منظمة الصحة العالمية

**المجلس التنفيذي** **م ت١٤٨/٣٠**
**الدورة الثامنة والأربعون بعد المائة** **١١ كانون الثاني/ يناير ٢٠٢١**
**البند ١٨-١ من جدول الأعمال المؤقت** **EB148/30**

# معلومات محدّثة عن إدارة وتكنولوجيا المعلومات

## تقرير من المدير العام

١- خلال الاجتماع الحادي والثلاثين للجنة البرنامج والميزانية والإدارة التابعة للمجلس التنفيذي في كانون الثاني/ يناير ٢٠٢٠، قدمت الأمانة تقريراً عن مبادراتها بشأن الأمن الإلكتروني.[١] وبالإضافة إلى ذلك، أبرز أحدث تقرير لمراجع الحسابات الداخلي، الذي نظرت فيه اللجنة خلال اجتماعها الثاني والثلاثين، العناصر الرئيسية لمراجعة خريطة طريق الأمن الإلكتروني.[٢] ويأتي هذا التقرير استجابةً لطلب اللجنة من الأمانة أن تقدم تقريراً عن إدارة الأمن الإلكتروني.

## التقدم المحرز قبل انتشار الجائحة

٢- الأمن الإلكتروني هو أحد مجالات النتائج الرئيسية في استراتيجية إدارة وتكنولوجيا المعلومات. والغرض المستهدف منه هو حماية الأصول الرقمية للأمانة، وتعزيز أمن البيانات، وضمان القدرة على تقديم الخدمات في ظل مستوى مقبول من المخاطر.

٣- وتشمل المبادرات المتخذة دعماً للأمن الإلكتروني تنفيذ تدريب إلزامي على نطاق المنظمة للتوعية بالأمن الإلكتروني؛ وإجراء تمارين منتظمة بشأن التصيُّد الإلكتروني شهرياً؛ وإطلاق الحدث السنوي للتوعية بالأمن الإلكتروني؛ وإنشاء مستودع مركزي لتسجيل حركة النظم لأغراض الاستدلال الجنائي؛ وتوحيد تنظيم الحواجز الوقائية؛ ونشر حل عالمي لمكافحة الفيروسات؛ وتنفيذ خدمة لتنقية حركة المرور على شبكة الإنترنت؛ وتفعيل المعلومات الاستخبارية عن التهديدات بحيث يمكن اتخاذ تدابير استباقية لتجنب الحوادث المستقبلية والتي يمكن التنبؤ بها.

٤- كما أنشأت الأمانة فريقاً مخصّصاً ومستقلاً في مجال الأمن الإلكتروني. وعلاوةً على ذلك، شرعت في إنشاء مركز للعمليات الأمنية المتكاملة يفي بالغرض، ويشمل تقصّي الهجمات الإلكترونية ومنعها واكتشافها واتّقائها ومواجهتها عند وقوعها.

٥- وتم تعزيز مجال الحوكمة من خلال: نشر استراتيجية الأمن الإلكتروني المعتمدة، وخريطة الطريق بشأن الأمن الإلكتروني، وسياسات الأمن الإلكتروني والقواعد والمعايير وإجراءات التشغيل الموحدة على الصعيد العالمي؛ وإنشاء مجلس الأمن الإلكتروني؛ ومراجعة ميثاق اللجنة التوجيهية العالمية المعنية بتكنولوجيا المعلومات لتلبية الحاجة إلى إيجاد مسؤولية شاملة عن الأمن الإلكتروني.

---

١ الوثيقة م ت١٤٦/٤٠.

٢ الوثيقة ج٧٣/٢٨.

## مواجهة الهجمات ذات الصلة بكوفيد-١٩

٦- منذ الإعلان عن جائحة كوفيد-١٩، لاحظت الأمانة تزايد الهجمات الإلكترونية المستهدفة. وتشمل هذه الهجمات التصيّد الاحتيالي، وسرقة الهوية، والتصيّد الإلكتروني الصوتي، والهجمات على البنية التحتية والتطبيقات المتصلة بتكنولوجيا المعلومات. فخلال الفترة بين آذار/ مارس وأيار/ مايو ٢٠٢٠، تم تسجيل أكثر من ١٣٠ ٠٠٠ من النطاقات المتعلقة بكوفيد-١٩، قدّر الباحثون أن ٧٠٪ مزيفة وأنها استُخدِمت لشنّ هجمات إلكترونية متعددة.

٧- ولا تفتأ الهجمات الإلكترونية تزداد بدرجة كبيرة من حيث الحجم والتعقيد. وقد اعتُبِر أن الحل الأوّلي المتمثّل في جمع معلومات استخبارية عن التهديدات غير كافٍ. وتم تنفيذ حل جديد في ٧ أيار/ مايو ٢٠٢٠، كشف عن تهديدات أخرى من جماعات متقدمة تشكّل تهديداً مستمراً. وأتاح ذلك للأمانة أن تعمل بشكل أسرع في إصلاح البنية التحتية والنظم والأدوات القائمة المتصلة بتكنولوجيا المعلومات.

٨- بيد أنه استناداً إلى تحليلات الاتجاهات التي أجرتها شركات متخصصة في الأمن الإلكتروني، من المتوقع أن تستمر الهجمات الإلكترونية. وينبغي تكثيف الجهود الرامية إلى تحديد هذه الهجمات الإلكترونية ومنعها والحماية منها والكشف عنها والتصدي لها والتعافي من آثارها. ونتيجةً لذلك، عجّلت الأمانة بتنفيذ برنامج الأمن الإلكتروني. وقد اتُّخِذت إجراءات رئيسية، بما في ذلك الإجراءات المبيّنة أدناه.

(أ) **التمويل.** ذكر تقرير مراجع الحسابات الداخلي في تشرين الأول/ أكتوبر ٢٠٢٠ أن مبلغ ١,٣ مليون دولار أمريكي كان غير ملائم لتنفيذ خريطة طريق الأمن الإلكتروني.[١] وقد وفّرت اللجنة التوجيهية العالمية المعنية بتكنولوجيا المعلومات مبلغاً إضافياً قدره ٤,٧ مليون دولار أمريكي، خَصَّصَ للبرنامج ما مجموعه ٦ ملايين دولار أمريكي.

(ب) **الفريق المعني بالأمن الإلكتروني.** تمت زيادة حجم الفريق من ستة أعضاء إلى ١١ عضواً، مع وجود موارد في جنيف وبودابست. وأنشئ *فريق لمواجهة الطوارئ* لشنّ أعمال هجومية من أجل التحقق من أمن نظم تكنولوجيا المعلومات، بما في ذلك تحديد مكامن الخلل في النظم وتقييم المخاطر.

(ج) **إنشاء مركز مُوَجَّه ومتكامل للعمليات الأمنية.** في حزيران/ يونيو ٢٠٢٠، أُنشئ مركز مُوَجَّه للعمليات الأمنية، تُدمج فيه العمليات الأمنية مع دائرة لإدارة المعلومات والأحداث الأمنية. ويوفر المركز رؤية واضحة لجميع الحوادث الأمنية، ويتيح للأمانة التركيز على الأحداث الأمنية التصعيدية. وفيما بين آب/ أغسطس وتشرين الثاني/ نوفمبر ٢٠٢٠، تم تقصّي ١٤,٥ مليار حدث أمني. وبتفعيل مركز العمليات الأمنية، تمكّنت الأمانة من تنقية بيانات الحوادث ومعالجتها وتحليلها وتركيز جهودها على ٢٤٣ حادثاً أمنياً تصعيدياً.

(د) **تحسين إنفاذ التحقق من المستخدمين.** تعكف الأمانة على تعزيز أساليب التحقق التقليدية (مثل التحقق من اسم المستخدم وكلمة المرور) بخدمات تحقق متعددة العوامل (مثل الشارات المرنة) لإثبات هوية المستخدم. وقد اكتمل الإنفاذ الكامل للتحقق المتعدد العوامل، ويغطي جميع خدمات الأمانة المتاحة على شبكة الإنترنت.

---

١ الوثيقة ج٢٨/٧٣.

(هـ) **الرصد المستمر لأصول تكنولوجيا المعلومات في المنظمة.** نفّذت الأمانة حلاً لكشف نقاط النهاية والتفاعل معها لتلبية الحاجة إلى الرصد المستمر للتهديدات التي تتعرض لها أصول تكنولوجيا المعلومات بالمنظمة والتصدي لها باستخدام أدوات لكشف الأنشطة المشبوهة واحتوائها (عند الضرورة) والتحقيق فيها. وهو يوفر رؤية شاملة لبيئة العمل ويهيئ القدرة على الكشف والحماية والمواجهة في الوقت المناسب. وحتى الآن، تمت تغطية ٨٨٪ من جميع أجهزة الحواسيب والخوادم على مستوى المنظمة، ويجري العمل على إكمال التنفيذ بنسبة ١٠٠٪ بحلول الربع الثاني من عام ٢٠٢١.

(و) **نظام لمنع انتحال شخصية المنظمة بالبريد الإلكتروني للاحتيال على الجمهور.** في المتوسط، يتم إرسال ٢,٣ مليون رسالة بريد إلكتروني متفرّدة كل شهر باستخدام العنوان <@who.int>. وفي نيسان/ أبريل ٢٠٢٠، كان حوالي ٨٠٪ من هذه الرسائل سرقات للهوية. وقد نفّذت الأمانة في أيار/ مايو ٢٠٢٠ حلاً للتحقق والإبلاغ والمطابقة على أساس النطاقات من أجل الحد من هذا السلوك قدر الإمكان وعدم السماح بإرسال رسائل باسم المنظمة إلا للمصادر المأذون لها. ومنذ ذلك الحين، ظلت ٩٦٪ من رسائل البريد الإلكتروني متوافقة، وتمت إزالة نسبة الـ٤٪ المتبقية التي تتضمن سرقات للهوية ولم تصل أبداً إلى صناديق البريد في المنظمات التي نفّذت تلك الحلول.

(ز) **سحب التطبيقات القديمة.** تتعرّض النظم القديمة التي تم تطويرها باستخدام تكنولوجيا عتيقة لهجمات متطورة. ويجري تطبيق عمليات تصحيح، ولكن في بعض الحالات يكون هذا التصحيح غير كافٍ لاتّقاء الهجمات المشبوهة بسبب تصميم النظام وبنيته البالية. ولذلك، قامت الأمانة بإحلال عدد كبير من التطبيقات التي لم يعد من الممكن إصلاحها أو تصحيحها.

٩- وتتطلب الإدارة الفعالة لبرنامج الأمن الإلكتروني تواصلاً وتنسيقاً مستمرّين. وعلى وجه الخصوص:

(أ) على الصعيد الداخلي، يتم توجيه التنسيق العالمي من خلال مجموعة الأمن الإلكتروني، التي تتألف من فريق الأمن الإلكتروني وممثلي جميع المناطق. وتنسّق هذه المجموعة أنشطة المنظمة المتعلقة بالأمن الإلكتروني، بما في ذلك تنفيذ إجراءات ومعايير وحلول الأمن الإلكتروني؛

(ب) أُنشِئت قناة اتصال مباشر مع عدة أفرقة معنية بالاستجابة للطوارئ الحاسوبية، ومنظمات حكومية وشركات خاصة من أجل تلقّي وتبادل معلومات استخبارية يُستنَد إليها في اتخاذ إجراءات بشأن التهديدات. ويجري يومياً تقاسم المؤشرات الدالة على مَواطن الضعف.

١٠- وبالإضافة إلى ذلك، فإن الأنظمة والتطبيقات المؤسسية – بما في ذلك نظام الإدارة العالمي والبريد الإلكتروني والمواقع الإلكترونية والمنصات التعاونية ومنصات التطوير – تخضع للمراقبة باستمرار، ويتم تطبيق عمليات تصحيح أمني دون تأخير للحدّ من مخاطر الأمن الإلكتروني أو القضاء عليها.

## تعزيز جهود الأمن الإلكتروني

١١- تنطوي خروقات وهجمات الأمن الإلكتروني، متى نجحت، على تكلفة باهظة. وتشمل التكاليف المحتملة الإضرار بقيمة الأمانة وسمعتها؛ والخسائر المالية المباشرة (العلاج، ووقت العمل، والتكاليف القانونية، والتكاليف المتصلة بالعلاقات العامة، وتكاليف الإخطارات)؛ والآثار المترتبة بالنسبة إلى توافر الأنظمة؛ وضياع بيانات حرجة؛ والمساس بسلامة البيانات.

١٢- ورغم كل الجهود المذكورة آنفاً التي بذلتها الأمانة، لاتزال هناك ثغرات ينبغي معالجتها وعدد من المجالات التي يتعين تحسينها. وثمة ضرورة لاتّباع مسارات العمل الثمانية الجديدة التالية من أجل حماية الأمانة من الجهات الفاعلة التي تشكّل تهديدات مستمرة متقدمة، وهي مدرجة في نطاق برنامج الأمن الإلكتروني.

(أ) **تحسين حماية البريد الإلكتروني بواسطة وصلات إلكترونية ومرفقات مؤمّنة.** تبدأ أكثر من ٩٠٪ من الهجمات الإلكترونية بتصيُّد الرسائل الإلكترونية، وذلك باستخدام الوصلات الإلكترونية والمرفقات. وسوف توفر سمات الأمان المدمجة في البريد الإلكتروني الحماية عن طريق تحسين التحقق التلقائي من مرفقات البريد الإلكتروني للمحتوى المشبوه، وسيتم التحقق من وقت النقرات في رسائل البريد الإلكتروني.

(ب) **تأمين استخدام شبكة الإنترنت.** سيوفر استخدام بديل إلكتروني عالمي الحماية لأجهزة النقاط النهائية التي تستخدم شبكة الإنترنت، سواء داخل مكاتب المنظمة أو خارجها. ويحقق ذلك ضبط وصول أجهزة النقاط النهائية إلى الإنترنت من خلال إتاحة التحقق من المواقع الإلكترونية وتنقيتها وحمايتها من البرمجيات الخبيثة.

(ج) **المسح الضوئي لتحديد الثغرات الأمنية في التطبيقات.** سيوفر ذلك تقييماً متسقاً وأفضل لأمن التطبيقات النقالة والتطبيقات القائمة على شبكة الإنترنت أثناء التطوير والاختبار والعمليات. والهدف من ذلك هو تحديد الثغرات الأمنية في النظم والشبكات والتطبيقات.

(د) **الحواجز الوقائية للتطبيقات الإلكترونية.** يمثل ذلك جيلاً جديداً من الحماية والوصول للتطبيقات الإلكترونية. وتعمل الحواجز الوقائية للتطبيقات الإلكترونية كدروع وبوابات يتم وضعها بين التطبيقات الإلكترونية وشبكة الإنترنت وتمنع تعرّض التطبيقات للهجوم. ويتم تعقُّب عمليات الوصول الخارجي وتنقيتها ورصدها.

(هـ) **ضبط تتبُّع الثغرات الأمنية.** يهيئ ذلك نظاماً للتحقّق والإبلاغ التلقائي عبر الإنترنت سيتم دمجه مع عمليات إدارة الحوادث والتغييرات والتصحيحات. وسييسر ذلك معالجة الثغرات الأمنية في النظم والتطبيقات غير المصحّحة.

(و) **تنظيم الوصول المتميّز.** يوفر ذلك للمنظمة رؤية المخاطر المحتملة المرتبطة بمختلف أنواع الوصول المتميّز ليس هذا فحسب وإنما يتيح أيضاً، من خلال تنفيذ أدوات مناسبة، الحماية من إساءة استخدام الحسابات ذات الامتيازات الرفيعة (مثل حسابات مديري النظم).

(ز) **الفصل بين إدارة المهام.** يضمن ذلك وجود تقسيم واضح للمهام والأدوار المتصلة بالوصول إلى النظم. ولا ينبغي أن تكون هناك حالات يتمكن فيها الفرد من طرح واعتماد معاملات من أجل ارتكاب جرائم إلكترونية (السرقة أو الاحتيال لتحقيق مكاسب شخصية).

(ح) **تكنولوجيا الخداع.** يولِّد ذلك فخاخاً أو شراكاً خداعية تهدف إلى خداع الجهات مصدر التهديد بإيهامها أنها اكتسبت موطئ قدم في المنظمة (على سبيل المثال، لسرقة وثائق تفويض أو أسرار). ومن شأن ذلك أن يحسِّن قدرة الأمانة على كشف سلوك الدخلاء الخارجيين واستخدام تلك المعارف لتعزيز أمن نظمها.

١٣- إن الحفاظ على الزخم أمر بالغ الأهمية. ومن شأن إدراج مسارات العمل هذه في جهود الأمانة المتعلقة بالأمن الإلكتروني أن يساعد على زيادة تعزيز طرائق تحديد الهوية والكشف والوقاية والحماية والمواجهة، مما يؤدي إلى تنفيذ خريطة طريق الأمن الإلكتروني.

## التمويل المستدام

١٤- أذن المقرّر الإجرائي ج ص ع٧٠(١٦) (٢٠١٧) للمدير العام بتخصيص مبلغ قد يصل إلى ١٥ مليون دولار أمريكي على الأقل بنهاية كل ثنائية، حسب المتاح، لاحتياجات الاستثمار في تكنولوجيا المعلومات في إطار صندوق البنية التحتية.[١] ويموَّل برنامج الأمن الإلكتروني الحالي من صندوق البنية التحتية.

١٥- وتعتبر الأمانة أن الأمن الإلكتروني أولوية قصوى. ومن الأهمية بمكان أن نحمي جميع الجهود التي بُذِلت حتى الآن وأن نواصل العمل الذي يجري القيام به لحماية المنظمة. وقد وُضِعت تقديرات أولية للتكاليف اللازمة من أجل استكمال برنامج الأمن الإلكتروني. غير أن تعزيز عمليات الأمن الإلكتروني بعد إكمال البرامج سيتطلب أيضاً استثمارات كبيرة في السنوات المقبلة.

١٦- وقد أوصت لجنة الخبراء المستقلين الاستشارية في مجال المراقبة بأن يُجرى استعراض شامل لإنفاق المنظمة على تكنولوجيا المعلومات كجزء من دورة التخطيط الشاملة.[٢] وينبغي أن ينظر هذا الاستعراض في تكاليف إدارة أعمال الأمانة وجميع المبادرات الهادفة لتغيير تكنولوجيا المعلومات، بما في ذلك الأمن الإلكتروني. وتُجري الأمانة هذا الاستعراض في السياق الأوسع لإعداد الميزانية البرمجية المقترحة ٢٠٢٢-٢٠٢٣.

١٧- وستُطلِع الأمانة الدول الأعضاء، من خلال الاجتماع الرابع والثلاثين للجنة البرنامج والميزانية والإدارة، على نسبة المبادرات (أي العمليات مقابل التغييرات)، بما في ذلك استعراض شامل مستكمل للإنفاق على تكنولوجيا المعلومات في المستقبل.

## الإجراء المطلوب من المجلس التنفيذي

١٨- المجلس مدعو إلى الإحاطة علماً بهذا التقرير.

= = =

١ انظر الوثيقة ج ص ع٧٠/٢٠١٧/سجلات/١.

٢ انظر الوثيقة EBPBAC30/2.