تحقيق المرونة في الأمن الإلكتروني من خلال نهج قائم على تحليل المخاطر

نهج قائم على تحليل المخاطر لتنفيذ برامج الحوكمة الإلكترونية الفعَّالة وإدارة المخاطر والامتثال داخل الجهات الحكومية وضمان تحقيق المرونة في ظل بيئة محفوفة بتهديدات تتزايد باستمرار

القمة العالمية للحكومات 2023

بالتعاون مع

EY

نبني عالماً أفضل للعمل

لإلهام الجيل القادم من الحكومات وتمكينه

القمة العالمية للحكومات هي منصة عالمية تهدف إلى استشراف مستقبل الحكومات حول العالم، تحدد لدى انعقادها سنوياً برنامج عمل حكومات المستقبل مع التركيز على تسخير التكنولوجيا والابتكار لمواجهة التحديات التي تواجه البشرية.

تبحث القمة العالمية للحكومات في نقاط الالتقاء ما بين العمل الحكومي واستشراف المستقبل والتكنولوجيا والابتكار، وهي منصة لتبادل المعرفة بين قادة الفكر ومركز للتواصل بين صنّاع السياسات والخبراء والروّاد في سبيل تحقيق التنمية البشرية وإحداث تأثيرات إيجابية على حياة المواطنين في جميع أنحاء العالم.

وتعتبر القمة العالمية للحكومات بوابة نحو المستقبل، إذ توفر مساحة لتحليل التوجّهات والمخاوف والفرص المستقبليّة، وميداناً لعرض آخر الابتكارات وأفضل الممارسات والحلول الذكيّة التي تحث على الإلهام وتحفّز الإبداع من أجل مواجهة التحدّيات المستقبليّة.

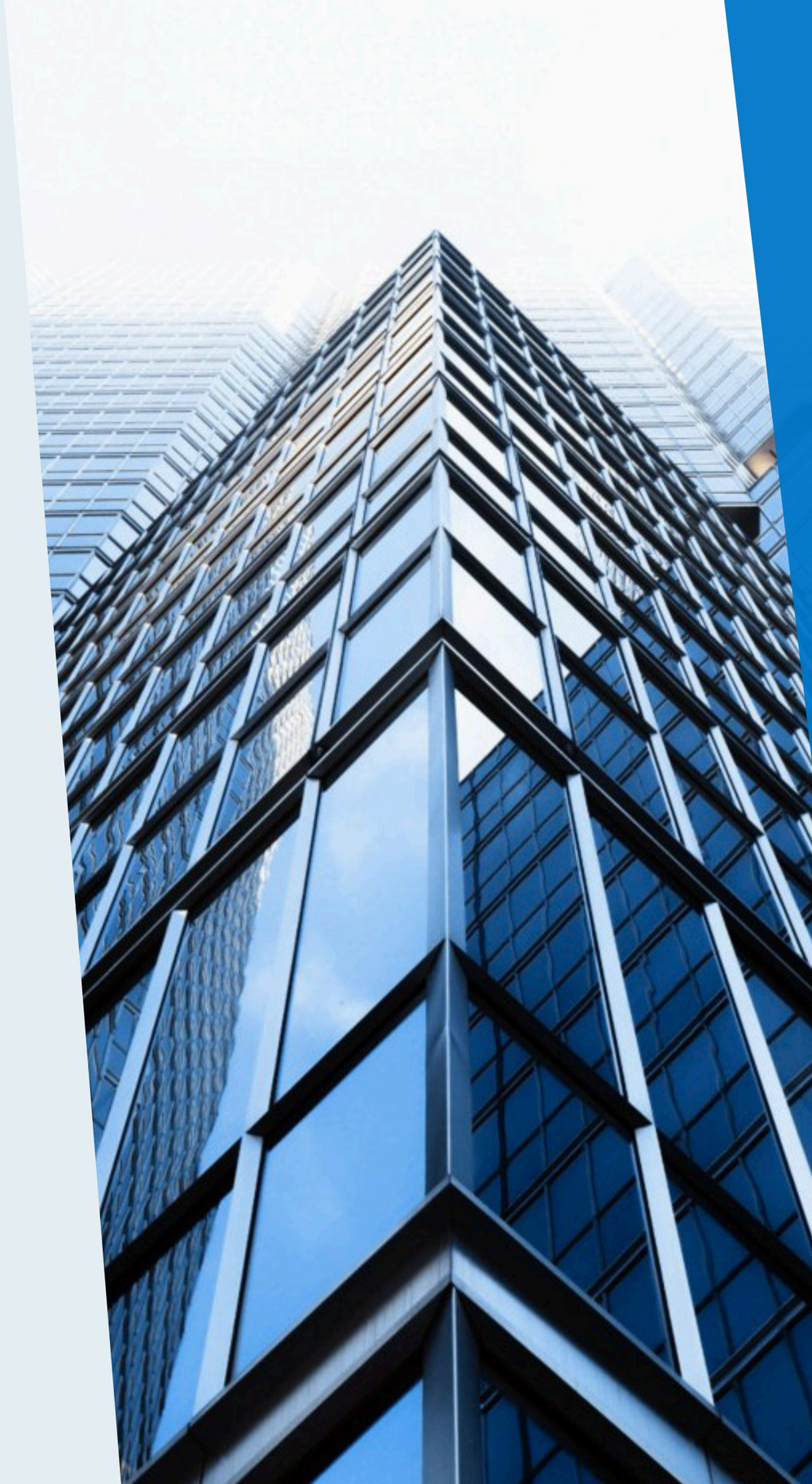
الفهرس

الموضوعات

القسم الأول

الملخص التنفيذي

تستند قدرة أي جهة على تحقيق أهدافها إلى مقدرتها على التغلب على المخاطر التي تواجهها بصورة فعَّالة، بما في ذلك المخاطر الإلكترونية. ومن المؤسف أن الإدارة التنفيذية ليست ملمة بمدى كفاءة إدارة المخاطر الإلكترونية في جهاتها ومدى مرونة عملياتها.



"قدَّم الاستطلاع العالمي لأمن المعلومات، الذي أجرته "إرنست ويونغ" في العام 2021 عرضاً موجزاً حول هذا الأمر حيث ذكر أن 56.2٪ من المدراء التنفيذيين الذين شملهم الاستطلاع لا يعلمون ما إذا كانت دفاعاتهم قوية بما يكفي للتصدي لإستراتيجيات الاختراق الجديدة التي يتبعها القراصنة أم لا[1]"

ورغم القلق المتزايد بشأن الحفاظ على المرونة في الأمن الإلكتروني، فقد أدى الضغط من أجل سرعة تحقيق التحول الرقمي لدفع الجهات الحكومية، لا سيما في الحكومة والقطاع الحكومي، إلى إهمال عمليات الأمن الإلكتروني. وربما لم يكن من قبيل المصادفة تزامن ذلك مع تزايد الهجمات الإلكترونية، لا سيما من الجهات التخريبية التي تقف وراء التهديدات الجغرافية السياسية مثل المجموعات التي ترعاها الحكومات والجهات الحكومية.

تعمل جميع الجهات الحكومية بشكل جوهري على أساس الثقة. لذا؛ يتعين على هذه الجهات إظهار تفانيها المتواصل في الحفاظ على السرية، وتأكيد توفر الأنظمة والخدمات، والحفاظ على أمن البيانات من أجل كسب ثقة المواطنين والحفاظ عليها. ومن ثم تشكل الهجمات الإلكترونية تهديداً لم يسبق له مثيل للحكومة والقطاع الحكومي. من الضروري وضع الأمن الإلكتروني في صميم إستراتيجية أي جهة حكومية، وذلك من خلال وضع برنامج فعَّال للحوكمة الإلكترونية وإدارة المخاطر والامتثال، مدفوع بنهج دمج الأمن في التصميم (SbD) الذي يجعل التفكير القائم على أساس تقييم المخاطر جزءاً من التصميم منذ بداية جميع المشاريع.

أتاحت لنا خبرات فرق إرنست ويونغ المتعددة الاختصاصات وكفاءاتها الأساسية في الحوكمة الإلكترونية وإدارة المخاطر والامتثال مساعدة العديد من الجهات الحكومية في وضع منهجيات فعَّالة لضمان المرونة في الأمن الإلكتروني. فقد أصبحت الجهات الحكومية الرائدة تبني منهجيات تراعي مناخ الأعمال، إلى جانب مشهد المخاطر الجغرافية السياسية، حيث بات من الواضح أن الحرب الهجينة، مثل الهجمات الإلكترونية، هي الواقع الجديد، وأن الجغرافيا السياسية والأمن الإلكتروني مرتبطان ارتباطاً وثيقاً.

وبينما لا توجد جهة محصنة ضد الهجمات الإلكترونية، فإن الجهات الحكومية التي لديها أنظمة دفاع إلكتروني قوية وأنظمة لحماية البيانات والجهات الحكومية التي تراعي اتباع نهج قائم على أساس تقييم المخاطر لتحقيق الأمن الإلكتروني، من المرجح أن تكون أكثر مرونة. إن النهج القائم على تقييم المخاطر من أجل تحقيق الأمن الإلكتروني يتيح للجهات الحكومية التركيز على حماية أصول المعلومات العالية القيمة والتخفيف من المخاطر الأعلى تأثيراً، ومن ثم تقليص المساحة المعرضة للهجوم. ويتطلب تنفيذ هذا النهج اتباع آلية متكاملة تراعي الجوانب المتعددة للجهة (مثل أنواع الأصول وتعقيد العمليات) ومنهجية تدريجية تشمل فهم بيئة الأعمال والتكنولوجيا، وتصنيف أصول التكنولوجيا، وتحليل المخاطر أو التهديدات، وتقييم تصميم التحكم وتنفيذ خيارات معالجة المخاطر.

يحدد هذا التقرير ضرورة تركيز الحكومة وجهات القطاع الحكومي على قدرات المرونة في الأمن الإلكتروني التي تقلل من تأثير أي هجمة إلكترونية ناجحة، وتقديم النهج المذكور أعلاه القائم على تقييم المخاطر من أجل تنفيذ برامج شاملة وفعَّالة للحوكمة الإلكترونية وإدارة المخاطر والامتثال التي تشمل في المقام الأول تقييمات المخاطر الإلكترونية مدعومةً بتقييمات فنية شاملة، مثل تقييمات مواطن الضعف واختبارات الاختراق ومراجعات إعدادات الأصول المهمة.

> إن النهج القائم على تقييم المخاطر من أجل تحقيق الأمن الإلكتروني يتيح للجهات الحكومية التركيز على حماية أصول المعلومات العالية القيمة والتخفيف من المخاطر الأعلى تأثيراً، ومن ثم تقليص المساحة المعرضة للهجوم "

القسم الثاني

الجغرافيا السياسية والمجال الرقمي: تأثير الفضاء الإلكتروني على الحكومة والجهات الحكومية

عند النظر إلى التطورات التكنولوجية الحديثة وترابط العالم، سندرك أنه لم يعد بإمكاننا فصل عالم التكنولوجيا عن عالم الأعمال وإغفال أهمية التكنولوجيا الحديثة للعمليات الحرجة. فقد أصبحت تكنولوجيا المعلومات والتكنولوجيا التشغيلية عناصر أساسية لا غنى عنها في مختلف القطاعات. وباتت العمليات تعتمد بشكل كبير على التكنولوجيا التشغيلية أو أنظمة التحكم الصناعية، بما في ذلك العمليات الحيوية في القطاعات الحرجة أو البنية التحتية للشبكات الحيوية (CNI)، مما أدى إلى أن تصبح هذه التقنيات مستهدفة بشكل رئيسي من المهاجمين التابعين للدول. وبينما يوجد العديد من الجهات ذات النوايا الخبيثة في الفضاء الإلكتروني، فإن الجهات التخريبية التي ترعاها الحكومات وتقف وراء التهديدات قادرةٌ على إلحاق أعلى درجات الضرر بالجهات الحكومية والقطاع الحكومي من خلال مستوى تطور هجماتهم. تنفذ الجهات التخريبية التي ترعاها الحكومات وتقف وراء التهديدات عمليات أمنية نيابةً عن الدولة، وفي أغلب الحالات يكتنف الغموض عملياتها.

ويمكن أن يُعزى انتشار الجهات التخريبية التي ترعاها الحكومات إلى عدم استقرار البيئة الجغرافية السياسية الحالية. وفي مثل هذه الحالة المتقلبة للشؤون الدولية، نتوقع ملاحظة المزيد من العمليات الإلكترونية المدفوعة بالجغرافيا السياسية على المدى القريب والمتوسط في المستقبل. ومن ثم فإن زعزعة الاستقرار واستمرار تجاوز الحد فيما يتعلق بالنشاط الإلكتروني الضار قد يؤدي أيضاً إلى إلحاق المزيد من الضرر. وقد لوحظ ذلك في الآونة الأخيرة لا سيما عندما تعرض عدد من أكبر شركات البنية التحتية الوطنية الحيوية في جميع أنحاء الاتحاد الأوروبي لهجمات إلكترونية خلال الحرب في أوكرانيا. وقد ورد في تقرير الدفاع الرقمي من مايكروسوفت لعام 2022 على لسان صانع البرمجيات أن الهجمات الإلكترونية المتصلة بأنشطة الدولة والتي تستهدف البنية التحتية الحيوية في جميع أنحاء العالم ارتفعت من 20٪ إلى 40٪ بين عامي 2021 و2022[2].

وخلال هذه الفترة، أخذ نوعان من البرمجيات الخبيثة المتطورة المصممة لاستهداف أنظمة التحكم الصناعية (ICS) في الانتشار بشكل متزايد، وهما Pipedream (Incontroller) وIndustroyer3، وكان تأثيرهما الأكبر في أوكرانيا، حيث تسببا في وقوع أضرار وأعطال في البنية التحتية للشبكات الحيوية الخاصة بالطاقة والمرافق والاتصالات السلكية واللاسلكية العديد من الأنظمة الأخرى. وإلى جانب ذلك، استغلت جماعات الجريمة المنظمة التي ترعاها الدولة الثغرات الأمنية (على وجه التحديد ثغرات الهجوم الفوري) لتنفيذ الهجمات الإلكترونية. ويعد ProxyLogon وأداة Fatedier Reverse Proxy وProxy Shell من بين هذه الثغرات الأمنية المسجلة وفقاً لتقرير التهديدات العالمية الصادر عن شركة "كراود ستريك" في عام 2022[3]. فمثلاً اكتُشف Proxy Shell أثناء عملية تجسس إلكتروني استهدفت مقدمي خدمات الاتصالات في الشرق الأوسط بواسطة إحدى مجموعات التهديدات المستمرة المتقدمة (APT) في عام 2022[4].

وقد تمتد الحرب الإلكترونية أيضاً إلى سباق التسلح بين الدول، مما قد يؤدي إلى اكتساب قدرات عسكرية على نحو تنافسي وتنافس الجهات التخريبية التي ترعاها الحكومات على أفضل التقنيات وأقواها. في عام 2022، حصلت مجموعات التهديدات المستمرة المتقدمة على معلومات تكنولوجية وملكية فكرية (IP) لصالح الصناعات المملوكة للدولة. مجموعة Winnti (جماعة التهديدات المستمرة المتقدمة رقم 41) على سبيل المثال، هي حملة عالمية للتجسس الإلكتروني تستهدف الشركات المصنعة في جميع أنحاء أمريكا الشمالية وأوروبا وآسيا في مجالات الدفاع والطاقة والطيران والتكنولوجيا الحيوية والصناعات الدوائية (هنريكيز، 2022)[5].

> وإلى جانب ذلك، تزايدت عمليات التأثير في عام 2022 لتمكين تأثير الحرب الدعائية من إضعاف الثقة والتأثير على الرأي العام لنشر الروايات عبر وسائل الإعلام وقنوات التواصل الاجتماعي التي تدعمها الحكومة وتؤثر عليها[6]

في عالمنا الحاضر، لا يمكن تفادي الحرب الإلكترونية. حيث إن زعزعة الاستقرار في العالم والتوترات السياسية وحتى الهجمات الإلكترونية بشكل عام، تُلزِم الدول بإعادة النظر في إستراتيجياتها الدولية وإدراج الأمن الإلكتروني ضمن الأدوات الأمنية للتصدي للهجمات الإلكترونية التي قد يترتب عليها آثار كارثية في القطاعات الحيوية.

وقد حدثت في شهر أبريل 2022 هجمة إلكترونية كبيرة في كوستاريكا، حيث تمكن المهاجمون من اختراق وزارة المالية وتسببوا في شل حركة شبكة الوزارة مطالبين بفدية قدرها 10 ملايين دولار أمريكي لإعادة إمكانية الدخول على الشبكة إلى الحكومة (ريد، 2022). ومن الأمثلة الأخرى تعرض خط "كولونيال بايبلاين"، وهو نظام خطوط أنابيب نفط أمريكي ينطلق من هيوستن بولاية تكساس، لهجمة من نوع برمجيات الفدية في مايو 2021. حيث كانت الشركة مسؤولة عن إمداد 45٪ تقريباً من الوقود الذي يستهلكه الساحل الشرقي للولايات المتحدة. وقد أدى الهجوم الإلكتروني إلى تعطيل أنظمة الكمبيوتر المسؤولة عن إنتاج الوقود من تكساس إلى شمال شرق البلاد، مما أدى إلى حالة من الفوضى شملت انتظار سائقي السيارات في طوابير لملء خزاناتهم وحاويات الوقود. ويمكن أن يترتب على هذه الهجمات عواقب وخيمة تبعاً لحجم الهجوم ونطاقه.

وقد تغيرت مفاهيم الحرب والسياسة في العصر الرقمي ويزداد تعقيد الهجمات مع استخدام تقنيات التكنولوجيا الحديثة، مثل الحوسبة الكمية وإنترنت الأشياء (IoT) وتقنية "البلوك تشين" (Blockchain). ومن ثم تتطلب طبيعة هذه المخاطر تعاون الحكومات مع القطاع الحكومي من أجل وضع اللوائح والسياسات والإجراءات لمواجهة التهديدات الإلكترونية والقضاء عليها على نحو فعَّال.

القسم الثالث

تطور البيئة التنظيمية للأمن الإلكتروني من أجل مكافحة آثار هشاشة الأوضاع في المشهد الجغرافي السياسي

في ظل الأوقات العصيبة، وبينما يستعيد العالم توازنه في ضوء الدروس المستفادة خلال جائحة كوفيد-19، يجب ألا يغيب عن أذهاننا أن البيئة في تغير مستمر ومليئة بالتحديات. فقد شهدنا خطوات لم يسبق لها مثيل في التحول الرقمي في الجهات الحكومية والخاصة وزيادة استخدامها للتقنيات من أجل تحقيق الأهداف الإستراتيجية. كما شهدنا في عام 2022 كيف تسببت التوترات الجغرافية السياسية في كشف حقيقة الحرب الإلكترونية كما رأينا في الحرب في أوكرانيا ومنطقة الشرق الأوسط، وأبرزها في المملكة العربية السعودية والإمارات العربية المتحدة وقطر، حيث كان لها تأثير على الصناعات والاقتصادات. وقد شجعت هذه السيناريوهات تهديدات الأمن الإلكتروني على النمو والتطور سريعاً، على الساحة الوطنية والعالمية. ومن ثم أصبحت الحكومة بوصفها صانعة للسياسات وجهة منفذة تتمتع بدور حاسم. تواجه الحكومة تحدياً في سبيل توفير بيئة آمنة ومرنة، حيث توفر الحكومة والقطاع الحكومي إلى جانب مقدمي خدمات البنية التحتية للشبكات الحيوية.

الأطر التنظيمية مقابل مشهد التهديدات الناشئة

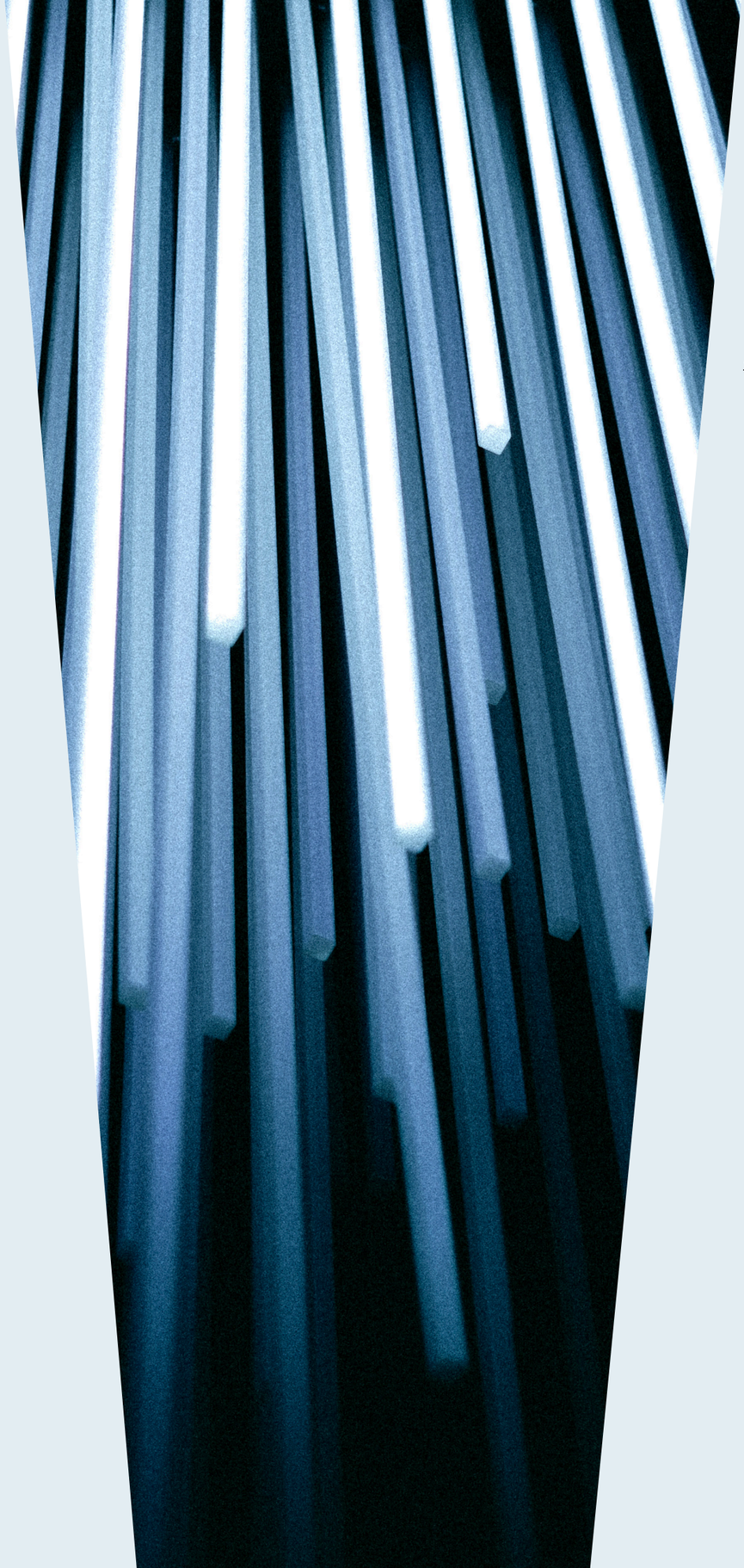
مع مشهد التهديدات المتطور دائماً، قد لا تكون الإرشادات التقليدية بشأن أفضل ممارسات الأمن الإلكتروني كافية لمواجهة التهديدات. وهذا يدفع سلطات الدولة إلى وضع تصور وتطبيق القواعد التنظيمية والتي من شأنها أن تعزز تنفيذ مرونة الأمن الإلكتروني وإدارتها لمكافحة مخاطر الجيل التالي. عندما نتحدث عن مرونة الأمن الإلكتروني، يمكننا أن نتصور بيئة توفر منظومة إلكترونية آمنة لتشمل البنية التحتية الأساسية ودعم الصناعات للاستمرارية والتعافي من الهجمات الإلكترونية. يمكن للأطر التنظيمية الوطنية للأمن الإلكتروني والتي تغطي موضوعات إدارة المخاطر وتحليل التهديدات الإلكترونية أن تساعد الحكومات في مكافحة التهديدات الناشئة.

إضافة إلى ذلك، يجب أن تكون القواعد التنظيمية قادرة على خلق بيئة مفتوحة تسمح بتبادل المعلومات والتعاون القوي وتشجع عليهما على المستويين القطري والصناعي. وقد تم توضيح ذلك من قِبل الفريق العامل المفتوح العضوية التابع للأمم المتحدة (OEWG) بشأن التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية، في مارس 2021. صادق الفريق على تقرير يحتوي على توصيات بشأن الأمن الإلكتروني وتم اعتماده من قِبل جميع البلدان بالإجماع.

الحرب في أوكرانيا ومساهمتها في التهديدات الإلكترونية العالمية

أظهرت الحرب في أوكرانيا نوعية جديدة من حروب القرن الحادي والعشرين. فقد أسفرت عن عددٍ من التداعيات العالمية التي امتدت إلى الفضاء الإلكتروني. أدى التصعيد المستمر إلى تفاقم ظاهرة "الهاكتفيزم"، والتي تعني اختراق شخص ما لنظام الكمبيوتر لأغراض سياسية أو اجتماعية، والحرب الإلكترونية التي هددت أيضاً من هم خارج حدود أوكرانيا. تُعد الحرب في أوكرانيا تذكيراً للدول الأخرى لتعزيز دفاعاتها في مجال الأمن الإلكتروني في حال زيادة التوتر داخل أراضيها وتأثير ذلك على سياساتها المحلية والخارجية. في ألمانيا، يتم تعزيز مرونة الأمن الإلكتروني بين الشركات التي تقدم خدمات حيوية مثل النقل والطعام والمرافق لمكافحة أي تهديدات محتملة جراء الحرب في أوكرانيا. من ناحية أخرى، كانت فنلندا مبدعة في الدعوة إلى المرونة الإلكترونية من خلال تقديم نظام قسائم من شأنه أن يمول الشركات لتحسين قدراتها الأمنية استجابةً للحرب في أوكرانيا ومحاولة الدولة للانضمام إلى منظمة حلف شمال الأطلسي (الناتو).

> في ألمانيا، يتم تعزيز مرونة الأمن الإلكتروني بين الشركات التي تقدم خدمات حيوية مثل النقل والطعام والمرافق لمكافحة أي تهديدات محتملة جراء الحرب الجارية في أوكرانيا "



إدارة المخاطر بوصفها متطلباً أساسياً

إن الهدف المتمثل في وجود بيئة تتمتع بالمرونة في الأمن الإلكتروني يستدعي من الحكومات توفير أساليب منظمة لقياس قدرة الجهات الحكومية على الحماية من الهجمات الإلكترونية. لقد رأينا الهيئات التنظيمية تعيد النظر في الإرشادات الحالية لديها المتعلقة بإدارة المخاطر للتأكد من أنها محدثة، لدعم الصناعات والجهات الحكومية في مكافحة التهديدات الإلكترونية. تحتاج الهيئات التنظيمية الوطنية إلى النظر في مجالات التركيز الرئيسية التالية بوصفها جزءاً من أطر الأمن الإلكتروني التي يتم تحديدها:

- **المساءلة الشاملة:** المرونة عمل جماعي، حيث تحتاج القواعد التنظيمية إلى تفويض الجهات الحكومية للتأكد من أنه ليس فقط المتخصصون في التشغيل أو الأمن الإلكتروني هم الذين يضمنون المرونة، ولكن أيضاً الأطراف المعنية الداخلية الأخرى، بما في ذلك الإدارة التنفيذية المباشرة للشركة وإدارة الموردين والخطوط الثانية والثالثة والشؤون القانونية ومجلس الإدارة، وغيرهم. إضافة إلى ذلك، ينبغي تشجيع الجهات الحكومية على وضع وتنفيذ إستراتيجية مرونة إلكترونية منسقة ومتعددة التخصصات بصورة فعَّالة واختبارها على أساس دوري من خلال عمليات المحاكاة.
- **إدارة المخاطر:** لا بد للقواعد التنظيمية أن توفر سبلاً للجهات الحكومية لتضمين متطلبات المرونة في الأمن الإلكتروني في إطار تحمل المخاطر. في هذا السياق، يحتاج خط الدفاع الثاني إلى مجموعة فعَّالة من المقاييس لتقييم مخاطر المرونة في الأمن الإلكتروني. قد تأتي العديد من هذه المقاييس من الخط الأول، لكن الخط الثاني يحتاج إلى مقاييسه الخاصة، لا سيما لتقييم المخاطر الإلكترونية للجهات الحكومية على المستوى الإجمالي.
- **التدقيق الداخلي:** يلعب خط الدفاع الثالث (التدقيق الداخلي) دوراً رئيسياً في التحقق والمراجعة. النهج الذي يتبعه الخط الثالث للتحقق من فاعلية الإطار (الأطر) الإلكتروني تم اعتماده من قِبل الخطين الأول والثاني لتقييم مخاطر المرونة في الأمن الإلكتروني وإدارتها، وهو أمر ضروري لضمان قدرة المرونة وفاعليتها على مقاومة الهجمات الإلكترونية.

في 13 مايو 2022، قام مجلس الاتحاد الأوروبي والبرلمان الأوروبي بمراجعة وتحديث التوجيه الحالي لأمن الشبكات والمعلومات (NIS) ليصبح توجيه أمن الشبكات والمعلومات NIS2. يضع التوجيه الجديد "خط أساس لإدارة مخاطر الأمن الإلكتروني والتزامات تقديم التقارير عبر القطاعات الحيوية". سيتم الاعتراف بالاتفاقية في جميع المناطق المشمولة على أمل وضع تدابير استباقية للتخفيف من حدة التهديدات في مختلف المجالات.

في الولايات المتحدة، أصدر المعهد الوطني للمعايير والتكنولوجيا (NIST) منشوراً منقحاً عن ممارسات إدارة مخاطر الأمن الإلكتروني لسلاسل التوريد للأنظمة والجهات الحكومية. يركز المنشور المنقح على مساعدة الشركات في فهم طرق تحديد مخاطر الأمن الإلكتروني وتقييمها والاستجابة لها في مختلف أنحاء سلاسل التوريد في كافة أنحاء الجهات الحكومية. إضافةً إلى ذلك، نشرت وزارة التجارة الأمريكية قاعدة مقترحة لتنفيذ القواعد التنظيمية وفقاً للأمر التنفيذي الصادر في مايو 2019، لتحسين سلسلة التوريد لخدمات تكنولوجيا الاتصالات والمعلومات (ICTS). سيعالج هذا المخاوف المتعلقة بتصميم المنتج وتطويره وتصنيعه وتوريده والتحكم في خدمات تكنولوجيا الاتصالات والمعلومات من قِبل الخصوم الأجانب.

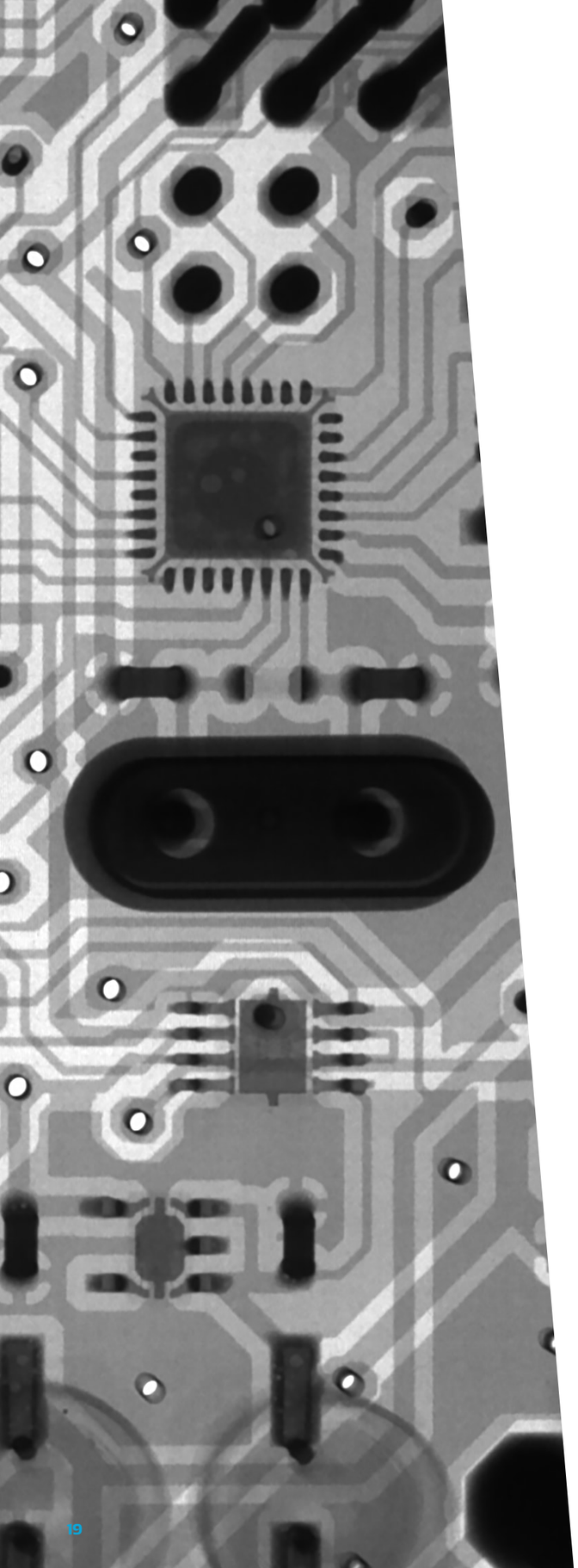
انتشار برامج الفدية

يتزايد تهديد برامج الفدية في عام 2022 ولا يزال يمثل خطراً كبيراً على الجهات الحكومية بجميع أحجامها في جميع القطاعات. يُظهر تقرير عام 2022 الصادر عن وكالة الاتحاد الأوروبي للأمن الإلكتروني (ENISA) حول مشهد تهديدات برامج الفدية كيف أن الجهات الحكومية لا تزال عرضة لهذا النوع من الهجمات وقد خلُص إلى أن لها تأثيراً مدمراً على هذه الجهات، خاصة إذا لم تكن مستعدة لمواجهتها.

دفعت المخاطر التي تفرضها برامج الفدية الهيئات التنظيمية والقائمين على تطبيق القانون في جميع أنحاء العالم إلى التعاون في مكافحة هجمات برامج الفدية. في يوليو 2021، بمنتدى الإنتربول الرفيع المستوى المعني ببرامج الفدية، تمحور النقاش حول أن منع برامج الفدية وتعطيلها بشكل فعَّال يتطلب "اعتماد التعاون الدولي نفسه المستخدم لمكافحة الإرهاب أو الاتجار بالبشر أو جماعات المافيا".[7] وقد دعت المجموعة أجهزة الشرطة في جميع أنحاء العالم لتشكيل تحالف عالمي مع شركاء المجال لوقف النمو المتسارع لبرامج الفدية. كما نشر المركز الوطني للأمن الإلكتروني في المملكة المتحدة (NCSC)، ومركز الأمن الإلكتروني الأسترالي (ACSC)، ومكتب التحقيقات الفيدرالي (FBI)، ووكالة الأمن القومي (NSA)، ووكالة الأمن الإلكتروني وأمن البنية التحتية (CISA) تنبيهاً مشتركاً[8]، يحث الشركات لاتخاذ إجراءات لحماية أنفسها من الهجمات.

من ناحية أخرى، لوقف انتشار هجمات برامج الفدية، تم سنُّ التشريعات التي تحظر دفع الفدية في ضوء الحرب في أوكرانيا. على سبيل المثال، قام مكتب مراقبة الأصول الأجنبية (OFAC) التابع لوزارة الخزانة الأمريكية بمنع دفع الفدية، بما في ذلك المدفوعات بالعملات الرقمية أو المدفوعات التي يتم تسهيلها من خلال الغير، إلى الأشخاص أو الكيانات الخاضعة للعقوبات.[9] إضافة إلى ذلك، أصدرت شبكة إنفاذ الجرائم المالية، كمحاولة أخرى لمنع دفع الفدية للكيانات الخاضعة للعقوبات، تنبيهاً إلى جميع المؤسسات المالية "للتيقظ ضد محاولات التهرب من العقوبات الموسعة وغيرها من القيود التي تفرضها الولايات المتحدة فيما يتعلق بالحرب في أوكرانيا".[10]

> تعمل الحكومات أيضاً بصورة استباقية لمكافحة برامج الفدية، ففي الولايات المتحدة، أطلق مكتب التحقيقات الفيدرالي وحدة استغلال الأصول الافتراضية (VAXU) لتتبع برامج الفدية وأرباحها [11]



تجديد الاهتمام بالأمن الإلكتروني الصناعي

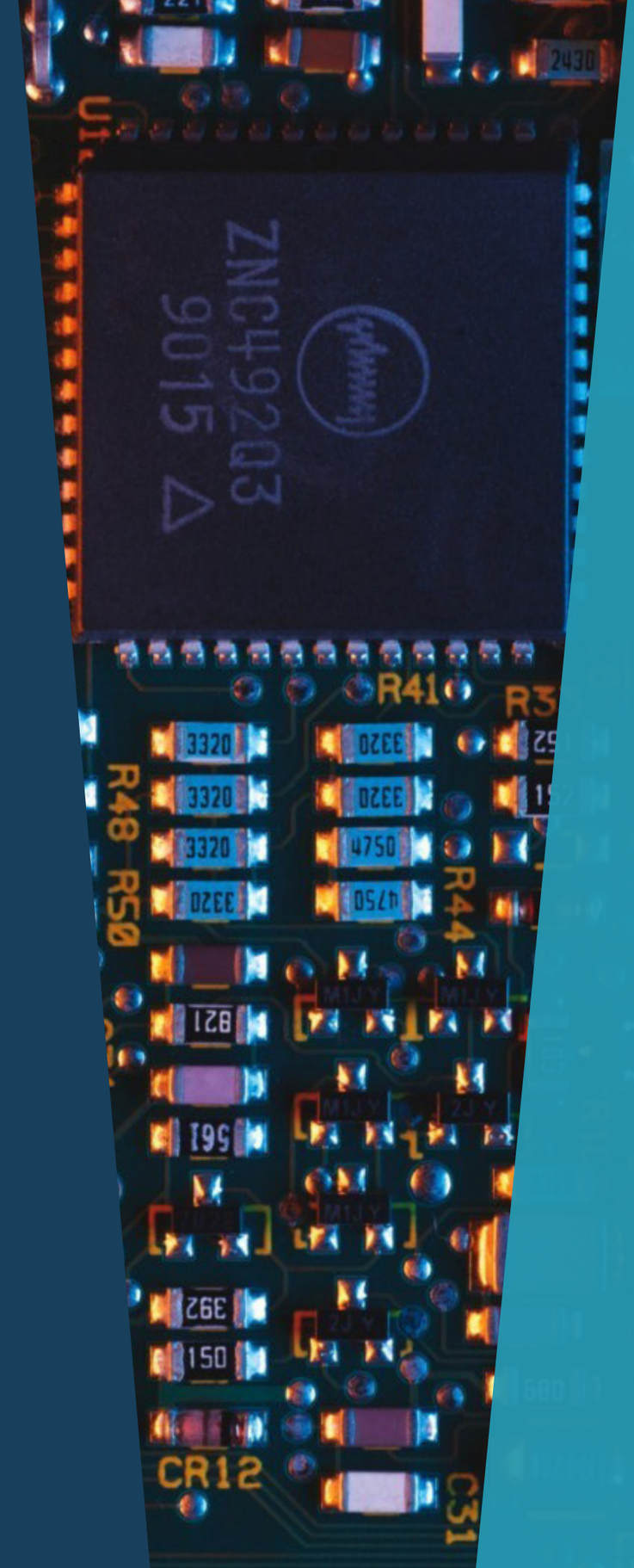
مع تزايد أجهزة التكنولوجيا التشغيلية وإنترنت الأشياء، يتطلب مجال الأمن الإلكتروني الصناعي اهتماماً متجدداً من الهيئات التنظيمية. لمكافحة سهولة التأثر المتزايدة لهذا المجال بالهجمات الإلكترونية، وضعت البلدان متطلبات تقنية لتعزيز الضوابط الأمنية على أجهزة التكنولوجيا التشغيلية/ إنترنت الأشياء. في أوروبا، أدخل الاتحاد الأوروبي تعديلات على توجيه الاتحاد الأوروبي بشأن المعدات اللاسلكية لعام 2014، والتي ستضمن أن تكون جميع الأجهزة اللاسلكية آمنة بما فيه الكفاية قبل بيعها. تطلب ذلك من الشركات المصنعة اتباع إجراءات وقائية جديدة للأمن الإلكتروني عند تصميم المنتجات وإنتاجها، وفرض حماية متزايدة للبيانات الشخصية.[12] بينما في الولايات المتحدة، أعيد تقديم تشريع يُعرف باسم قانون الحماية الإلكترونية "Cyber Shield Act" في الكونجرس في 15 مارس 2021. في حال إقراره، سيضع القانون [13] معايير أمان لأجهزة إنترنت الأشياء بناءً على توصيات لجنة استشارية مكونة من خبراء في الأمن الإلكتروني من الحكومة والأوساط الأكاديمية والجهات الخاصة. سيُسمح لمصنعي الأجهزة الذين يستوفون هذه اللوائح بتسمية منتجاتهم بعلامة تشير إلى أنهم استوفوا المعايير وأن منتجاتهم أكثر أماناً. تدرس أستراليا أيضاً تحويل مجموعة من اللوائح الطوعية إلى لوائح إلزامية من شأنها تحديد مجموعة من متطلبات الحد الأدنى للأمن الإلكتروني فيما يتعلق بالأجهزة الذكية ذات الجودة الاستهلاكية.[14]

تزايد متطلبات الإبلاغ عن الجرائم الإلكترونية

لمزيدٍ من ممارسة المرونة، تم تقديم لوائح جديدة لتحقيق شفافية أفضل بشأن حوادث الأمن الإلكتروني. بشكل عام، توجد هذه المتطلبات في أنظمة سرية البيانات، حيث توجد متطلبات بشأن إشعارات خرق البيانات. الآن، أدركت الحكومات أن الهجمات الإلكترونية تتجاوز مسألة اختلاس البيانات الشخصية. ففي الولايات المتحدة، تم تمرير قانون الإبلاغ عن الحوادث الإلكترونية للبنية التحتية الحرجة (CIRCIA) في مارس 2022. سيتطلب ذلك من شركات البنية التحتية الحرجة، بما في ذلك الخدمات المالية، الإبلاغ عن حوادث الأمن الإلكتروني، مثل هجمات برامج الفدية، إلى وكالة الأمن الإلكتروني وأمن البنية التحتية(CISA). [15] إضافةً إلى ذلك، في الجدول الزمني نفسه، اقترحت هيئة الأوراق المالية والبورصات الأمريكية (SEC) قاعدة تطالب الشركات المدرجة في البورصة بإبلاغ هيئة الأوراق المالية والبورصات بحوادث الأمن الإلكتروني، وقدراتها في مجال الأمن الإلكتروني، وخبرة مجلس الإدارة في مجال الأمن الإلكتروني ومراقبته إليه.[16] إضافة إلى ذلك، وقع رئيس الولايات المتحدة على "قانون مقاييس أفضل للجرائم الإلكترونية" والذي يحدد المتطلبات التي تهدف إلى تحسين الإبلاغ والتتبع الإلكتروني من أجل زيادة تسليط الضوء على نواقل الهجوم وتطور الهجمات.[17]

التحدي المستمر للهيئات التنظيمية

مع زيادة الرقمنة في العالم واستمرار تطور المشهد الجيوسياسي العالمي، لا توجد استجابة قياسية لجميع تهديدات الأمن الإلكتروني. من الضروري أن تضع الحكومات اللوائح والمبادئ التوجيهية التي من شأنها أن تمكن القطاعات والجهات الحكومية من ممارسة المرونة في الأمن الإلكتروني داخل بيئتها الخاصة. يتمثل التحدي في أن تكون الهيئات التنظيمية على دراية بالبيئة الرقمية المتغيرة، وأن تسبق خطواتها خطوات الجهات التخريبية، وأن تُوجِد طريقاً تكون فيه المجالات منفتحة على التعاون والشراكات.



القسم الرابع

نهج حوكمة فعال لإدارة المرونة في الأمن الإلكتروني

مع التهديد المتزايد والمتواصل والمشهد الجيوسياسي، أصبح من الضروري الآن للحكومة والجهات الحكومية تعزيز مرونة الأمن الإلكتروني بوصفه جزءاً من مهامها. وبإعادة النظر في تعريف المرونة، فهي قدرة الجهة الحكومية على التنبؤ بالأحداث التخريبية ومقاومتها والتعامل معها، وتكييف العمليات في البيئة وإعادة تشكيلها. من خلال تطبيق هذا المفهوم في الأمن الإلكتروني، تهدف المرونة إلى صد الهجمات الإلكترونية المحتملة وضمان التعافي منها، دون فقدان البيانات أو تهديد لها، بعد أي هجوم.

في حين أن تعريفها قد يبدو سهلاً، فإن التحدي الرئيسي يكمن في بناء نظام بيئي، حيث يمكن للحكومة ومكوناتها تحقيق عملية مستدامة ومرنة. بطبيعة الحال، فإن دور الحكومة بوصفها صانعة السياسة هو سن اللوائح التي من شأنها أن تنشئ مرونة في مجال الأمن الإلكتروني عبر مكوناتها.

إن الطبيعة السريعة التطور لبيئة المخاطر الإلكترونية تجعل من المهم بشكل متزايد أن تتبنَّى الحكومة والجهات الحكومية نهجاً قائماً على المخاطر للأمن الإلكتروني. لا تستطيع الجهات الحكومية بكل بساطة حماية كل شيء بالدرجة نفسها. الخطوة الأولى هي تنفيذ الحوكمة الإلكترونية بصورة صحيحة. تدرك الإدارة أن الأمن الإلكتروني يمثل خطراً كبيراً، وربما يُعد الخطر رقم واحد. إنها تعلم أن الخطر يتغير بسرعة وأنه من الصعب مواكبة ذلك. ومع ذلك، فإنها تكافح لتحديد الكيفية التي يجب أن تتطور بها حوكمتها. من الناحية العملية، ستؤثر مجموعة أوسع من الاتجاهات على التصميم المستقبلي لحوكمة المخاطر الإلكترونية. وتشمل هذه القوانين الجديدة للخصوصية والبيانات، وتنفيذ ثلاثة خطوط دفاع للأمن الإلكتروني (3LoD)، والحاجة إلى تضمين الأمن الإلكتروني في الابتكار، والامتثال للوائح الجديدة والتوقعات الإشرافية المعززة. إن تقدير هذه الاتجاهات الأوسع أمر مهم لتصميم أفضل للحوكمة.

دور خطوط الدفاع الثلاثة للأمن الإلكتروني

	من يمثلها؟	ما أدوارها في الأمن الإلكتروني؟	ما التحدي الذي تواجهه؟
الخط الأول	وحدات الأعمال وفرق أمن المعلومات مع المساءلة المباشرة لتحمل مسؤولية المخاطر الإلكترونية وفهمها وإدارتها	• قياس ومراقبة وإدارة وتخفيف المخاطر الإلكترونية وسرعة التأثر في نطاق تحمل المخاطر الإلكترونية المعتمد من مجلس الإدارة إذا كانت وحدات الأعمال الأمامية تعمل مع فرق أمن المعلومات والأمن الإلكتروني • تحديد المخاطر الإلكترونية واحتماليات التعرض لها في كل مجال من مجالات الأعمال • تطوير المعايير والإجراءات التي تنفذ إطار عمل المخاطر الإلكترونية للخط الثاني في سياق مخاطر الأعمال المحددة	• أن يصبح التفكير في الأمن الإلكتروني جزءاً لا يتجزأ من العمليات اليومية • أن يحدد الخط الأول (وليس مجموعة الأمن الإلكتروني) المخاطر الإلكترونية بصورة صحيحة، وأن يضع ضوابط قوية ويحافظ عليها
الخط الثاني	مديرو المخاطر المسؤولون عن إجمالي المخاطر الإلكترونية على مستوى الجهة الحكومية، والذين يتم منحهم سلطة مستقلة لتحدي نهج الخط الأول تجاه المخاطر الإلكترونية بشكل فعال	• وضع إطار عمل للمخاطر الإلكترونية ومطالبة تنفيذ الخط الأول له • تطوير تحمل الشركة للمخاطر الإلكترونية ومراقبة التوافق معها • الإبلاغ عن إجمالي المخاطر الإلكترونية على مستوى الجهة الحكومية	• وضع مجموعة مستنيرة من المقاييس الإلكترونية على مستوى الجهة الحكومية • مواءمة إطار عمل إدارة المخاطر الإلكترونية مع إطار عمل المخاطر العام • البحث عن الموهوبين الذين هم على دراية بالمخاطر والأمن الإلكتروني
الخط الثالث	فريق التدقيق الداخلي الذي يوفر ضمانات لحوكمة المخاطر الإلكترونية الشاملة للشركة	• تدقيق العناصر الإلكترونية الأساسية، إما كتدقيق منفصل (على سبيل المثال، بشأن ضوابط الوصول) أو مع عمليات تدقيق ذات صلة بموضوع محدد (على سبيل المثال، إدارة مخاطر الموردين) • تقييم التصميم العام وفاعلية إدارة المخاطر الإلكترونية عبر الخطين الأول والثاني	• تقديم رؤى تعمل على تحسين جودة الضوابط الإلكترونية • تحديد أفضل نهج لتقييم إطار عمل مخاطر الأمن الإلكتروني بشكل مستقل

يجب أن يبني قسم المخاطر في الخط الثاني قدراته. يجب أن يتم دمج المخاطر الإلكترونية في إطار تحمل المخاطر على مستوى الجهة الحكومية، حتى تتمكن الإدارة من الموافقة رسمياً على تحملها للمخاطر الإلكترونية. يجب دمج إطار عمل إدارة المخاطر الإلكترونية بشكل كامل في نهج إدارة المخاطر على العموم الأوسع للجهة الحكومية، وأن ينسجم مع أطر عمل تكنولوجيا المعلومات والمخاطر الأمنية والمخاطر التشغيلية. سيحتاج الخط الثالث (التدقيق الداخلي) إلى تركيز أقوى على الأمن الإلكتروني، والموظفين الجدد (أو القدرات المشتركة)، ورؤية أكثر استقلالية حول مدى قدرة مجلس الإدارة، والخط الأول والثاني، على الإشراف على المخاطر الإلكترونية وتقييمها وإدارتها. يتمثل التحدي الرئيسي لجميع الخطوط الثلاثة في إدارة المخاطر الإلكترونية المرتبطة بالغير. تدفع الهيئات التنظيمية بشكل متزايد نحو المزيد من الرقابة المستمرة والتفصيلية على الغير، لا سيما فيما يتعلق بالأمن الإلكتروني والمرونة وحماية البيانات.

دمج المرونة في الأمن الإلكتروني منذ البداية

وبالرغم من التحديات التي يفرضها مشهد المخاطر الإلكترونية الذي يتغير باستمرار، حيث يبدو أن خبرة الجهات التخريبية والتهديدات في زيادة يوماً بعد يوم، تحتاج الحكومة والجهات الحكومية إلى مناقشة فرصة مهمة، وهي دمج المرونة في الأمن الإلكتروني ضمن أساس أي تغيير تنظيمي. وإضافةً إلى ذلك، يجب أن يرتبط دمج المرونة في الأمن الإلكتروني بنشر ممارسة "الثقة عن طريق التصميم"، وهي أمر يصدر من أعلى التسلسل الهرمي إلى أسفله لدمج الأمن الإلكتروني عند تصميم جميع المنتجات والعمليات والتطبيقات والخدمات أو إعادة تصميمها أو عند النظر في أي شراكة بين القطاع الحكومي والقطاع الخاص. ويمكن للإدارة العليا دعم هذا المفهوم وتعزيزه من خلال التحقق الأمني قبل إطلاق المبادرات أو عند بدء العمل على كل مبادرة.

من الضروري أن ندرك أن أجهزة إنترنت الأشياء النموذجية قد تشكل تحديات لمفهوم "الثقة عن طريق التصميم". فقد صُممت هذه التقنيات بشكل عام مع مراعاة السرعة، وقد توفر وصولاً سهلاً إلى الجهات التخريبية التي تقف وراء التهديدات. وبالمثل، فإن العديد من برامج التحول الرقمي لا تتضمن خاصية الأمان حتى يُجرى تنفيذها، وهي عملية تؤدي دائماً إلى إحداث ثغرات أمنية. ومن ثم فإن دعم الإدارة العليا لإدخال المتطلبات الأمنية في وقت مبكر من مرحلتي التصميم ووضع المفاهيم أمر ضروري، إلى جانب دمج الثقة في كل ما يجري تصميمه أو إعادة تصميمه. وعادة قد توجد مقاومة داخلية للتغيير نظراً لوجود تصور عام خاطئ بأن هذا سيؤدي إلى إبطاء الأعمال. فالغرض من هذا الدور المُسند للإدارة العليا هو ضمان تحقيق التعاون منذ المراحل المبكرة، مما يجعله أمراً بالغ الأهمية في نموذج "الثقة عن طريق التصميم".

معادلة المخاطر

يمكّن دمج الأمن في مرحلة تصميم المبادرات الرئيسية الجهات الحكومية من تخفيف المخاطر، إلا أنه لا يقضي عليها تماماً. لذا؛ قد تحتاج الشركات إلى اتخاذ قرارات صعبة حول أماكن الاستثمار، وهنا يأتي دور التقييم الكمي للمخاطر. إذ من الضروري أن يفهم الأطراف المعنية الرئيسية حجم المخاطر واحتمال حدوثها وتقدير التكلفة المالية للأضرار المتكبدة إن وجدت. ويمكن حساب الحجم المحتمل لخطر معين باستخدام هذه الصيغة: خطر = تهديد (مثل البرمجيات الخبيثة) × الثغرة الأمنية × التأثير على الجهة (من حيث عملياتها وسمعتها على سبيل المثال). وبينما يوجد العديد من الافتراضات المدمجة في مثل هذه المعادلة، فإن الحكومة والجهات الحكومية تسعى إلى قدر أكبر من التقدير الكمي للموارد المالية من أجل اتخاذ قرارات حوكمة أكثر استنارة حول الإقدام على المخاطر وتحملها.

التقييمات المستقلة

تستخدم العديد من الشركات أطر عمل ومبادئ معروفة للتعامل مع حوكمة الأمن الإلكتروني، إلا أن استخدام جهة خارجية لأغراض التحقق يعد خطوة أساسية في ربط المخاطر بالبرامج والضوابط وربط النتائج بعمليات الجهة. لذا؛ من الضروري أن تعين الحكومة والجهات الحكومية جهة خارجية من أجل تقييم برنامج أمن الجهة الحكومية. اختارت بعض الجهات الحكومية إجراء تحقيق ومراقبة بخطوات بسيطة للغاية مع الرئيس التنفيذي لأمن المعلومات، والتي استغرقت عدداً محدوداً من الساعات. لمزيدٍ من التأكيد، يسعى الآخرون إلى تطبيق اختبار مراقبة إضافي لأطر العمل ذات الصلة (على سبيل المثال، المعهد الوطني للمعايير والتكنولوجيا [NIST]). وللحصول على أعلى مستوى من الضمان، يتم طلب رأي بيِّن من طرف خارجي مستقل يستخدم نظام المعهد الأمريكي للمحاسبين القانونيين (AICPA) وضوابط النظام والمؤسسة (SOC) لإطار الأمن الإلكتروني، والذي يوفر تقييماً لبرنامج إدارة المخاطر الإلكترونية على مستوى الجهة الحكومية.

يجب أن نسعى إلى جعل المرونة في الأمن الإلكتروني بداية سلسة لخطوات نحو الحفاظ على الإنجاز المستمر للعمليات في ظل أي أعطال. ويمكن وضع الأساليب التالية في الاعتبار لتحقيق ذلك:

تقييم ملف المخاطر وتحديد المخاطر والتهديدات وأوجه الضعف الرئيسية

إن تقييم مخاطر المرونة في الأمن الإلكتروني، إلى جانب إسناد الأولوية إلى مدى الخطورة، يعد لبنة البناء الأساسية لأي برنامج للمرونة للإلكترونية. هذه هي الخطوة الأولى في تحقيق المرونة في الأمن الإلكتروني ويمكن تحقيقها من خلال ما يلي:

- إعداد عملية تقييم مخاطر فعَّالة: تحديد المخاطر هو دور مناصب الخط الأول والثاني. ما مدى كفاءة الخط الأول في النظر إلى المخاطر الإلكترونية ومخاطر المرونة، من وجهة نظرهم؟ ما مدى تقييم الخط الثاني بشكل مستقل لهذه المخاطر من أجل معارضة وجهة نظر الخط الأول على نحو فعَّال وتكميلها؟

- سيحتاج تحليل المخاطر على أيدي الخطين الأول والثاني إلى إجراء تحديث روتيني؛ نظراً للطبيعة السريعة التطور للمخاطر الإلكترونية.

- وضع ضوابط فعالة: وضع ضوابط في ضوء تقييمات المخاطر يعد أمراً بالغ الأهمية. إذ يجب أن تقلل هذه الضوابط من المخاطر المتبقية في إطار تحمل الشركة للمخاطر بوجه عام من أجل تحقيق المرونة. ويتضمن ذلك الإلمام بكيفية تأثير الاعتماد على الجهات الخارجية على بيئة المراقبة.

- تقديم رأي ذي أولوية على مستوى الجهة الحكومية للعمليات والتدفقات الحرجة: بالنظر إلى الموارد المحدودة ووقت الإدارة والميزانية والأشخاص، يتعين على الشركات حتماً منح الأولوية لأنشطة معينة تتصل بالمرونة وتحديد العمليات والأنظمة التي تتطلب إستراتيجية متمايزة. وسيؤدي ذلك على الأرجح إلى وجود وجهات نظر مختلفة داخل كل شركة حول ما يمكن اعتباره أمراً حرجاً. وقد يكون لخط الدفاع الأول للجهة ولجنة إدارة المخاطر والهيئات التنظيمية تعريف مختلف للأمر الحرج. ومن ثم يتعين على الجهات الحكومية إدارة مطالب الأطراف المعنية بشأن تحقيق المرونة.

تحديد الأنظمة وتصميمها وحمايتها

يعد تحديد الأنظمة والأصول الأعلى أهمية (بما في ذلك الأصول العالية القيمة) متطلباً أساسياً لتحقيق المرونة في الأمن الإلكتروني. وبمجرد تحديد الأنظمة الحرجة، يتعين على الجهة الحكومية ما يلي:

- تحديد المنظومة البيئية للأنظمة: يمكن استخدام عدد من التقنيات لتحديد الأصول على نحو مناسب، أحدها هو تحليل تأثر العمل (BIA) الذي يمكنه تحديد العناصر والأصول الإلكترونية داخل الجهة نفسها، وتصنيف الأصول الإلكترونية والتقنية بناءً على السرية والسلامة والتوافر (CIA)، وإنشاء ملفات تعريف وسجلات للمخاطر الإلكترونية.

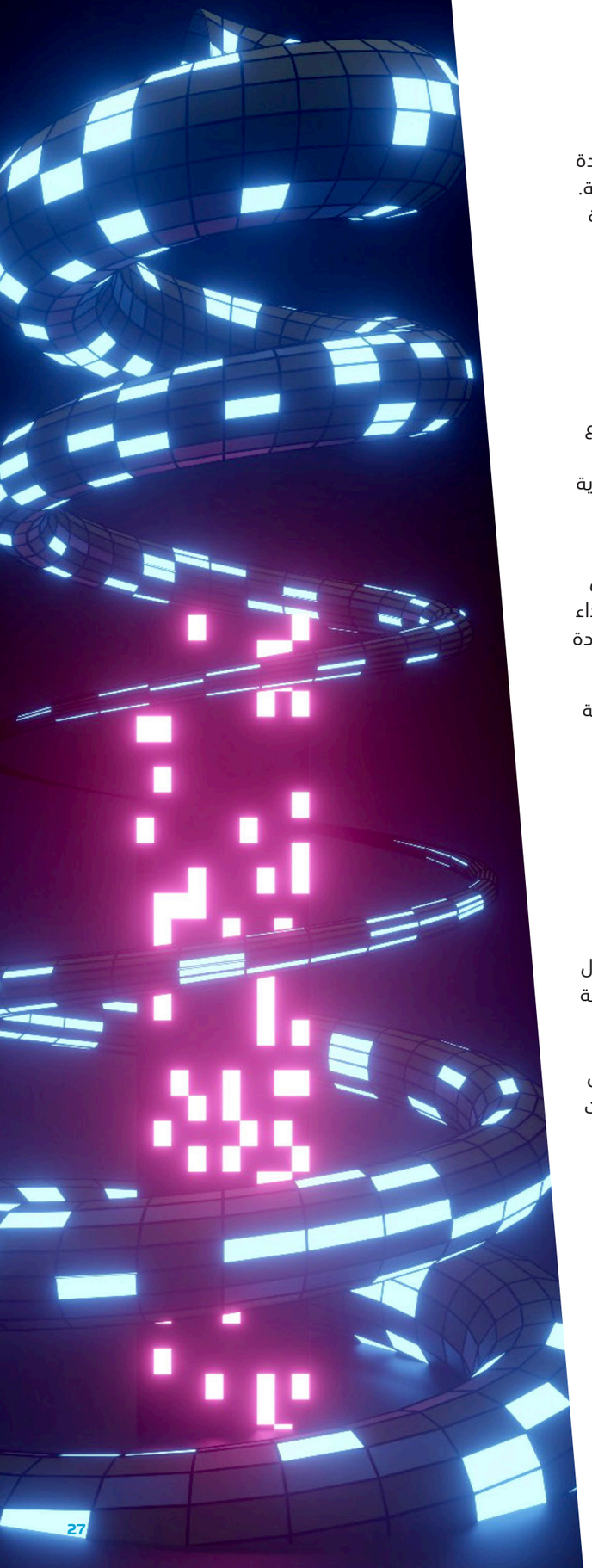
- تقييم وتحسين بنية النظام وتصميمه: يجب أن تتمتع الأنظمة الحرجة بالمرونة والسرعة والصمود بما فيه الكفاية، إذ لا ينبغي تحقيق الأمن الإلكتروني بعد فوات الأوان ويجب علينا دمج الأمن في تصميم بنية النظام. يجب على الجهة الحكومية تحديد مجموعة معينة من متطلبات الأمان التي تفرض سلامة الأمن الإلكتروني الرئيسية مثل التجزئة والحد الأدنى من مستوى الوصول والحد من ناقلات التهديد، وما إلى ذلك.

- تقييم ما إذا كانت الأنظمة والأدوات المستخدمة لمراقبة البنية التحتية تتضمن ثغرات أمنية رئيسية أم لا: طبقت الجهات الحكومية مجموعة متزايدة من الأدوات بغرض تقييم شبكاتها وأنظمتها لاكتشاف التهديدات وتطبيق أدوات التشفير لحماية المعلومات الحساسة. إلا أنه من الضروري أن تتحقق الجهات الحكومية من أن تلك الأدوات، في حد ذاتها، لا تشكل تهديدات أمنية إضافية.

- تقييم تقادم النظام: اعتمدت كل جهة حكومية إستراتيجيتها الخاصة لإدارة تقادم النظام، مثل السرعة التي تنتقل بها إلى الإصدارات الجديدة من البرمجيات أو الأجهزة، ونهج تصحيح المسار، ودرجة اعتماد الشركة (أو عدم اعتمادها) على الأنظمة التي لم تعد مدعومة من البائع. وبينما قد تكون الإستراتيجية العامة منطقية بالنسبة للجهة الحكومية ، فمن الضروري أن تثبت الجهات أنها قد درست بعناية اعتماد إستراتيجية متمايزة تمثل أهمية بالغة للأنظمة الحرجة. كذلك أظهرت هجمات برامج الفدية الأخيرة على مستوى العالم إمكانية تتبع حالات تعطل الأنظمة إلى حالات الاعتماد على الإصدارات القديمة وممارسات تصحيح المسار السيئة، حيث إن ذلك غير مقبول للأنظمة الحرجة.

إدارة الجهات الخارجية الحرجة وحالات الاعتماد الرئيسية الأخرى

تحتاج الجهة الحكومية إلى تقييم حالات الاعتماد على الجهات الخارجية، لا سيما تلك التي تدعم العمليات



والأنظمة الحرجة أو تتصل بها. وقد يشمل ذلك إعادة تقييم كيفية تحديد الموردين وحالات الاعتماد الحرجة. يجب تقييم الموردين الحرجين ووضعهم تحت مراقبة أشد من غيرهم. يتعين على الجهة الحكومية:

- تقييم مرونة الموردين وممارسات الأمن الإلكتروني: ويمكن تحقيق ذلك قبل تأهيل الموردين، ولكن قد يكون ذلك أمراً متعجلاً فيه للغاية ويحتاج إلى إعادة النظر، أو قد فات أوانه. ستحتاج الشركات إلى تحديد مدى سرعة الموردين في إنشاء نسخة احتياطية من أنظمتهم بعد وقوع بعض الأعطال، وإذا حدثت حالة تعطل ممتدة، فكيف يمكن للمورد تقديم الدعم لضمان استمرارية العمل.

- إدارة بنود العقود والالتزامات: تحتاج الجهة الحكومية إلى دمج شروط تعاقدية توضح مستوى الأداء إضافةً إلى المخاطر الرئيسية ومؤشرات الأداء التي يتعين على المورد استيفاؤها على وتيرة محددة مسبقاً.

- إجراء المراقبة المستمرة: ستحتاج الجهة الحكومية إلى إعادة تقييم نهجها لمراقبة الموردين الحرجين بصفة مستمرة. وفي حال عدم توفر مراقبة آنية، فإن المراقبة شبه الآنية (أي خلال اليوم) ستكون مطلوبة.

المرونة في الأمن الإلكتروني

إذ لا تزال الشركات بحاجة إلى إجراء أنشطة الكشف والاستجابة والاستعادة بصورة مستمرة حتى في حال وجود أفضل تخطيط على مستوى العالم. فهم بحاجة إلى التواصل بشكل فعال أثناء الأعطال المحتملة والفعلية. وعند حدوث هجمات إلكترونية، يجب على الجهة الحكومية التحرك بسرعة لاكتشافها والتصدي لها. أما إذا نجحت هذه الهجمات، فستحتاج الشركات إلى تحديد كيفية الرد. وفي سياق المرونة، تشمل محاور التركيز الرئيسية للهيئات التنظيمية والجهات الحكومية ما يلي:

- بناء قدرات الكشف: يعد الكشف عن المشكلات أمراً ضرورياً، فهو بمثابة شريان الحياة لتحقيق المرونة. ومن ثم يجب على الجهة الحكومية وضع برنامج من خلال جمع المعلومات عبر مصادر مختلفة وتحليلها واستخدامها لمواصلة تحسين الوضع الأمني.
- تعزيز قدرات الاستجابة: تعد القدرة على الاستجابة والعمل جزءاً أساسياً من المرونة، ويتحقق ذلك من خلال وجود برنامج استجابة للحوادث. إذ يجب أن يسهل البرنامج الانتقال الفعال من الاستجابة للحوادث إلى إدارة الأزمات. ويعد من أفضل الممارسات لاختبار خطة الاستجابة بانتظام من أجل تقييم الفاعلية والحفاظ على براعة الأطراف المعنية الرئيسية في أداء أدوارهم ومسؤولياتهم.
- تطبيق قدرات الاستعادة والتحسين باستخدام الاختبار: إن استعادة النظام بعد حدوث عطل أمر مهم، ومن ثم يتعين على الجهة الحكومية تحديد الحوادث الإلكترونية التي تمثل تحدياً خاصاً في مواجهة استعادة النظام عندما تكون الأنظمة معطلة. ويجب مراجعة مواقع الاستعادة بانتظام لضمان قابلية وصول عالية للأنظمة الحرجة. وتعد البيانات، بوصفها جزءاً من عملية الاستعادة، عنصراً مهماً أيضاً، من حيث التحقق من سلامتها وجودتها وضمان عدم التلاعب بها من قبل مهاجم ما أو برمجية ضارة.
- وضع خطط التصعيد والتواصل: يجب على الجهة الحكومية تحديد نهج للتصعيد السريع والفعال خلال أوقات الأعطال. إذ يجب تصعيد الاتصالات عند وقوع مشكلة وتنبيه الأطراف المعنية الرئيسية، مثل خط الدفاع الأول والإدارة العليا والمنظمين والعملاء، إذا لزم الأمر.

القسم الخامس

تطبيق نهج سريع لإدارة المخاطر الإلكترونية وتلبية متطلبات الامتثال

تحتاج الجهات الحكومية إلى اتخاذ خطوات حثيثة لتحديد المخاطر المرتبطة بأعمالها وإدارتها والحماية من الهجمات الإلكترونية من أجل تقليل أي تأثير على العمليات التجارية. إن وضع إستراتيجية لإدارة المخاطر الإلكترونية يمكن أن يساهم في اتخاذ قرارات مستنيرة بشأن المخاطر المرتبطة بالعمليات التجارية من منظور داخلي وخارجي.

ولم تعد إدارة المخاطر الإلكترونية أمراً اختيارياً، بل أصبحت ضرورية لمساعدة الجهة الحكومية على تحديد المخاطر الإلكترونية الرئيسية التي يمكن أن تؤثر على أعمالها. ومن ثم فإن الإلمام بالمخاطر وما يرتبط بها من تحمل المخاطر والإقبال عليها يمكن أن يوجه الجهة الحكومية في تخصيص ميزانية وموارد فعالة لتقليل التأثير المحتمل من خلال البدء في وضع ضوابط مناسبة بوصفها تدابير مضادة.

والهدف من عملية إدارة مخاطر الأمن الإلكتروني هو تحديد المخاطر الإلكترونية على أصول معلومات الجهات الحكومية وتقييمها والتخفيف من أثرها ومراقبتها. ويجب أن تكون هذه العملية منهجية وقابلة للتكرار، بحيث يمكن للجهة أن تكون على دراية جيدة بالمخاطر الإلكترونية الأساسية وتتخذ الإجراءات المناسبة لحماية أصولها.

العناصر الرئيسية للمرونة الإلكترونية

يتطلب تحقق المرونة في الأمن الإلكتروني اتباع نهج متكامل للحوكمة والمخاطر والامتثال من خلال مراعاة المخاطر والتهديدات إضافةً إلى قدرات المرونة. ومن أجل الحفاظ على منظومة بيئية مرنة، يعد تمكين وظائف الحوكمة الإلكترونية والمخاطر والامتثال داخل الجهات الحكومية أمراً بالغ الأهمية لتحفيز تلبية متطلبات الأمان الرئيسية عبر مختلف وحدات الأعمال. ويمكن لوظائف الحوكمة الإلكترونية والمخاطر والامتثال أن تستعين بسلسلة من التقييمات من أجل تحديد طبيعة المخاطر والتهديدات ذات الصلة، إضافةً إلى الاستفادة من معلومات التهديدات من المصادر الداخلية والخارجية. يمكننا شرح هذا النهج باستخدام الرسم البياني الموضح أدناه الذي يبدأ بتحديد أهمية الأصول من حيث السرية والسلامة والتوافر (CIA) وكذلك تحليل تأثر العمل (BIA) التقليدي الذي يضع في الاعتبار تأثير الأعطال على سير العمليات.

شكل 1

المرونة في الأمن الإلكتروني

نهج ثلاثي المحاور لتحديد المخاطر والتهديدات

حددنا نهجاً ثلاثي المحاور لمساعدة الجهات الحكومية على فهم موقفها من المخاطر وتحديد بيئة التهديدات المحيطة بها ومنح الأولوية لحماية الأصول الحرجة، باستخدام سلسلة من التقنيات والتقييمات التي أثبتت جدواها للجهات الحكومية، والتي تعمل في مختلف القطاعات في جميع أنحاء العالم.

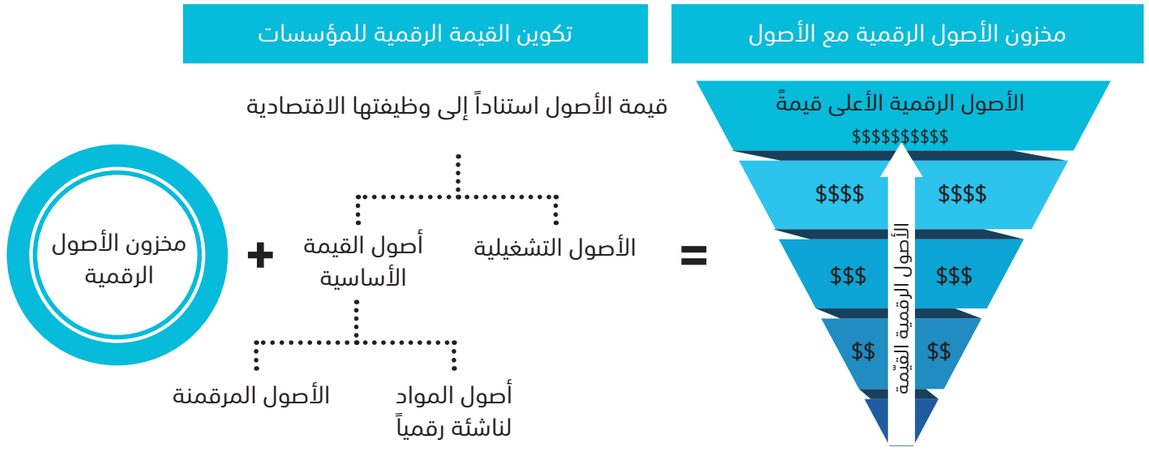
تحديد "الأصول الأعلى قيمةً" لدى الجهات الحكومية

عندما يتعلق الأمر بالأصول الأعلى قيمة لدى أي جهة حكومية، يتعين على الجهة إنفاق كل ما يلزم من أجل تأمينها. ويجب عليهم فعل ذلك مع التأكد من أنهم ينفقون أكثر من اللازم دون داعٍ كما سبق أن وضحنا ذلك في الشكل 2. ويمكن للجهات الحكومية تقييم قيمة مرونتها الإلكترونية من خلال أدوات النمذجة الاقتصادية المصممة وفق احتياجات الجهة.

حيث يساعد تطبيق نموذج اقتصادي إلكتروني في تحديد الأصول الأكثر أهمية التي تتطلب الحماية، وتحديد الخسائر الاقتصادية بعد التعرض لهجمات الأمن الإلكتروني. فمثلاً ما الخسارة المقدرة لجهة معينة في حال فقدها مليون سجل من سجلات العملاء وأصبحت هذه الخسارة علنية؟ من خلال استخدام هذا النموذج، يمكن للجهات الحكومية وضع رسم بياني يحدد كيف ستبدأ القيمة المعرضة للخطر في الانخفاض؛ لأنها تزيد من الضوابط الدفاعية لمنع الهجمات ذات الصلة بتصورات الخسارة الاقتصادية الإلكترونية.

شكل 2

نهج ثلاثي المحاور لتحديد المخاطر والتهديدات



أ. تصنيف الأصول من حيث السرية والسلامة والتوافر (CIA)

يمكن تحديد أهمية الأصول باستخدام نموذج أمن المعلومات الثلاثي؛ السرية والسلامة والتوافر. ينبغي أن تتمتع الجهة الحكومية بإشراف شامل على أصول معلوماتها، ويجب تصنيفها من خلال تقييم كل أصل وفقاً لنموذج السرية والسلامة والتوافر الثلاثي. ويمكن تنفيذ ذلك من خلال تحديد معدل تأثير كل عنصر داخل نموذج السرية والسلامة والتوافر الثلاثي وفقاً لمقياس محدد مسبقاً. على سبيل المثال، يمكن أن يتراوح مقياس معدل التأثير من منخفض إلى مرتفع. ومن ثم يمكن للجهة الحكومية أن تقيس الحد الأقصى للمعدل عبر عناصر نموذج السرية والسلامة والتوافر الثلاثة لكل أصل وتحديد أهمية الأصول وفقاً لذلك.

ومن شأن ذلك أن يساعد الجهات الحكومية على فصل الأصول غير الحرجة عن أنشطة تقييم المخاطر غير الضرورية التي تستغرق وقتاً طويلاً. يدعم هذا النهج وجود مستودع شامل للأصول الأعلى قيمةً يعكس مدى أهميتها وفقاً لنموذج السرية والسلامة والتوافر الثلاثي الذي يركز على تحديد أولوياتها من أجل اتخاذ خطوة تقييم المخاطر.

ب. نهج تكامل الأصول الأعلى قيمةً مع نموذج السرية والسلامة والتوافر

ثمة طريقة أخرى لعرض الأصول الأعلى قيمةً، ألا وهي النظر إلى العمليات التجارية بوصفها أصولاً يمكن أن تتعرض للمخاطر الإلكترونية. ومن ثم تصبح إجراءات العمل عاملاً أساسياً يجب على الجهات الحكومية مراعاته عند تحديد الأصول، على نحو يتوافق مع إجراء تحليل تأثر العمل (BIA).

ويمكن للجهة الحكومية الارتقاء بمستودع أصولها الأعلى قيمةً من خلال دمج أصولها الحرجة مع إجراءات العمل الأشد حرجاً في الجهة. ومن ثم فإن وجود نهج متكامل يساعد في بناء المرونة والجهود الإلكترونية جنباً إلى جنب من أجل تحقيق رقابة صارمة على المخاطر الإلكترونية داخل الجهة الحكومية.

وإضافةً إلى ذلك، يضيف دمج إجراءات الأعمال مزية كبيرة إلى مستودع الأصول الأعلى قيمةً تمكّن الجهات الحكومية من ربط أهداف زمن الاستعادة (RTO) وأهداف نقطة الاستعادة (RPO) بكفاءة في كل عملية تجارية. ويمكن للجهات الحكومية أن تشرف على تأثير الأعمال ومضاعفاتها في حال الاستغلال الناجح للأوضاع، مما يساعد في تخفيف أثر المخاطر على نحو مستنير واستباقي.

إجراء تقييم مخاطر الأمن الإلكتروني

أ. الاستفادة من المعلومات الخاصة بالتهديدات وملخصاتها

من الضروري الاستثمار في استخبارات التهديدات الإلكترونية (CTI) لفهم وضع الجهة الحكومية من حيث المخاطر والأساليب والتقنيات والإجراءات المحتملة (TTPs) وتقييم الطريقة التي يدبر بها منفذو التهديدات الهجمات ويديرونها. وغالباً ما ترتبط استخبارات التهديدات الإلكترونية (CTI) ارتباطاً وثيقاً بمطاردة التهديدات الإلكترونية (CTH) وتوفر رؤية للمخاطر المناسبة التي تسمح للجهات الحكومية بتحديد مجموعة قدرات المرونة المطلوبة لديها. وتعد مطاردة التهديدات الإلكترونية واحدة من أنشطة الدفاع الإلكتروني الفعَّالة. وهي عبارة عن عملية بحث استباقي ومتكرر عبر الشبكات لاكتشاف التهديدات المتقدمة التي تتهرب من الحلول الأمنية الحالية وعزلها.

تركز استخبارات التهديدات الإلكترونية على تحديد وتحليل الدوافع والأساليب والقدرات والأدوات الخاصة بالخصوم الذين قد يسعون لاستهداف إحدى الجهات عن طريق دمج تحليل خارجي بالبيانات التي كانت مقسمة في السابق داخل الجهة. وبينما قد تختار بعض الجهات الحكومية تعريف استخبارات التهديدات الإلكترونية بوصفها مكوناً أو خدمةً تعتمد على المدخلات، فمن الضروري ملاحظة أن دورة حياة الاستخبارات القائمة على العمليات ضمن إطار عمل تشغيلي تعد ضرورية لتقديم نتائج فعَّالة. ووفقاً لذلك، يلزم وجود برنامج شامل لاستخبارات التهديدات الإلكترونية يتألف من عمليات لجمع المعلومات الاستخبارية التكتيكية والإستراتيجية وإنتاجها ونشرها إلى جانب التعزيز المستمر لتحديثات التوعية بالأوضاع في الوقت المناسب (والتي تُعرف أيضاً باسم "الاستخبارات الحالية"). حيث يساعد ذلك في تحديد الخصم المعني، وطريقة مهاجمته للجهة وأسباب الهجوم، والإجراءات التي يمكن اتخاذها بعد التسوية الأوَّلية، وأين يمكنهم التواجد داخل الجهة، وطريقة اكتشاف الهجوم أو الرد عليه.

شكل 3

النهج المقترح للمعلومات المتعلقة بالتهديدات الإلكترونية

1. جمع وتحليل

التقنيات والموارد

المعلومات التكتيكية
- مستودعات المؤشر
- تغذية المؤشر والمجتمعات
- منصات التحليل

المعلومات الإستراتيجية
- منافذ التقارير المعلوماتية
- منصة تحليل التهديدات
- أدوات التصور
- معلومات المصادر المفتوحة

المعلومات الحالية
- تحليل وسائل التواصل الاجتماعي
- تحليل الويب العميق أو الخفي
- معلومات المصادر المفتوحة

الوظائف

دعم عمليات الأمن
- جمع المؤشرات
- تحليل سلسلة الهجوم
- دعم الصيد

مصفوفات التهديد وتحليل الاتجاه

البحث والتقرير والتقييمات

نمذجة التهديد

محاذاة الأعمال التجارية
- تقييم المخاطر
- تحديد الأولويات
- دعم القرار

الإنذار المبكر
- حملات الهجوم
- وسائل التواصل الاجتماعي
- الأحداث الجغرافية السياسية
- القدرات الناشئة

2. الدمج

قدرات الأمن الإلكتروني لفرق إرنست ويونغ

المراقبة الأمنية	الاستجابة للحوادث	إدارة الثغرات الأمنية
الهجوم والاختراق	الدفاع النشط	حماية الأصول ذات القيمة العالية

الأعمال التجارية لفرق إرنست ويونغ

المفاعلات المعيارية الصغيرة في الأعم	المفاعلات المعيارية الصغيرة في الصن
المفاعلات المعيارية الصغيرة الإقليمية	

خارجي

شركاء تبادل المعلومات وائتلاف الابتكار الصناعي

ينبغي دمج استخبارات التهديدات الإلكترونية التي جرى جمعها وإنتاجها من خلال عمليات مصممة لدعم المسؤولين عن اتخاذ القرارات والعمليات الأمنية والمسؤولين عن المرونة. ويجب تصميم عمليات الإدخال ونواتج برنامج استخبارات التهديدات الإلكترونية بهدف تحسين الوعي بالتهديدات الإلكترونية في جميع أنحاء الجهة الحكومية بأكملها عبر مختلف المستويات. وترى فرق عمل شركة إرنست ويونغ أنه يمكن تحقيق ذلك عندما يُنظر إلى استخبارات التهديدات الإلكترونية من خلال عدسة مكونات الاستخبارات "التكتيكية" و"الإستراتيجية" و"الحالية" وتسليمها إلى الأطراف المعنية بغرض تحديد خطط تحقيق المرونة في الأمن الإلكتروني واختبار آليات الاستجابة للأزمات الإلكترونية.

ب. تحديد المخاطر الإلكترونية الداخلية والخارجية

الهدف من تحديد المخاطر هو اتخاذ قرار حول ما يمكن أن يتسبب في وقوع خسارة محتملة، واكتساب معرفة متعمقة حول طريقة حدوث الخسارة ومكان وقوعها والأسباب التي أدت إلى حدوثها. ومن ثم يجب على الجهات الحكومية العمل على تحديد وتقييم المخاطر الإلكترونية الداخلية والخارجية المحتملة بوصفها خطوةً أوَّليةً للسيطرة على المخاطر. ويمكن التعامل مع تحديد المخاطر الإلكترونية من خلال نهج قائم على التصورات المحتملة أو نهج قائم على التصنيف إلى فئات من أجل الإلمام بالثغرات الأمنية ذات الصلة.

ج. تحليل المخاطر الإلكترونية وتقييمها

عندما يتعلق الأمر بتقييم المخاطر الإلكترونية، يجب على الجهات الحكومية مراعاة التأثير الذي يمكن أن تسببه المخاطر الإلكترونية المحتملة وإمكانية وقوع المخاطر، مما يؤدي إلى الإلمام بمعلومات تصنيف المخاطر الكامنة إلى مخاطر حرجة ومخاطر عالية ومخاطر متوسطة ومخاطر منخفضة. (التأثير × الاحتمال = المخاطر الكامنة).

ومن ثم يجب على الجهات الحكومية مواصلة تحليل تصنيف المخاطر الكامنة من خلال تحديد وتقييم الضوابط الأمنية المطبقة حالياً ومدى فاعليتها من أجل الكشف عن نقاط الضعف والثغرات الأمنية، وكذلك لفهم التأثير المنخفض وإمكانية الاستغلال الناجح للأوضاع، مما يؤدي إلى توفر معلومات حول المخاطر المتبقية، والتي تعد تصنيف المخاطر النهائي المستخدم في تصنيف مخاطر إلكترونية معينة.

ويمكن استخدام التقييمات الفنية في إطار تقييم المخاطر من أجل التحقق من المخاطر المحتملة على عناصر التكنولوجيا. وفي أغلب الأحوال، يُجرى تقييم الثغرات الأمنية واختبار الاختراق (VAPT) ومراجعة التكوين التي تتحقق من تطبيق ضوابط التحصين لاستكمال عملية تقييم المخاطر المعتادة. إلا أنه بناءً على المخاطر التي جرى تحديدها ومدى تعقيد عملية التطبيق، يوصى باستخدام تقنيات مراجعة إضافية مثل مراجعات الدمج وتحليل الشفرات الديناميكية، من بين أمور أخرى، لضمان اكتشاف جميع المخاطر المنفَّذة وتقييمها.

أنواع التقييمات الفنية التي يمكن استخدامها جنباً إلى جنب مع تقييم المخاطر لاكتشاف نقاط الضعف والثغرات الأمنية بدقة

- تقييم الثغرات الأمنية واختبار الاختراق (VAPT): يعد هذا التقييم أحد التقييمات الفنية الأكثر استخداماً، حيث يستهدف البنية التحتية الفنية للجهة الحكومية بالكامل استناداً إلى نطاق التقييم.

- مراجعة التكوين: تعد مراجعة التكوين جانباً أساسياً من جوانب تحصين النظام، ويتضمن ذلك مراجعة آمنة للتكوينات الأساسية لعنصر معين داخل النظام.
- اختبار الاختراق أو اختبار اختراق الفريق الأحمر: يعد هذا الاختبار تدريباً عملياً على الهجمات الناجحة بغرض تحسين دفاعات الأمن الإلكتروني للجهة الحكومية والتأكد من الاستعداد لحمايتها من الهجمات الحقيقية في ظل بيئة تشغيلية.

وضع خطط للتعامل مع المخاطر وعملية القبول

يجب على الجهات الحكومية وضع إدارة مخاطر الأمن الإلكتروني ومعالجتها في مقدمة أولوياتها، بسبب بيئة العمل التقنية المتغيرة باستمرار والتي تطرح مخاطر إلكترونية متزايدة دون أهداف محددة. ينبغي تركيز الجهود على معالجة المخاطر الإلكترونية الحرجة بشكل فعال وسريع حيثما ومتى لزم الأمر، تجنباً للعواقب غير المرغوب فيها.

وبعد الحصول على نتائج منظمة لتقييم المخاطر الإلكترونية، يمكن للجهات الحكومية تحديد المخاطر الأكثر حرجاً بناءً على تصنيف المخاطر المتبقية واتخاذ قرار مستنير على ضوئها بشأن كيفية المضي قدماً في معالجة المخاطر. وإذا كان خيار العلاج المقترح يميل إلى التخفيف، فإنه يجب على الجهة وضع خطة علاج فعَّالة يُجرى تحليلها والتحقق منها لمعالجة المخاطر الإلكترونية المحددة وحماية الجهة وفق نموذج السرية والسلامة والتوافر (CIA).

ولكن إذا كان خيار العلاج المقترح يشير إلى قبول المخاطر أو نقلها أو تفاديها، يجب على الجهة الحكومية وضع عملية إدارية لكل خيار علاج مقترح للتأكد من الإلمام بالمخاطر وإدارتها ومعالجتها على نحو جيد وفقاً للعملية التنظيمية المعتمدة.

أتمتة لوحات المعلومات وتكاملها لرصد المخاطر في الوقت الفعلي تقريباً

يجب على الجهات الحكومية التفكير في استخدام لوحة معلومات آلية لإدارة المخاطر تتكامل مع نتائج تقييم المخاطر. يمكن أن يساعد ذلك في الإشارة إلى تصنيفات المخاطر والمعلومات المرتبطة بها وإظهارهما بدقة على لوحة معلومات تنفيذية شاملة. تتمتع الجهات الحكومية التي تعمم هذا المستوى من العناصر التمكينية الناضجة بمزيد من التبصر والتحكم في مخاطرها الإلكترونية، حيث إنها تمكننا من الحصول على رؤية شاملة لفهم المخاطر التي تشكل أكبر تهديد لعمليات الجهة وأعمالها، وإدارتها وفقاً لذلك.

يساعد استخدام لوحة معلومات إدارة المخاطر في تحسين عملية مراقبة المخاطر من خلال تقديم عروض مرئية لمراجع إحصائية مركزة لنتائج تقييم المخاطر. يشكل هذا بصورة أساسية مراقبة تصنيفات المخاطر والتقدم المحرز في معالجة المخاطر المرتبطة بها. إضافة إلى ذلك، يمكن لمالكي الأصول تصور وضع المخاطر في لوحة معلومات موحدة، مما يوفر طريقة سهلة وفعَّالة لتحليل عواقب المخاطر الإجمالية ويمكن أن يساعد في اتخاذ الإجراءات التصحيحية اللازمة.

توضح لوحة معلومات إدارة المخاطر حالة مؤشرات الأداء الرئيسية للمخاطر في الجهة الحكومية (KPI) وتمكن موظفي الأمن الإلكتروني من مراقبة التقدم المحرز في أنشطة معالجة المخاطر، وتوضح لوحة المعلومات المكونات التالية (على سبيل المثال لا الحصر):

- عدد التهديدات المحددة
- النسبة المئوية للمخاطر المحددة عبر مقياس التصنيف
- متوسط المخاطر لكل مالك
- متوسط المخاطر المعالجة

تساعد أتمتة لوحة معلومات إدارة المخاطر في توصيل معلومات المخاطر بصورة أفضل بين الجهات المعنية، إذ توفر تقنيات التصور نظرة عامة سريعة على اتجاهات المخاطر الرئيسية وتسمح لموظفي الأمن الإلكتروني بإدارة المخاطر المحددة وتحديد أولوياتها.

تحقيق الامتثال من خلال إدارة المخاطر:

ينبغي أن يكون برنامج إدارة مخاطر الأمن الإلكتروني متوائماً ومتوافقاً مع المعايير الوطنية والدولية المعمول بها. ينبغي اعتبار اللوائح معياراً لأداء أنشطة تقييم المخاطر. تلتزم الجهات الحكومية بتحديد متطلبات الامتثال اللازمة استناداً إلى تشريع الجهة المعمول به والمهام الخاصة بالصناعة.

يُعرض عدم الامتثال للمهام المنظمة الجهات الحكومية نسبياً إلى المخاطر والتهديدات مثل العقوبات المالية والإضرار بالسمعة.

يمكن للمنظمات التي تتبع نظام إدارة مخاطر الأمن الإلكتروني وفقاً لمتطلبات الامتثال أن تحدد بسهولة الضوابط المقررة وتقيّم المخاطر الناشئة عن التقصير في الضوابط المقررة أو عدم تنفيذها على نحو فعال. وبذلك، يمكن للجهات الحكومية مراقبة وتتبع حالة الامتثال لكل ضابط من الضوابط نتيجةً لمخرجات تقييم المخاطر. إضافة إلى ذلك يمكن الاستفادة من وجود خطة علاجية للمخاطر لترسيخ خطة الامتثال العلاجية وفقاً لذلك.

يمكن للتعاون المستَثمَر بين إدارة المخاطر الإلكترونية وإدارة الامتثال أن يقترح منهجية موحدة لتحقيق كلا الجانبين مع تقليل الوقت والجهد المخصصين لكل مهمة على حدة.

القسم السادس

إدارة استمرارية الأعمال وتعريف الاستجابة وإستراتيجيات التعافي

مع التطور المستمر في عالم الرقمنة، يعتمد المشهد الاقتصادي الحالي العالمي على الحلول القائمة على التقنية والعمليات الرقمية أو الآلية. معظم هذه الأشياء مفتوحة على العالم بأكمله عبر الإنترنت. وهذا ينشئ مساحة من التهديد الإلكتروني الذي يفرض على الجهات الخدمية والحكومية الاستثمار في إدارتهم والتوجه نحو حماية خدماتهم. لذا؛ ينبغي دمج مفاهيم المرونة في الأمن الإلكتروني في أنشطة استمرارية الأعمال المؤسسية لضمان توافر خدماتهم الأساسية وتقليل تأثير الاضطراب على الخدمات المقدمة للمنتفعين.

تكمن أحد أبرز منهجيات التعامل مع المرونة في الأمن الإلكتروني في استمرارية الأعمال في استخدام نهج المخاطر على مستوى الجهة الحكومية. تسعى هذه المنهجية إلى دمج أنشطة إدارة مخاطر استمرارية الأعمال والتي تُنفذ على المستوى المؤسسي بما في ذلك المجال الإلكتروني.

وعلى الجانب الآخر، فعند تحديد المخاطر الإلكترونية، ينبغي مراعاة مخاطر استمرارية الأعمال من ناحية:

- الجانب التشغيلي مثل سلامة ورفاهية ومدى توافر الموظفين المسؤولين عن الإدارة وأداء الأنشطة اليومية الإلكترونية. قد تتسبب استمرارية أنشطة الإدارة الإلكترونية وأنشطة المتابعة مثل الأعطال في عدم الظهور لمساحة التهديد المؤسسية والانتهاكات المحتملة.
- منظور التأثير المتتالي والمترابط. وخير مثال على ذلك انقطاع الكهرباء الذي يُنظر إليه بوصفه اضطراباً بسيطاً غير متعمد، قد يكون في الواقع خللاً متعمداً ضمن جزء من الهجوم الإلكتروني المتقدم للتغلب على ضوابط الأمن المادي، والضوابط الموجودة في المكان مثل كاميرات المراقبة.

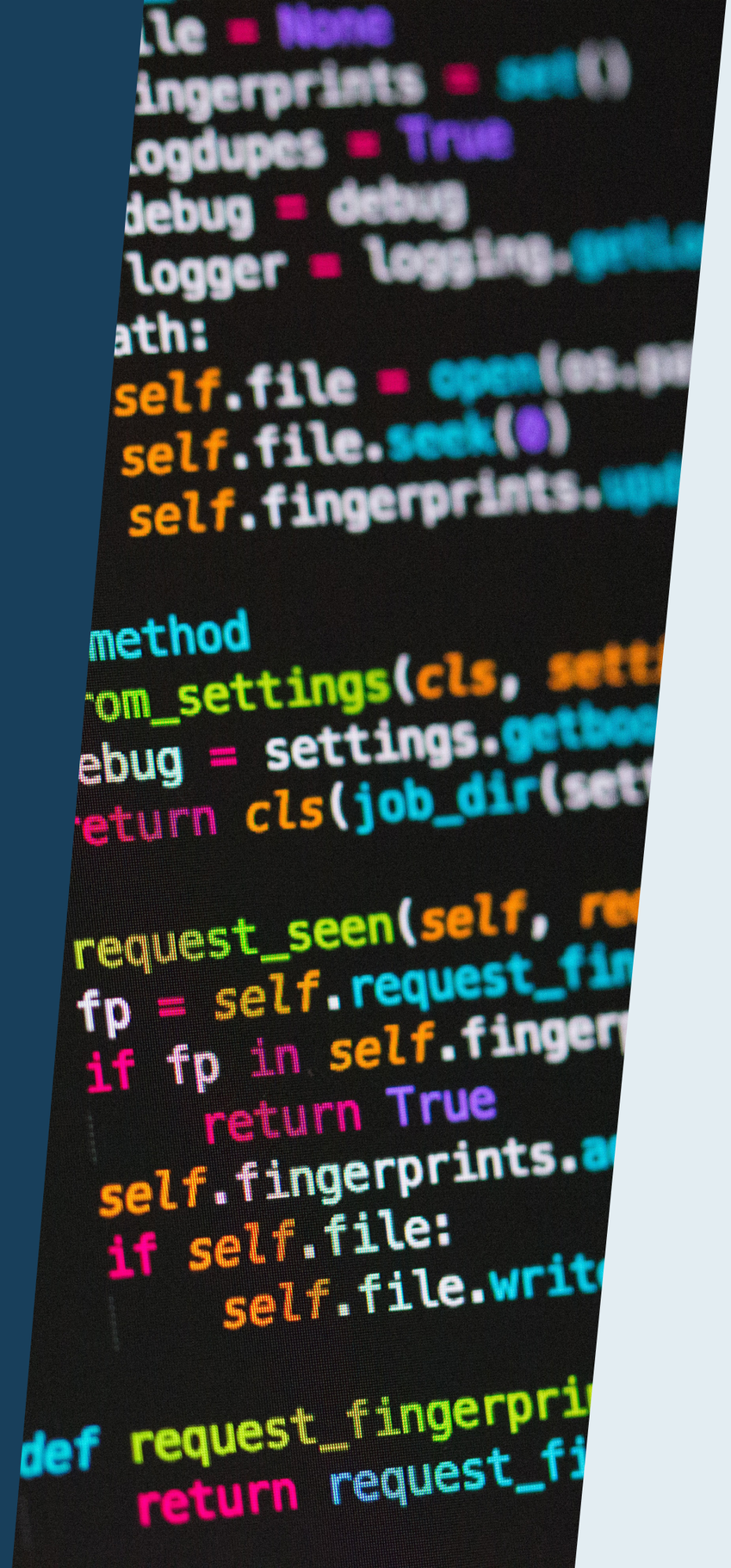
يتطلب تقييم ملف مخاطر الجهة الحكومية تعريف الخطط العلاجية للمخاطر، حيث يشكل هذا اللبنة الأساسية في تعريف إستراتيجيات وحلول المرونة المناسبة. وفر المجال رقم ISO of 17 Domain 27001 2013: توجيهاً مناسباً للجهات الحكومية التي ترغب في أن تتبنَّى الاستمرارية في قدراتها الإلكترونية. ينبغي أن تغطي هذه الإستراتيجيات والحلول عدة دعائم أساسية تشمل الناس والتقنية والموقع والسجلات الحيوية والتقنيات التشغيلية والمتطلبات التشغيلية. ينبغي إدراج ملف المخاطر الإلكترونية ضمن جزء لا يتجزأ من هذه الأنشطة.

نقطة التقاء أخرى بين المرونة في الأمن الإلكتروني واستمرارية الأعمال ألا وهي خطط الاستجابة والتعافي. ينبغي أن تحدد هذه الخطة خطوات العمل في عملية استئناف العمليات ضمن فترة زمنية مستهدفة للتعافي.

ومما له أهمية قصوى كذلك أن نجد الخطة المحددة مقيَّمة لضمان السريان والفاعلية في المواقف المعاكسة. يمكن للجهات الحكومية عمل محاكاة للأمن الإلكتروني ليس لاختبار الخطة فحسب، بل لمعرفة مدى وعى الأطراف المعنية الرئيسية بمسؤوليتهم خلال حالات الأعطال أو الأزمات أو بناء الخبرة.

وأخيراً، للتكيف مع الأوضاع بعد وقوع عطل، سواء كان إلكترونياً أو غير إلكتروني، أهمية كبيرة، حيث يمكن أن يجعل الوضع اعتيادياً في الجهة. فعلى سبيل المثال، طبقت معظم الجهات الحكومية مفهوم العمل عن بُعد لتتناول مخاطر الاستمرارية خلال جائحة كوفيد-19. يتجلى هذا في العديد من الجهات الحكومية بوصفه حلاً أكثر فاعلية من ناحية التكلفة مقارنةً باستخدام موقع بديل للعمل أو حتى الموقع الرئيسي، مما يؤدي إلى ظهور نماذج تشغيل جديدة. وبذلك فإن العمل الافتراضي هو الوضع الاعتيادي الجديد ويستلزم ذلك تنفيذ ضوابط إلكترونية محكمة لضمان المرونة.

وفي النهاية، فإن المرونة هي الانضباط التنظيمي والسرعة في تطوير القدرات والتعزيز الدائم لها بهدف ضمان التسليم المستمر للخدمات الرئيسية بما في ذلك الأمن الإلكتروني. ينبغي أن تتبنَّى الجهات الحكومية مفهوم الإلمام بالحالة والتعاون الذي يرسخ المرونة في ثقافتها.



القسم السابع

الخاتمة

تعمل التقنيات الجديدة على تسريع وتيرة التغير الرقمي والاستخدام الواسع النطاق للأتمتة وتحليلات البيانات والسحابة. تهتم الحكومة والجهات الحكومية بشكل متزايد بقدراتها فيما يتعلق بالمرونة وتتطلع إلى توفير نهج أكثر أماناً وتأميناً وبأسعار معقولة لتأمين أنظمتها وبياناتها. فقد يكون الانتهاك القادم من مورد أو طرف ثالث أحد أكبر المخاطر التي يواجهونها.

مع التركيز على المعلومات، والاتصالات، والتكنولوجيا (ICT) وخدمات الإدارات الأخرى ومنتجاتها، تتطلب الحكومة والجهات الحكومية فهمًا أفضل للمخاطر المحتملة التي يمكن أن يشكلها الاعتماد على المورد على الجهة، والأصول المهمة التي قد تكون مستهدفة، والمخاطر الإلكترونية التي قد تنجم عن الأشخاص والعمليات والتقنيات. من خلال فهم المخاطر المحتملة، ستكون القيادة أو الإدارة العليا قادرة على اتخاذ قرارات مستنيرة بشأن المخاطر فيما يتعلق بإجراءات الحد من وطأة المخاطر المحتملة.

إذا قبلنا أن التعرض لشكل من أشكال الهجوم الإلكتروني أمر لا مفر منه، فستزداد أهمية تطبيق الجهة الحكومية لأنظمة وإستراتيجيات تعمل على إعادة العمل كالمعتاد بأسرع طريقة ممكنة، والتعلم مما حدث، والتكيف وإعادة تصميم الجهة الحكومية لتحسين المرونة في الأمن الإلكتروني في المستقبل. ومن الضروري أن يكون لدى الحكومة والجهات الحكومية برنامج مركزي للاستجابة للاختراق الإلكتروني على مستوى كل جهة (CBRP) أو خطة لإدارة الأزمات الإلكترونية تجمع بين مجموعة واسعة من المعنيين الذين يجب أن يتعاونوا لمعالجة الخرق. ويجب قيادة هذا البرنامج من قِبل شخص ذي خبرة في التكنولوجيا وقدرة على إدارة الاستجابة التشغيلية والتكتيكية اليومية. كما يجب أن يتمتع هذا القائد بخبرة متعمقة في القانون والامتثال، إذ يمكن لأي خرق إلكتروني أن يؤدي إلى مشكلاتٍ قانونية وتنظيمية معقدة ذات تأثيرات مالية.

عندما يتعلق الأمر بحوكمة الأمن الإلكتروني، فإن أحد أهم الأشياء التي يمكن للجهات الحكومية القيام بها هو تحديد المسار المناسب لتنفيذ ذلك والتوافق مع الإدارة بشأن التحمل المناسب للمخاطر المتعلقة بالأمن الإلكتروني.
ويمكن للإدارة العليا للجهات الحكومية إرسال هذه الرسالة جزئياً من خلال حوكمتها والتركيز على الأمن الإلكتروني. فمن الضروري أن تأخذ الإدارة العليا الأسئلة التالية في اعتبارها: كم من الوقت يقضيه المعنيون الرئيسيون في الأمن الإلكتروني على مدار العام؟ هل يوضع الأمن الإلكتروني على جدول أعمال الاجتماعات مرة واحدة في السنة أم أنه جزء من معظم الاجتماعات؟

الإدارة العليا هي المسؤولة بشكل أساسي عن الإستراتيجية وإدارة المخاطر، ومن المستحيل فعليًا إجراء هذه المحادثات دون مناقشة شاملة حول التكنولوجيا والأمن. الإدارة العليا التي تركز بصورة مناسبة على الأمن الإلكتروني هي تلك التي تدمج الموضوع باستمرار في مناقشات منتظمة حول الإستراتيجية والمخاطر، وتعطي الأولوية للتعليم الذاتي وتطلب المشورة الخارجية لتعزيز الكفاءة الإلكترونية للجهة. كما تجري مناقشات غير منقحة مع كبير مسؤولي أمن المعلومات (CISO) في الجلسات التنفيذية وترسل باستمرار رسالة واضحة إلى الإدارة مفادها أن إعطاء الأولوية للأمن الإلكتروني هو جزء لا يتجزأ من الجهة الحكومية.

جزء مهم آخر من تحديد المسار المناسب وهو التأكيد على أن المخاطر الإلكترونية ليست مجرد مشكلة تتعلق بتكنولوجيا المعلومات ولكنها مشكلة على مستوى الجهة الحكومية تشمل جميع الأقسام والوظائف. ووفقًا لذلك، تحتاج الإدارة، بخلاف مهمة الأمن، إلى أن تكون ضليعة بشأن الضوابط والإجراءات التي تحمي عملياتها، وكيفية تدريب الموظفين واختبارهم بدءاً من الإدارة ووصولاً إلى الخط الأمامي، وماهية البروتوكولات التي يجب اتباعها في حال وقوع اختراق أو حادثة إلكترونية.

من خلال اتباع نهج فعَّال للرقابة والحوكمة الإلكترونية، تلعب الإدارة العليا دورًا مهمًا في تشجيع أصحاب الاختصاصات والأقسام على تولي مسؤولية أكبر تجاه المخاطر الإلكترونية، ويتعين عليها فهم ما إذا كان يتم تقاسم مسؤولية الأمن الإلكتروني عبر الجهة الحكومية وكيف يتم ذلك.

دمج الأمن الإلكتروني في محادثات الإدارة العليا الشاملة مع جميع كبار المدراء التنفيذيين وقادة الأقسام يوضح أن الأمن الإلكتروني جزءٌ لا يتجزأ من العمليات في جميع أنحاء الجهة، وأن القادة مسؤولون عن دورهم في دعم البنية التحتية للأمن الإلكتروني. إن إعطاء الأمن الإلكتروني الأهمية نفسها التي تحظى بها الشؤون المالية والقانونية في القرارات الحاسمة، يعزز الرسالة بأنه أمر مهم في إطار العمل.

دعوة للعمل

قد يكون إنشاء نهج شامل قائم على الأعمال لمكافحة الهجمات الإلكترونية أمرًا مربكًا حينما يكون لدى الجهة الحكومية بالفعل اضطراب في العديد من الجبهات المختلفة. ومع ذلك، يجب أن يكون الأمن الإلكتروني من أولويات العمل الأساسية ويجب أن يحظى بأولوية قصوى من قِبل الحكومات الحديثة والجهات الحكومية. فيما يلي أهم 10 أشياء يجب على الإدارة أخذها في الاعتبار أثناء تنفيذ خطط المرونة في الأمن الإلكتروني:

1. دمج الأمن الإلكتروني في إستراتيجية المواهب وإنشاء دور لكبير مسؤولي أمن المعلومات بما يتناسب مع غرض الجهة الحكومية. ويجب أن يتمتع كبير مسؤولي أمن المعلومات (CISO) بالمرونة لتحديد هيكل تنظيمي يأخذ مجموعة واسعة من العوامل في الاعتبار ويضع المرونة على رأس مخططات الأولويات الخاصة به.

2. تحديد مسؤوليات الأمن الإلكتروني لدى الجهة الحكومية بوضوح وإنشاء مصفوفة توزيع المسؤوليات (RACI matrices) والتي تشرح مسؤولية جميع المعنيين المشاركين في الحفاظ على المرونة الإلكترونية خلال وقوع أي حادث والمساءلة التي يخضعون لها وأدوارهم التي تم التشاور بشأنها والإبلاغ بها.

3. وضع الأمن الإلكتروني في طليعة إستراتيجية عمل متعددة المهام. فيجب ألا يُنظر إلى ذلك على أنه مشكلة تتعلق بتكنولوجيا المعلومات وينبغي النظر إلى وظائف الأمن الإلكتروني على أنها عامل تمكين من قِبل وظائف الأعمال الداعمة. كما يجب أن تُعمم خطط المرونة على جميع المعنيين ويتم إبلاغهم بها.

4. التأكد من أن الأمن الإلكتروني هو جوهر الابتكار الرقمي وعامل مساعد له وليس عائقاً أمامه. فالتحدث عن تضمين مفهوم "الثقة عن طريق التصميم" أسهل من تنفيذه. ومن ثم، من الضروري للإدارة التنفيذية توفير الدعم للجوانب والمتطلبات الأمنية مع إيصال أهمية إدارة المخاطر الإلكترونية والمرونة في الأمن الإلكتروني عبر جميع وحدات الأعمال.

5. فهم كيفية تأثير القواعد التنظيمية على العمليات، والعمل مع الهيئات التنظيمية لإرساء قدرات المرونة في الأمن الإلكتروني التي تعالج المتطلبات الأساسية. فيجب النظر إلى الهيئات التنظيمية على أنها شريك أساسي وليس للحفاظ على الامتثال فحسب، بل لضمان تنفيذ المتطلبات الأساسية بطريقة سلسة وتحديد جميع التحديات في المراحل الأوَّلية.

6. تحديد معدل المخاطر لجميع أصولك الرئيسية ووضع نهج حماية لكل أصل مع التركيز على الأصول الأكثر أهمية. يُعد تحديد مدى أهمية كل أصل مطلبًا حاسمًا لكل جهة حكومية؛ لأنه يترتب على ذلك تحديد مستوى الحماية والذي سيتم تطبيقه على الأصول. فحماية كل أصل داخل الجهة بالدرجة نفسها من الضوابط ليس نهجًا ممكنًا، ومن ثم، من الضروري اتباع نهج أكثر واقعية ينظر إلى الخطر على أنه عنصر أساسي.

7. وضع نموذج ديناميكي وسريع الاستجابة لإدارة مخاطر الأمن الإلكتروني لتمكين الجهة الحكومية من توسيع النطاق إذا كان هناك تصعيد للمخاطر الخارجية أو قرار لتغيير القدرة على تحمل المخاطر المؤسسية.

8. دمج الامتثال في إستراتيجية الأمن الإلكتروني، بحيث تُعاد قيمة أي أموال مستثمرة في الامتثال من خلال توفير دفاع مناسب للجهة الحكومية.

9. تعزيز المرونة من خلال وجود خطة عمل واتصال واضحة للأزمة عندما تسوء الأمور، بحيث يمكن التفكير ملياً في إدارة الأزمات والاستمرارية وممارستها على جميع مستويات الجهة الحكومية.

10. التعاون مع الأقران للبحث عن المزيد من الحلول داخل القطاعات. فالمخاطر الإلكترونية الحالية تهدد النظام البيئي الحكومي بأكمله، وقد يؤدي فشل أحد اللاعبين الرئيسيين إلى الإضرار بسمعة المجال بأكمله.

وفي الختام، لم يعد كافياً النظر إلى المرونة في الأمن الإلكتروني على أنها فكرة مستدركة؛ يجب تضمين نهج الجيل التالي للحوكمة والمخاطر والامتثال في نظام الحصانة الخاص بالحكومة والجهات الحكومية بوصفه درع حماية في عالم يسوده عدم اليقين وتتزايد به التهديدات الإلكترونية.

المراجع:

1. https://www.ey.com/en_vn/ey-global-information-security-survey-2021
2. Tom, Burt, 4 November 2022. “Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression,” Microsoft Corporate Vice President, Customer Security & Trust (Burt, 2022).
3. Link to reference: https://www.crowdstrike.com/resources/reports/global-threat-report/
Direct link to report: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf
4. https://thehackernews.com/2022/12/chinese-hackers-target-middle-east.html
5. https://www.securitymagazine.com/articles/97549-winnti-apt-group-stole-trillions-in-intellectual-property
6. https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/
7. https://www.interpol.int/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL
8. https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/
9. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf, 21 September 2021
10. https://www.fincen.gov/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions, 07 March 2022
11. https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security
12. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5634
13. https://www.congress.gov/bill/117th-congress/senate-bill/965
14. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice
15. https://www.cisa.gov/circia
16. https://www.sec.gov/news/press-release/2022-39
17. https://www.congress.gov/bill/117th-congress/senate-bill/2629/text

لمزيدٍ من القراءة:

- ENISA — Threat Landscape Report 2022
- EY — Thought Leadership — Cyber resilience: evidencing a well-thought-out strategy
- EY — Thought Leadership — An integrated vision to manage cyber risk
- EY — Thought Leadership — Why proactive beats reactive in Cybersecurity today?
- EY — Thought Leadership — Cybersecurity in the age of geopolitical rises and global uncertainties
- EY Global Information Security Survey 2021 — Cybersecurity: How do you rise above the waves of a perfect storm?
- Gartner — How Geopolitics Impacts the Cyber-Threat Landscape
- Harvard Business Review — Is Your Board Prepared for New Cybersecurity Regulations?
- World Economic Forum — Global Cybersecurity Outlook 2022 — January 2022

المساهمون

سامر محمد عمر
شريك/ مدير أول
samer.m.omar1@sa.ey.com

سلام شومان
قائد فريق
salam.shouman@jo.ey.com

فادي موسى
قائد
fadi.mousa1@sa.ey.com

سيدهش مدباتكال
مدير
siddhesh.mudbhatkal@mu.ey.com

إياد حداد
مدير
eyad.haddad1@sa.ey.com

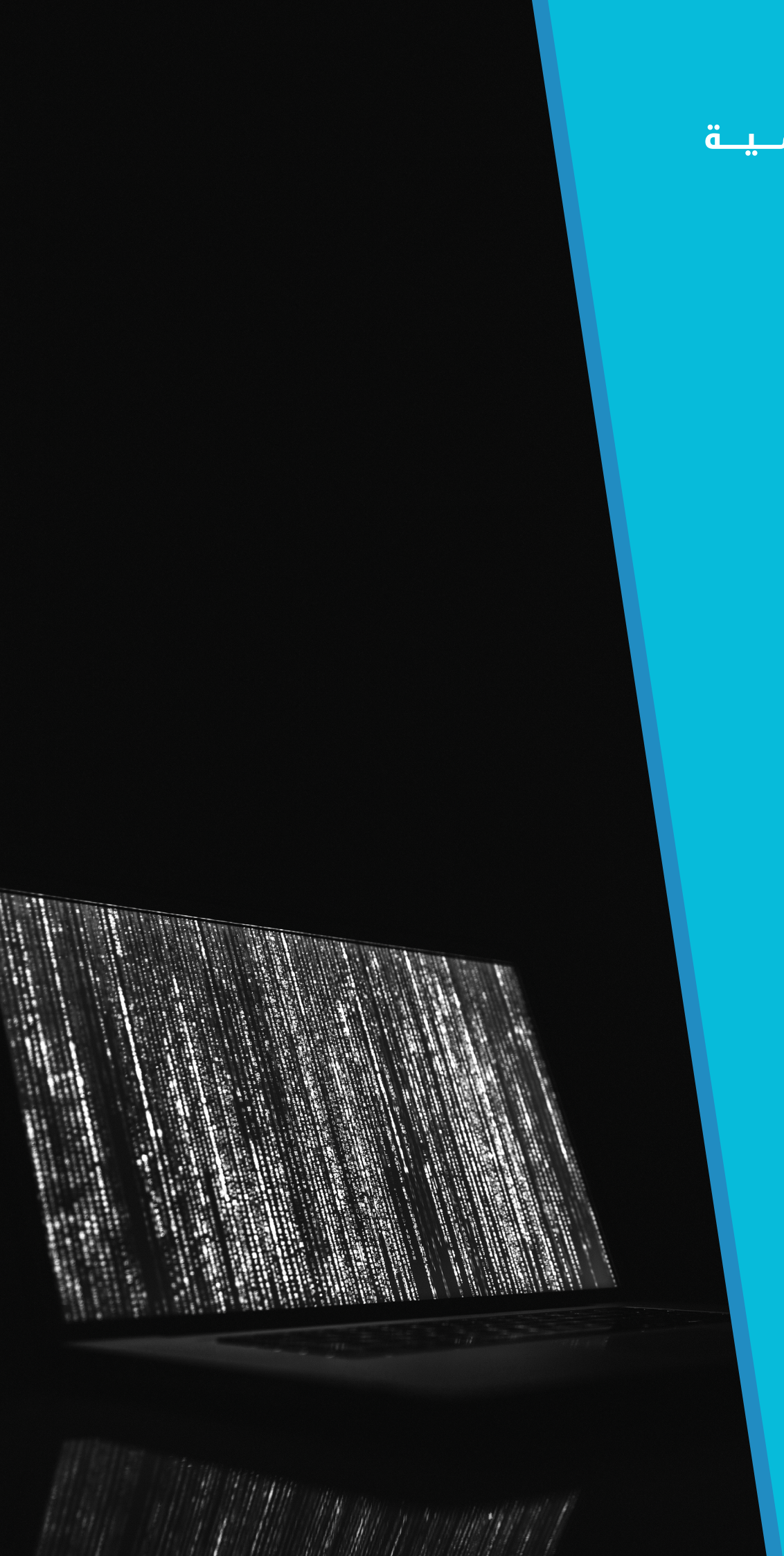
إدمارك م بيلونز
مدير
edmark.m.billones@ae.ey.com

شذى المطيري
مدير
shatha.almutairi@sa.ey.com

مصعب أبو طه
مستشار أول
musab.abutaha@jo.ey.com

ياسمين عبد الله
مستشار أول
yasmeen.abdullah@jo.ey.com

شوكت النابلسي
مستشار أول
shawkat.alnabulsi@jo.ey.com



القمة العالمية للحكومات

@WorldGovSummit

#WorldGovSummit

مع أطيب التحيات

worldgovernmentsummit.org