتها لبناء نظام إيكولوجي مستقل للتحقق وإقرار الصلاحية (IV&V)[15] لاختبار واعتماد منتجات من منظور ضمان الأمن السيبراني على المستوى الوطني في المملكة العربية السعودية. وتهدف المبادرة أيضاً إلى تحديد وتصنيف العتاد والبرمجيات التي تتسم بدرجة عالية من الحساسية للمخاطر والتهديدات السيبرانية. وهي تسعى كذلك إلى المساهمة في تطوير القدرات البشرية في مجال التحقق وإقرار الصلاحية. وتنظر خارطة طريق المبادرة في البدء ببرنامج طوعي قبل أن تجعله التزاماً إلزامياً. وأشارت الهيئة الوطنية للأمن السيبراني أيضاً إلى أهمية أن يصبح مثل هذا النظام البيئي "مستداماً ذاتياً" في نهاية المطاف، واضاء ذلك الطريق لنهج الهيئة في تشجيع أصحاب المصلحة في السوق على إجراء مثل هذه التقييمات.

وفي ميدان أمن إنترنت الأشياء، تقدم المملكة المتحدة أيضاً دراسة حالة للتطور من نهج طوعي إلى نهج إلزامي. وفي السنوات الأخيرة، قررت المملكة المتحدة، من خلال التشريعات، فرض متطلب أمني أساسي لمنتجات إنترنت الأشياء الاستهلاكية استناداً إلى معيار المعهد الأوروبي لمعايير الاتصالات، ETSI 303 645، وهو أول معيار للأمن السيبراني قابل للتطبيق عالمياً لأجهزة إنترنت الأشياء الاستهلاكية. ففي المملكة المتحدة، سيتعين على المصنعين والمستوردين والموزعين الالتزام بثلاثة من المبادئ التوجيهية الأمنية الثلاثة عشر الصادرة عن المعهد الأوروبي لمعايير الاتصالات (ETSI)، ويخول القانون الحكومة صلاحيات لاعتماد متطلبات إضافية عند الضرورة، تبعاً لتقييمات التهديد المنتظمة. وقد جاء قرار فرض خط أساس للمتطلبات الأمنية بعد فترة من الاعتماد الطوعي. وفي عام 2018، وضع البلد مدونة ممارسات[16] طوعية لأمن إنترنت الأشياء للمستهلك، ولكن التزام دوائر الصناعة لم يكن على النحو المتوقع. وبينت الأدلة التي جمعت من خلال عمليات التشاور أن المستهلكين يثمنون الأمن وأنهم على استعداد لدفع علاوة سعرية لقاء المنتجات المأمونة. ولكن التهديدات الأمنية لا تخضع لنفس مستوى التنظيم القوي الذي تخضع له سلامة المنتجات، مما يؤدي إلى نقص الشفافية من جانب المصنعين وبطء اعتماد السياسات الأمنية. وتوصلت الأدلة أيضاً إلى أن سوق المنتجات الاستهلاكية القابلة للتوصيل لا يشجع اعتماد الميزات الأمنية الأساسية، لأن المستهلكين يفترضون في الغالب أن المنتجات آمنة أصلاً. ويرمي النظام إلى معالجة هذه الفجوة بفرض عناصر مدونة الممارسات لضمان إدراك المصنعين لمواطن الضعف واتخاذ خطوات للتخفيف منها. وسيدخل نظام أمن المنتجات والبنية التحتية للاتصالات (PSTI) حيز النفاذ في أبريل 2024 وسيطبق على أي منتج استهلاكي يمكنه التوصيل بالإنترنت[17].

ومن التحديات التي تحدَدت، التأثير الممكن على المشاريع الصغيرة والصغيرة جداً التي قد تواجه صعوبات في الالتزام بالنظام الجديد. وتعكف سلطة الإنفاذ في المملكة المتحدة على وضع إرشادات للتخفيف من أي تأثير غير متناسب. وبالإضافة إلى العمل مع دوائر الصناعة، أفادت المملكة المتحدة بأن المتطلبات الثلاثة الأولى المزمع فرضها في الخطة قد تحدَدت وأُعلنت بشفافية لعدة سنوات. وعلى مر السنين، أجرت المملكة المتحدة تمارين بشأن عملية تنفيذ النظام، بما في ذلك متطلبات كلمة المرور، والمعمارية الأساسية، للمنتج والتعرض للثغرات الأمنية، ومتطلبات الشفافية الأمنية. وقد أظهر تقييم التأثير أن الفوائد الإجمالية لخفض حجم الهجمات السيبرانية على المستهلكين والشركات يُتوقع أن تتجاوز التكاليف المرتبطة بالنظام. وبما أن نظام أمن المنتجات (PSTI) لعام 2022 هو أول تشريع إلزامي لمنتجات الأمن السيبراني

[14] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090018PDFE
[15] https://nca.gov.sa/en/news?item=535
[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
[17] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090014PDFE

في العالم، فإن تكلفة إنفاذ النظام غير مؤكدة، ولكن التقديرات الأولية تشير إلى أن التمويل المخصص سيكون كافياً.

وفي بعض الحالات، يتحدد التمييز بين فرض ممارسة الضمان أو إبقائها طوعية من خلال هوية المستعمل أو العميل. فعلى سبيل المثال، أطلقت جمهورية كوريا برنامجها لضمان الأمن السحابي (CSAP)، وهو شهادة أمنية لخدمات الحوسبة السحابية.[18] وبصفة عامة، تكون شهادة CSAP طوعية. ولكن يتعين على العملاء في القطاع العام (أي الوكالات العامة) استخدام خدمة سحابية حاصلة على شهادة CSAP وفقاً للوائح ذات الصلة، وبالتالي يتعين على مقدمي الخدمات السحابية الحصول على شهادة عند تقديم الخدمات السحابية للوكالات العامة.

الاستنتاج 4: نظراً لمشهد التهديد الدينامي ومخاطر الأمن السيبراني الناشئة، لا يمكن لممارسات ضمان الأمن السيبراني أن تبقى ساكنة وتلزم مراجعتها وتكييفها بمرور الوقت

يعتبر إجراء عمليات مراجعة داخلية منتظمة يمكنها أن تساعد على تحديد الثغرات في الضوابط ومخاطر التعرض، فضلاً عن الاشتراكات في المعلومات الاستخبارية عن التهديدات، من الممارسات السديدة. وحتى في حال اعتماد منتج ما، فإنه قد يعاني، على مدى دورة حياته، من عيوب أمنية. وتتطلب خطة إصدار الشهادات تقديم المعلومات في وقت محدد، وهي لا تحتسب للتغيرات الدينامية في التهديدات مستقبلاً. وأظهرت دراسة حديثة أجرتها شركة BitSight وجود علاقة قوية بين ضعف "إيقاع الترقيع التصحيحي" لنقاط الضعف واحتمال التعرض لحادث أمني سيبراني[19]، مما يشير إلى الأهمية الحاسمة لتحديث أنظمة بمجرد توفر البرمجيات التصحيحية الأمنية، مع مراعاة التوزيع المختلف المبلغ عنه للبرمجيات التصحيحية في جميع أنحاء العالم.

واختبار الاختراق هو عملية لضمان الأمن تساعد في تقييم أمن نظام تكنولوجيا المعلومات وتحديد مواطن الضعف التي يمكن استخدامها لاستغلال الأنظمة. وتدير هيئة تنظيم الاتصالات في المملكة المتحدة (Ofcom) طواعية مع مقدمي خدمات الاتصالات، الخطة TBEST، ويهدف مخطط الاختبار هذا إلى تحفيز هجوم سيبراني من أجل تحديد مواطن الضعف الأمنية التي تمكن بعد ذلك معالجتها من خلال عملية جبر لتحسين الوضع الأمني لشبكة المشغلين.[20] وقدمت الهيئة التنظيمية لمحة عامة عن العملية وعن مختلف أصحاب المصلحة المعنيين. وعلى نطاق أوسع، تعد هذه الخطة مثالاً لنهج نظام إشرافي تتبعه هيئة تنظيم الاتصالات (Ofcom)، وهي تؤكد أهمية بناء علاقات تعاونية مع دوائر الصناعة التي تنظمها الهيئة. وحتى الآن، فإن جميع مقدمي خدمات الاتصالات في المملكة المتحدة اعتمدوا خطة TBEST طواعية أو يقومون بذلك، وقد أدخلوا تغييرات نتيجة لذلك. وليست خطة TBEST "معياراً" ولا هي عملية إصدار شهادات. والهدف منها هو تمكين مقدمي خدمات الاتصالات من التنبه إلى التهديدات السيبرانية وتنفيذ التغييرات المناسبة في الوقت المناسب لتحسين قدراتهم في مجال الدفاع السيبراني. وإذ يعي المشغِّل الثغرات الأمنية ومواطن الضعف هذه ويعالجها، يصبح في وضع أقوى بكثير لحماية شبكاته.

الاستنتاج 5: تُبذل جهود لتثقيف المستهلكين والمصنعين بشأن أهمية الأمن السيبراني وفوائد اختيار المنتجات الأكثر أمناً

بُذلت جهود لتثقيف الجمهور بشأن أهمية الأمن السيبراني وفوائد اختيار منتجات أكثر أمناً.

وأحد النهج في هذا الصدد يتمثل في وضع خطة لتوسيم الأمن السيبراني (CLS)، ويمكن أن تكون المنتجات المعتمدة مصحوبة بوسم على النحو المعمول به في سنغافورة مثلاً. وتعمل مخططات الوسم أساساً كأداة إعلامية للمستهلكين. وقد ناقشت وكالة الأمن السيبراني (CSA) في سنغافورة مخططاً لتوسيم الأمن السيبراني يهدف إلى مساعدة المستهلكين على التمييز بين أجهزة إنترنت الأشياء الأكثر أمناً والأقل أمناً.[21] والمخطط طوعي (باستثناء مسيِّرات Wi-Fi التي يكون إلزامياً لها) وله أربعة مستويات، حيث يمثل المستوى 1 هو خط الأساس الأمني. ويستند المستويان 1 و2 إلى التقييم الذاتي من جانب المصنعين أما المستويان 3 و4 فيعتمدان على تقييم طرف ثالث بواسطة مختبر معتمد. والمخطط متعدد المستويات لتحفيز المصنعين على إدراج تدابير أمنية إضافية تتجاوز المتطلبات الأساسية. وناقشت وكالة الأمن السيبراني (CSA) أيضاً المفاضلات التي ينطوي عليها فرض معايير الأمن السيبراني، بما في ذلك خطر خروج المصنعين من السوق نتيجة لزيادة تكاليف الالتزام. وبدلاً من ذلك، فإن الهدف هو تغيير عقلية المصنعين لكي ينظروا إلى الأمن السيبراني كعامل تمكين وتمييز في السوق وليس كتكلفة. وفيما يتعلق بتأثير مخطط وسم الأمن السيبراني في سنغافورة، فالعملية لا تزال في مراحلها المبكرة، والجهود جارية لتشجيع المصنعين على المشاركة في الخطة وتحسين أمنهم السيبراني. وسيجرى استطلاع عام مرة أخرى في المستقبل لتقييم وعي المستهلك وسلوكه. وتقل تكلفة الالتزام إلى أدنى حد على المصنعين في المستويين 1 و2، ولم تحدث زيادة كبيرة في تكلفة المنتجات على المستهلكين. وبوجود الخطة الطوعية، يُتوقع لقوى السوق أن تدفع عجلة التحسينات في الأمن السيبراني بين المصنعين.

وبعيداً عن الوسوم، من المهم بالقدر نفسه الاستثمار في الضوابط التقنية وبناء الوعي وتثقيف السكان بشأن مخاطر الأمن السيبراني التي تواجهها المنظمات والبلدان. وتشكل هجمات برمجيات الفدية حالياً الاتجاه الأكثر إقلاقاً. وبالنسبة لهذه الأنواع من الهجمات، فإن الناقل الرئيسي للهجوم - بمعنى الطريقة التي يدخل بها المجرم إلى شبكة أو نظام - هو

[18] https://isms.kisa.or.kr/main/csap/intro/index.jsp

[19] https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity

[20] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work

[21] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090016PDFE

عبر رسائل البريد الإلكتروني التصيدية.[22] وفي هذا السياق، كثيراً ما يتمكن المجرمون السيبرانيون من تجاوز الضوابط الأمنية عند قيام الأشخاص بالنقر على بريد إلكتروني تصيدي. ولذلك فمن الأهمية بمكان لضمان الأمن السيبراني أن تتم توعية المواطنين والموظفين بهذه القضايا.

الاستنتاج 6: من المهم السعي للتوصل إلى اتفاقات دولية بشأن التآزر/التنسيق والمعاملة بالمثل

إن وجود اتفاقات المعاملة بالمثل بين نماذج ضمان الأمن السيبراني، أي مخططات إصدار الشهادات والوسم، يمكن أن يكون عاملاً محدداً في توسيع نطاق هذه الممارسات. وكما أوضح أصحاب المصلحة، يمكن لاتفاقات المعاملة بالمثل أن تساعد في تسهيل التزام الجهات الفاعلة الصناعية العاملة في أسواق متعددة. ولكن بالنظر إلى أن اتفاقات المعاملة بالمثل هي آلية رسمية تقيدها قيود وطنية كثيرة وتستغرق وقتاً للموافقة عليها وتوقيعها، يجب ان تلتمس ممارسات ضمان الأمن السيبراني أوجه تآزر مع النهج الدولية القائمة التي تتماشى مع الاحتياجات والأولويات الوطنية. ومن شأن ذلك أن يخفف العبء التنظيمي على مقدمي المنتجات والخدمات بغية تجنب المتطلبات المتناقضة.

وشددت وكالة الأمن السيبراني (CSA) على أهمية التعاون الدولي في وضع وتنفيذ مخططها لتوسيم الأمن السيبراني. وقد وقعت سنغافورة ترتيبات الاعتراف المتبادل مع فنلندا وألمانيا وتعمل على توسيع شراكاتها في هذا المجال. وتأملت سنغافورة في تجربتها معربةً عن رأيها بأن الحكومات يتعين أن تكون استباقية في إرساء الاعتراف، على الرغم من أن للمصنعين أيضاً مصلحة في دعم عملية الاعتراف لأنها تقلل من عبء الاختبارات المتكررة وإصدار الشهادات، فضلاً عن النفاذ إلى الأسواق، في ولايات قضائية مختلفة. وتنطوي العملية على جمع الأطراف المهتمة معا لتنسيق المتطلبات ووضع معايير مشتركة واقعية وغير مغالية في أعبائها.

وعلى المستوى الأوروبي، تتمتع وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) بصلاحية وضع ثلاث خطط لإصدار الشهادات من شأنها أن تحظى بالاعتراف عبر السوق الداخلية، فتحصل بالتالي على "الاعتراف المتبادل" التلقائي عبر الاتحاد الأوروبي (EU). والخطط هي: 1) *خطة المعايير المشتركة التي وضعها الاتحاد الأوروبي لمنتجات تكنولوجيا المعلومات والاتصالات*، حيث يجري وضع القانون التشريعي الخاص بها بغية الاعتماد؛ و*خطة الخدمات السحابية*، وهي قيد مناقشات مستفيضة، وأخيراً، *خطة تكنولوجيا الجيل الخامس (5G)* الجاري تطويرها[23].

وبالإضافة إلى المعاملة بالمثل، وبالنظر إلى الأسواق الدولية التي تعمل فيها صناعة الاتصالات، فإن تنسيق متطلبات الأمن الأساسي هو أيضاً من الاعتبارات الهامة. وتقدم معايير المعهد الأوروبي لمعايير الاتصالات (ETSI) بشأن المنتجات الاستهلاكية لإنترنت الأشياء مثالاً على هذا المسعى. والسؤال الرئيسي هو إلى أي مدى ستتسق الأطر التنظيمية المختلفة، وإلى أي مدى ستترابط من خلال المعايير الدولية نفسها. وفي هذا الصدد، لوحظ في ورشة العمل أن تعزيز، بل وإيجاد، المكان المناسب للحوار يشكل تحدياً. وفي مجال التنسيق، تتطلب أنشطة وكالة الأمن السيبراني الأوروبية (ENISA) في مجال تقييس الأمن السيبراني وتكنولوجيا الجيل الخامس التعاون بين CEN وCENELEC وETSI وISO وIEC GSMA و3GPP وGlobalPlatform. ويتمثل أحد النواتج الرئيسية للوكالة في تجميع ضوابط أمن تكنولوجيا الجيل الخامس من منظمات وضع المعايير (SDO) المختلفة في مستودع واحد[24].

[22] تكتيك شائع يستخدمه المجرمون السيبرانيون لخداع الناس كي يكشفوا عن معلومات حساسة أو ينزلوا برمجيات ضارة تصيب النظام المستهدَف/الشبكة المستهدَفة.

[23] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090019PDFE

[24] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

الملحق: أمثلة على ممارسات ضمان الأمن السيبراني

البلد أو المنظمة	اسم الممارسة	نوع الممارسة	مجال تطبيق الممارسة	نوع النهج	المرجع
أستراليا	توجيه الأمن من خلال التصميم للجهات المصنعة فيما يتعلق بإنترنت الأشياء	توجيه	إنترنت الأشياء	طوعي	رابط
أستراليا	مدونة ممارسات: تأمين إنترنت الأشياء للمستهلكين	مدونة ممارسات	إنترنت الأشياء	طوعي	رابط
البرازيل	القانون 2021/77 – المتطلبات الدنيا للأمن السيبراني لمعدات الاتصالات	متطلبات لخطة إصدار الشهادات	معدات الاتصالات	طوعي	رابط
البرازيل	القانون 2023/2436 – المتطلبات الدنيا للأمن السيبراني لتقييم مطابقة معدات منشآت العملاء(CPE)	متطلبات لخطة إصدار الشهادات	معدات منشآت العملاء	إلزامي	رابط
المملكة العربية السعودية	نظام مستقل للتحقق وإقرار الصلاحية (IV&V)	اختبار واعتماد المنتجات. تحديد هوية وتصنيف الأجهزة والبرمجيات	المنتجات	طوعي بداية	رابط
جمهورية كوريا	برنامج ضمان أمن الخدمات السحابية (CSAP)	خطة لإصدار الشهادات	الخدمات السحابية	مركب - طوعي بوجه عام. إلزامي فيما يتعلق بتوفير الخدمات السحابية للوكالات العامة.	رابط
سنغافورة	خطة وسم الأمن السيبراني	خطة لإصدار الشهادات والوسم	إنترنت الأشياء	مركب - طوعي بوجه عام. إلزامي فقط فيما يتعلق بالمسيرات المنزلية لتكنولوجيا Wi-Fi.	رابط
المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية	نظام أمن المنتجات والبنية التحتية للاتصالات (أمن المنتجات)	متطلبات الأمن الدنيا	المنتجات القابلة للتوصيل	إلزامي	رابط
المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية	الخطة TBEST	اختبار الاختراق	شبكات الاتصالات	طوعي	رابط

منشورات ITU

نُشرت في سويسرا، جنيف، 2024

ITU Disclaimer: https://www.itu.int/en/publications/Pages/Disclaimer.aspx

الاتحاد الدولي للاتصالات

Place des Nations, CH-1211 Geneva Switzerland