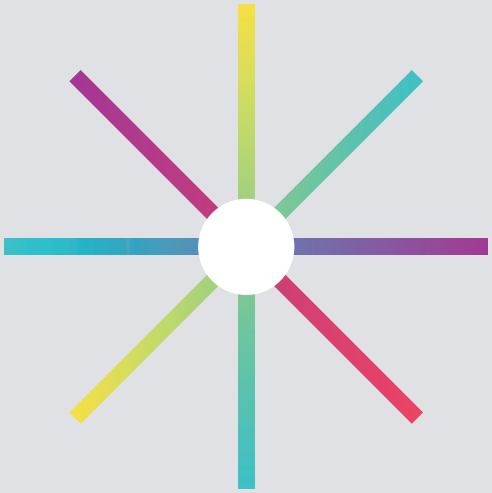
دليل الأمان الإلكتروني لعام ٢٠١٨:

استخدام المخترقين والمدافعين للتصميم وتعلم الآلة

جدول المحتويات



تقرير الأمان الإلكتروني لعام ٢٠١٨

مقدمة

تتطور الحياة وسبل العيش بشكل سريع عبر الإنترنت في جميع أنحاء العالم، وبدأت العوالم المادية والرقمية في التداخل، كما يمكن للعملات الرقمية شراء سلع وخدمات في العالم الحقيقي دون أن يكون لها شكل ملموس في العالم الحقيقي. فالذكاء الاصطناعي يدعم صنع قرار تشغيل المركبات ذاتية القيادة بالإضافة إلى اكتشاف عقاقير فعالة جديدة يوميًا وتخصيص الدروس للمساعدة في تعلم الطلاب.[١و٢و٣] وفي الوقت ذاته، يُجري الأطباء عمليات جراحية لإنقاذ حياة الأشخاص على الجانب الآخر من العالم عبر الإنترنت والروبوتات المتحركة فائقة الإمكانات، في حين تقوم أجهزة الاستشعار المتصلة بالشبكات بإحداث تحولات جذرية في مختلف المجالات بداية من توليد الطاقة إلى وسائل النقل العامة.[٤] ففي كل عام، تتوسع قائمة المجالات التي يتم تزويدها بأجهزة الاستشعار والأجهزة الذكية والمعالجات الدقيقة.

الشيء الوحيد الذي لا يتغير هو أنه حيثما تسنح الفرصة، تسعى الجهات الإجرامية والسياسية المشكوك في نزاهتها إلى استغلال الثغرات لتحقيق مكاسب. كما أن العديد من الأدوات والأساليب التي تقدم فوائد عظيمة للمجتمع تجعل المحاولات الخبيثة أسهل وأكثر ضررًا. فهجمات البرامج الضارة والتصيد الاحتيالي وحجب الخدمات الموزّع (DDoS) ليست إلا عددًا قليلاً من الحيل التي تعرقل سبل التطور الرقمي التي تدفع مسبيرة تقدم عالمنا.

وبالنسبة لمحترفي أمان المعلومات، فإن الدفاع الناجح ضد التيار العنيف من الهجمات المتواصلة حاليًا عبر الإنترنت هو ما يؤرقهم ويعملون على تحقيقه طوال الوقت كجزء أساسي من مهمتهم الأصلية. إذًا من الفائز؟ هل هم المهاجمون أم المدافعون؟ نظرًا للوتيرة اليومية التي تتكرر بها الاختراقات الناجحة التي تؤدي إلى شلل في عمليات الشركات وخسارة الملايين من الدولارات من قيمة الأسهم بين عشية وضحاها، فمن الصعب التكهن بذلك.[٥]

ولكي نجعل المشهد الحالي والمستقبلي أكثر وضوحًا، عكفنا مع خبراء الأمان الإلكتروني على إنشاء هذا الدليل الحديث. وقد استفادت HP من كبار المفكرين في مجال أمان المعلومات بهدف مساعدة صانعي القرار الذين يقودون جهود أمان المعلومات في الشركات متوسطة الحجم والمؤسسات في فهم جميع الخيارات المتاحة لمنع الضرر الناجم عن انعدام الأمان على الإنترنت.

القسم ١:

تقرير الحالة

تقرير الأمان الإلكتروني لعام ٢٠١٨

سيظهر نوع جديد من البرامج الضارة على الإنترنت كل أربع ثوانٍ.

سيتم تسجيل ما يقرب من ٦ إلى ١١ مليون إصابة جديدة بالبرامج الضارة على أجهزة الكمبيوتر التي تعمل حاليًا باستخدام برنامج واحد فقط لمكافحة الفيروسات.[٦] وسيتم إطلاق حوالي ٧٠٠ هجوم للتصيد الاحتيالي بهدف إغراء الأشخاص غير المكترثين بالنقر فوق ارتباط احتيالي من شأنه أن يسهل على المخادع سرقة بياناتهم الشخصية أو الوصول إلى شبكة إحدى الشركات.[٧] وسيظهر نوع جديد من البرامج الضارة على الإنترنت كل أربع ثوانٍ.[٨]

ينفق عدد لا حصر له من المخترقين نحو ١٥٠ دولار أمريكي لاستئجار شبكة روبوت (شبكة اختراق) لإطلاق هجوم "حجب الخدمات الموزّع" (DDoS) لمدة أسبوع واحد بهدف تعطيل خدمة عبر الإنترنت أو شبكة من خلال خلق ازدحام بيانات بها[٩]. وبشكل تراكمي حول العالم، فإن هذه الهجمات تطلق بشكل منتظم نحو ٥٠٠ جيجابت في الثانية من البيانات المسلحة تجاه خوادم الشركات والحكومات في جميع أنحاء العالم بهدف استهلاك النطاق الترددي للشبكة وتعطيل الأهداف.[١٠،١١]

وفي الوقت ذاته، نجد الملايين من أجهزة الكمبيوتر والطابعات المتصلة بالشبكة والكاميرات وأجهزة التحكم في الحرارة وغيرها من أجهزة إنترنت الأشياء (IoT) غير مؤمّنة نظرًا لعدم تثبيت أحدث تصحيحات الأمان ووجود شخص لديه نوايا سيئة في انتظار العثور على باب مفتوح للوصول إلى أكثر البيانات حساسية لدى الشركات.[١٢]

وكانت النتيجة تدفق مستمر للتقارير الإخبارية حول عمليات الاختراق الناجحة في الشبكات التي يتعين أن تكون آمنة. وفي غضون الأيام القليلة الأولى من عام ٢٠١٨، أغلقت برامج طلب الفدية شبكة مستشفى إقليمية من أجل دفع مبلغ من البيتكوين، بينما تم تعطيل جهة حكومية محلية وجميع أنظمة الكمبيوتر لمدرسة واحدة في مقاطعة بالولايات المتحدة الأمريكية.[١٣ و١٤ و١٥]
وفي الوقت ذاته، تم العثور على ثغرة كبيرة داخل الرقاقات الدقيقة، مما يعني أن كل كمبيوتر حديث لم يتماخترقه هو في خطر حاليًا.[١٦]

من الواضح أن هذه الهجمات ذات دوافع مالية، فهي لا تستهدف فحسب مجموعات، مثل خرق بيانات البنوك الهندية لعام ٢٠١٦ أو شركات كبرى مثل Sony وEquifax وYahoo فحسب،[١٦] بل يسعى المخترقون من خلالها أيضًا إلى ابتزاز الشركات الصغيرة والمتوسطة ومقدمي الرعاية الصحية والمؤسسات الحكومية المحلية والشبكات الأخرى.[١٨]
وفي حقيقة الأمر، فإن هناك الكثير من المحفزات النقدية التي يزداد فيها التهديد. **وقد تبين من خلال** أحد التحليلات أن تكلفة الجرائم الإلكترونية بحلول عام ٢٠٢١ ستبلغ ٦ ترليون دولار أمريكي –نعم ترليون– وهذا يعني أن قيمتها أكبر من المكاسب التي تنتجها التجارة العالمية في العقاقير غير المشروعة.[١٩]

لا تهمل الحقيقة الواضحة

هذه التهديدات مألوفة تمامًا لدى خبير أمان المعلومات جيسون أوكيفي "مستشار أمان الطباعة لدى HP". فهو يدرك أن الأشرار يحصلون على مساعدة كبيرة جراء سلوك مستخدم الكمبيوتر غير المقصود ودفاعات الأمان الإلكتروني المنتشرة بشكل جزئي بسبب وجود كثير من موظفي الأمان الإلكتروني غير المتمكنين أو الذين يعانون من ضغوط شديدة.[٢٠]

وأثناء تقييم ثغرات شبكات الكمبيوتر لدى الشركات، اكتشف "أوكيفي" جميع أنواع المشاكل التي تجعل مهمة المخترق أكثر سهولة، بما في ذلك الإغفالات الخطيرة من قبل أقسام تكنولوجيا المعلومات التي يتعين عليهم التركيز عليها بشكل أفضل.

وخلال أحد هذه التقييمات، طُلب من "أوكيفي" محاولة استكشاف البنية التحتية لبيئة تكنولوجيا المعلومات عن كثب لدى مؤسسة تصنيع ضخمة. ومن بين العديد من المشاكل، وجد أن كلمات المرور الافتراضية المعيّنة من قبل المصنع لم يتم تغييرها على ٩٠ بالمائة من طابعات الشركة البالغ عددها ٣٦٠٠٠ طابعة والمنتشرة في جميع أنحاء الشبكة، مما يسمح لأي شخص لديه معرفة بها بتجاوز جميع خطوط الأمان على الأجهزة. وقد تبين من خلال تحقيق إضافي أجراه "أوكيفي" أنه تم تكوين الطابعات بشكل غير صحيح، مما قد يسمح لجهة خارجية بالوصول إلى الطابعات وإعادة تكوينها لسرقة البيانات من الشبكة أو استغلالها في خدمة كشبكة روبوت (شبكة اختراق). وتذكر أوكيفي أن جايسون "نائب رئيس مجلس الإدارة" قد انتقد هذا التحقيق قائلاً له "هل تمزح معي؟". "لقد كان غاضبًا."

ومع الانتشار والتطور السريعين لأجهزة إنترنت الأشياء والأجهزة الأخرى المتصلة بكل من إنترنت خارجي وشبكة داخلية للشركة دون الحاجة إلى مصادقة سليمة، تتاح للأشرار مجموعة كبيرة من نقاط الوصول. لقد ولى الوقت الذي كان يشعر فيه مدير أمان المعلومات أن المهمة قد تم إنجازها بمجرد حماية الخوادم المهمة لعمليات الشركة الأساسية بشكلٍ كافٍ. لكن الآن، يتعين أن يمتد غطاء الأمان إلى ما يصل أحيانًا إلى ملايين الأجهزة المتصلة في المكاتب البعيدة وبداخل جيوب الموظفين.

وفي هذا السياق صرحت "شيفان أولبرايت" كبيرة خبراء تقنيات أمان الطباعة لدى HP[٢١] قائلة "إننا نحاول حماية أجهزة الكمبيوتر الشخصية والخوادم والأجزاء الأساسية الأخرى من الشبكات، ولكن أجهزة إنترنت الأشياء تجعل الشبكات حاليًا في خطر أكبر". واستطردت "عادة ما تكون هناك ثغرة واحدة على الأقل في كل ١٠٠ سطر من التعليمات البرمجية. فما على المخترقين سوى مجرد العثور على هذه الثغرة للدخول إلى النظام. ونحن نريد أن نضمن خفض الثغرات المكشوفة إلى إلى أقل عدد ممكن."

عادة ما تكون هناك ثغرة واحدة على...

الأقل في كل ١٠٠ سطر من التعليمات البرمجية...

ما على المخترقين سوى مجرد العثور على هذه الثغرة للدخول إلى النظام.

الوصول من أي مكان

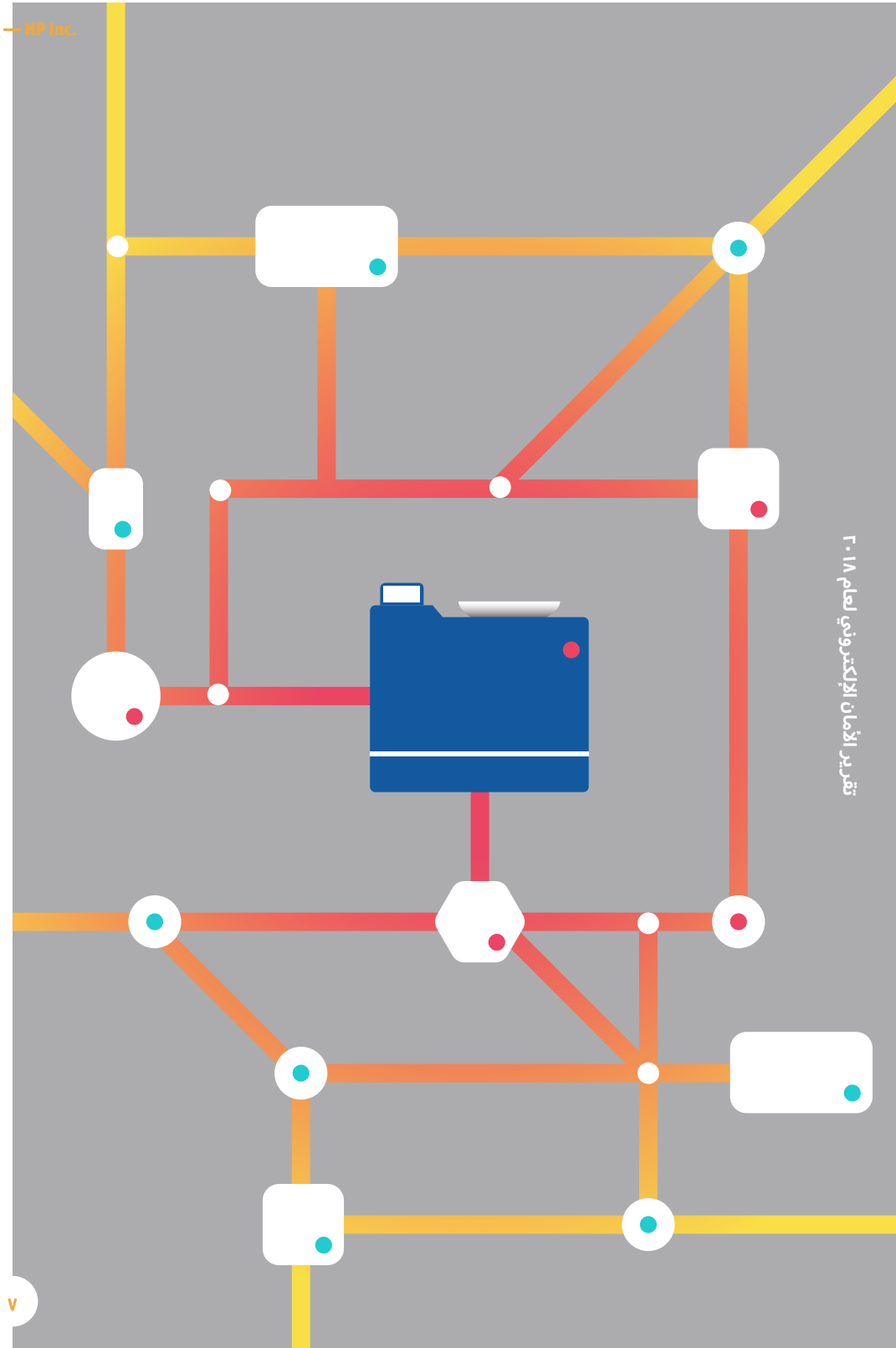
في هذه الأيام، يسيطر على المخترقين طموح بتحقيق أرباح هائلة مما يدفعهم إلى الابتكار والإبداع. تقول أولبرايت "إن شبكات الروبوت (شبكات الاختراق) من أكبر التهديدات، فهي عبارة عن أدوات مؤتمتة تعمل على آلاف من أجهزة إنترنت الأشياء التي تم اختراقها. ولكي يُنشئ المحتالون شبكة روبوت، فإنهم يخترقون معالجات الأجهزة غير المؤمّنة، ثم يستخدمون الأجهزة المخترقة لاستخراج (تعدين) البيتكوين، أو يمكنهم تأجير شبكات الروبوت الخاصة بهم لإطلاق هجمات "حجب الخدمات الموزّع" (DDoS) التى تسعى للحصول على فدية.[٢٢]

وبالنظر إلى حجم محاولات الاختراق التي تحدث باستمرار والعدد المتزايد للطرق التي يمكن للمخترقين استغلالها، يقول "أوكيفي" وغيره من الخبراء بأنه قد يكون من الأفضل لمديري الأمان التفكير في الشبكات المحيطة بهم التي تم اختراقها بالفعل.
وأضاف أوكيفي "على مجتمع الأمان أن يتقبل تمامًا أن شبكاتهم من المحتمل أنها قد تعرضت بالفعل للخطر، إلا أنهم لا يزالون لا يعرفون ذلك بعد".

وتبين لأوكيفي من خلال بروتوكولات الأمان الإلكتروني التي حللها لما يزيد عن ٥٠ من الشركات الصغيرة والمؤسسات بأن كل منها بها نقاط ضعف من شأنها أن تسمح للمخترقين بالوصول إلى الشبكة من خلال إحدى الطابعات أو الكاميرات أو الأجهزة المحمولة أو الأجهزة الطرفية الأخرى المتصلة بها.

لذا، فإن مفتاح الحفاظ على أمان الشبكة هو منح موظفي تكنولوجيا المعلومات الأدوات اللازمة لاكتشاف الاختراقات وحماية الأجهزة الطرفية – فهي فرص يتم التغاضي عنها بسهولة ويستغلها عدو يتمتع بإصرار كبير إذا لم يتم الدفاع عنها بشكل صحيح. وشدد "أوكيفي" على أنه إذا كانت هناك اختراق، فمن المهم أن تكون هناك استجابة قوية للمعالجة لاحتواء الضرر وإصلاحه بسرعة.

يتفق دانيال كالاي –مؤسس شركات خدمات تكنولوجيا المعلومات المدارة التي تتضمن شركة أمان إلكتروني للمنازل والشركات الصغيرة Shieldly– مع أولبرايت وأوكيفي على أن التركيز يجب أن يكون على تأمين حدود الشبكات والأجهزة الطرفية الخاصة بها.[٢٣] لكنه يعتقد أن الدفة قد مالت بعيدا جدًا عن التفكير في الوقاية واتجهت إلى التركيز المفرط على الاسترداد والمعالجة. ولكنه يختلف مع فكرة أن الشبكة المخترقة أمر لا مفر منه في المشهد الرقمي في هذه الأيام.



يقول كالاي "لقد كان الأمان الإلكتروني يُستخدم للوقاية. لكنه يستخدم حاليًا للعلاج. وإنه لمحزن أن ننظر إلى الأشياء التي يفعلها الأشخاص الذين فقدوا الثقة في أدوات الوقاية. ولكن يمكن فعل الكثير لمنع أي هجوم."

ثمن الفشل

إن الاستخدام الأفضل لأجهزة ومعايير وبروتوكولات الأمان من شأنه التأكيد على تحسين النتائج للأشخاص الذين قاموا بتأسيس برامج للدفاع الإلكتروني بجدية، ولكن أرقام العالم الحقيقي تظهر وجود فجوة كبيرة بين التخطيط والتنفيذ.[٢٣] وعلى الرغم من أن التهديدات نفسها تستهدف جميع المؤسسات، فإن المشكلة لدى الشركات الأصغر حجمًا تكون كبيرة للغاية نظرًا لأنها لا تملك نفس المال والوقت والموارد التعليمية للاستثمار في الأمان الذي تقوم به المؤسسات والشركات الأكبر.[٢٥]

لذا، يجب تذكير كل شخص مسؤول عن أمان معلومات الشركات بالمخاطر التالية: احتمال خسارة ملايين الدولارات وانخفاض المصداقية والثقة في أعين العملاء ورفع دعاوى قضائية وحدوث اضطرابات تجارية ضخمة.

ووفقًا لتقرير أصدره معهد بونيمون Ponemon Institute –مجموعة أبحاث مستقلة لأمان المعلومات– فإن متوسط تكلفة خرق البيانات قد بلغ ٣,٦٢ مليون دولار أمريكي في عام ٢٠١٧.[٢٦] وقد أجرى الباحثون مقابلات مع مسؤولين في ٤١٩ شركة في ١٣ دولة، ووجدوا أن كل سجل ضائع أو مسروق يكلف ١٤١ دولار أمريكي في المتوسط، وهو رقم يتضاعف بسرعة إلى جانب الأثر المتزايد لهذه الحوادث. وفي الواقع، كشفت الدراسة أن حجم الاختراق زاد في المتوسط بنسبة ١,٨ بالمائة على أساس سنوي في عام ٢٠١٧.

وقد أبلغت كل شركة من الشركات التي شاركت معلوماتها مع Ponemon Institute عن حدوث خرق بسبب هجوم ضار أو إجرامي ووجود خلل في النظام أو حدوث خطأ بشري، فقد تم اختراق ٢,٦٠٠ إلى أقل من ١٠٠,٠٠٠ اختراق في كل حادث. وقد استغرق المشاركون في الدراسة أكثر من شهرين في المتوسط للتعرُف على الاختراق واحتوائه.

البرامج الضارة تزداد ذكاءً

يقول "جوناثان جريفين" باحث أمان كبير في HP Labs إنه يشهد الكثير من الانتهاكات الضخمة التي تحدث "مستوى مروعًا من الأضرار والدمار"، بما في ذلك هجمات NotPetya لعام ٢٠١٧ التي أثرت على الشركات في الولايات المتحدة وعبر أوروبا، إذ يبدو أن هدفها الأساسي كان مدمرًا تمامًا.[٢٧] وكما هو الحال مع العديد من الهجمات الناجحة الأخرى، فقد كان الدفاع ضد WannaCry متاحًا قبل بدء التفشي. ولكن لسوء الحظ، لم تقم العديد من الشركات –الكبيرة منها والصغيرة على حد سواء- بتثبيت التصحيحات البسيطة للبرامج التي من شأنها أن تمنع الاختراق.

لكن الاختراقات الناجحة لا تدل بالضرورة على تراجع الأمان. وقد لاحظ "جريفين" وفريقه في معمل HP للبرامج الضارة أن البرامج الضارة قد أصبحت أكبر وأكثر تعقيدًا على مدار السنوات الثلاثة الماضية. وأصبحت البرامج الضارة حاليًا تتمتع بوظائف أفضل بشكل كبير مقارنة بمجموعة البرامج التجارية جيدة التصميم عالية الجودة.
ويقول "جريفين" أن المجرمين والمخترقين الذين ترعاهم الدول هم من الفنيين المنظمين وذوي الكفاءة العالية الذين يطورون مهاراتهم ويدمجون أدوات جديدة باستمرار، مثل تعلم الآلة الذي يمكّن الأنظمة من التعلم من تجاربها وتحسين مهاراتها الذاتية دون الحاجة إلى إجراء برمجة مباشرة.

> يزيد مزيج التعقيدات المتزايدة للهجمات وعدم الاهتمام الكافي بالأمان الإلكتروني من المخاطر على شبكات الشركات.

يزيد مزيج التعقيدات المتزايدة للهجمات وعدم الاهتمام الكافي بالأمان الإلكتروني من المخاطر على شبكات الشركات. ولحسن الحظ، لاحظ "جريفين" أن العديد من علماء ومهندسي الكمبيوتر في جميع أنحاء العالم يعملون على تحسين الدفاعات. ويقول الخبراء بأن الشركات تدرك جيدًا أن نشر جدار الحماية وبرامج مكافحة الفيروسات هو مجرد بداية لبرنامج فعال يتمتع بدفاعات متعددة الطبقات واكتشاف الاختراق بشكل أساسي.

القسم ٢:

فكر مثل دافنشي: العالم بحاجة إلى مزيد من المعرفة بشأن عالم الأمان الإلكتروني

تتطلب تهديدات الأمان الإلكتروني الحالية والمتطورة مزيجًا من الفن والعلم.

تمت صياغة مصطلح "رجل النهضة" –للشخص الذي يمتلك مواهب في مجالات مختلفة– مع وضع ليوناردو دافنشي في الاعتبار. فقد كان رسام التحفتين الفنيتين "العشاء الأخير" و"الموناليزا" مهندسًا بقدر ما كان فنانًا. وباعتباره مهندسًا عسكريًا لمدة تقرب من عقدين من الزمان قام دافنشي بتحصين نظام الدفاع في ميلان إلى جانب اختراعه وتطويره لأسلحتها أيضًا. وعلى مدار حياته، قام أيضًا بإنشاء وتنقيح أساليب إنشاء الجسور وتطوير مكونات الآلات مثل التروس الدودية وعجلات التوازن. فقد كان خبيرًا في علم السوائل المتحركة (الهيدروليات) وتصميم المركبات المدفوعة بالزنبرك.

يمكن لعالم الأمان الإلكتروني الاستفادة من بعض الدروس من هذا الخبير. فتهديدات الأمان الإلكتروني الحالية والمتطورة تتطلب مزيجًا من الفن والعلم خاصة فيما يتعلق بالتصميم.

ويتعين على الأشخاص المكلفين بحماية معلومات المؤسسة دراسة جميع الأصول المادية والرقمية المتعلقة المؤسسة ومعرفة مكانها على الشبكة وكيفية الاتصال بها وعلاقتها بالأصول الأخرى. ولعل الأهم من ذلك، هو أن الاستخدام الفعلي للأجهزة الطرفية، مثل الهواتف الذكية والطابعات وأجهزة الكمبيوتر المحمولة من قبل الموظفين أثناء قيامهم بعملهم يجب أن يكون في مركز الأمان وتصميم البنية.

وفي نهاية المطاف، فإن أفضل دفاع يجعل الشبكة آمنة حتى دون علم المستخدمين بوجود أنظمة أمان. من المفيد لمديري أمان المعلومات أن يضعوا في اعتبارهم ما يلي: استخدام تقنية ذكية غير مرئية تتطور تدريجيًا مع التهديد.

المراقبة النشطة ضرورية

"ألين كينت" هو مستشار للأمان الإلكتروني يعمل لدى شركة NAES، فهي شركة تقدم مجموعة من الخدمات للصناعات بدءًا من توليد الطاقة إلى تصنيع عجينة الورق والورق النهائي.[٢٨] إذ يفحص "كينت" محطات توليد الطاقة ما يصل إلى عشرين مرة في السنة بحثًا عن ثغرات في الأمان الإلكتروني، ويتم استدعاؤه لتنفيذ أعمال تدقيق لمنتجي الطاقة ومالكي أنظمة التوزيع والموزعين، حتى يكونوا مستعدين لإجراء فحوص مفوضة فيدراليًا الدفاعات الإلكترونية لديهم.

وتُجرى عمليات التدقيق الفيدرالية هذه كل ثلاث إلى ست سنوات اعتمادًا على مدى التأثير المحتمل للاختراق على الكيان من حيث استقرار الشبكة الكهربائية بأكملها. ومن المدهش أن معظم مولدات الطاقة عادة ما تعتبر منخفضة التأثير. ولكن، قد تنشأ إمكانية حدوث تأثير كبير إذا كانت هناك مشكلة نظامية في مركز مراقبة سلطة الموازنة الذي يدير إمداد الكهرباء المتقلب والطلب في الأقاليم والدولة.

وقبل بدئه العمل في البنية الأساسية المهمة لتوليد الطاقة، عمل "كينت" في مجال الأمان الإلكتروني في القطاع المصرفي، لذلك كان يفكر في طرق لإفشال تهديدات العصابات الإجرامية المنظمة والكيانات الحكومية الدولية لسنوات. فهو يقول بأنه على الرغم من الأعمال الكثيفة بدرجة كبيرة التي يتعين على مشغلي المعدات الكهربائية القيام بها ليكونوا متوافقين مع المعايير الفيدرالية –على النقيض من الصناعة المالية– فإن الأمان الإلكتروني في قطاع الطاقة هو في الواقع "على ما يرام". وأضاف "إنه ليس رائعًا، لكنه على ما يرام."

ويقول "كينت" بأن أكبر التحديات التي يواجهها هو تثقيف المديرين بشأن عدم وجود حل كافٍ للأمان الإلكتروني يمكنهم تثبيته ونسيانه. ونوه على "أنه يجب أن تتم مراقبة الدفاعات باستمرار. ولكن معظم الشركات الأصغر في أي صناعة لا تريد أن تدفع مقابلاً لشخص ما للقيام بذلك. إنها نفقات مستمرة بلا طائل – إلى أن يقع حدث يبين أهمية ذلك العمل مقارنة بتكلفة هذا الراتب."

ويقول "كينت" بأن الشركات بحاجة إلى بدء برنامج الأمان الإلكتروني من خلال القيام بالإجراءات الأربعة التالية: تثبيت جدار حماية والتأكد من تكوينه بشكل سليم للعمل بشكل صحيح؛ وضع أنظمة تراقب وتصفي المحتوى الخطير أو المشتبه فيه من البريد الإلكتروني ومستعرضات الويب؛ فصل الأصول المحمية عن الأصول التي لا تحتاج إلى نفس مستوى الحماية (في منتج الطاقة، على سبيل المثال، فصل أجهزة الكمبيوتر التي تشغل المحطات عن تلك التي تدير العمليات التجارية)؛ وإنشاء بروتوكولات وتعيين أشخاص وبرامج لمراقبة كل ذلك بفعالية. هذا هو نموذج الأمان الإلكتروني القياسي الذي يطلق عليه الدفاع عن الحدود الخارجية: فهو يبني جدران رقمية وأنظمة لاكتشاف الاختراق لحجب المخترقين.

ولكن توجد حاليًا أسلحة جديدة متوفرة تمنح مديري الأمان الإلكتروني شجاعة كبيرة. فمنذ وقت ليس ببعيد، اعتقد الخبراء أنه لا توجد استراتيجية وقائية يمكن أن تلاحق كل تهديد جديد من الإنترنت. ولكن في هذه الأيام، بدأت أدوات الاكتشاف التلقائي في مراقبة شبكاتها أثناء العمل لمعرفة كيفية تحرك البيانات بشكل طبيعي خلالها كي تتمكن من اكتشاف عمليات الاختراق وإيقاف تحويلها إلى حوادث مدمرة. إذ يمكن لحدث يبدو صغيرًا، مثل كمبيوتر محمول يرسل عددًا من وحدات الجيجابايت من البيانات من شبكة ترسل في المعتاد مئات من وحدات الميجابايت أن يصدر تنبيهًا بأن شيئًا ما غير طبيعي.

الركائز الأساسية الأربعة للأمان الإلكتروني على الشبكات:

١. **تثبيت جدار حماية**

٢. **مراقبة وتصفية المحتوى الخطير أو المشتبه به**

٣. **فصل الأصول المحمية**

٤. **إنشاء بروتوكولات**

طبقات الحماية مهمة كطبقات الملابس في الشتاء

تقول أولبرايت التي تعمل لدى شركة HP "إننا نحتاج إلى بناء أجهزة تكون لديها مستويات دفاع متعددة. وهذا ما نطلق عليه الدفاع بعمق. ومن منطلق إدراكك أنه لا يمكنك الحماية من كل شيء، يجب أن تكون قادرًا على اكتشاف السلوك غير الطبيعي داخل الجهاز الذي قد يكون دليلاً على الهجوم."

ويقول "فالي علي" كبير متخصصي التكنولوجيا لدى شركة HP –متعمقًا في هذا الموضوع– بأن إمكانيات الأمان والاكتشاف يجب دمجها في الأجهزة الموجودة على الشبكة وليست المثبتة بعد ذلك.[٢٩] فقد تقدمت تحليلات الأمان –هي عبارة عن برنامج يكتشف التهديدات عند دخولها ويوقفها تلقائيًا كما يخلص الجهاز من البرامج الضارة– بسرعة في السنوات الأخيرة. ولكن للعمل على النحو الأمثل، يتعين أن تكون مضمّنة بحيث تكون واضحة للمستخدم إلى جانب تمتعها بالمرونة الكافية لمواجهة مجموعة متنوعة من الهجمات.

ويجب أن تتم عمليات شراء تكنولوجيا المعلومات فقط بعد دراسة متأنية للعثور على الجهاز الذي سيؤدي المهمة ويحمي المستخدمين والبيانات. ويقول علي "إن كل عملية شراء للأجهزة هي بمثابة قرار أمني"، مضيفًا إلى أن الأمان هو مزيج يجمع بين التكنولوجيا والوعي والمعالجة والحوكمة.

وإلى جانب وجود إمكانيات الكشف والاستجابة والتعليم الذكي، يجب أن تتمتع الشبكات والأجهزة بالمرونة للاسترداد والمعالجة في الوقت المناسب بعد عمليات الاختراق. وأوضح قائلاً "إنك ستتعرض للهجوم. لذا، يجب أن تكون قادرًا على اكتشاف الهجوم والتعرف عليه والقضاء عليه بسرعة وعلى نطاق واسع."

"أنت بحاجة إلى أن تكون قادرًا على اكتشاف الهجوم والتعرف عليه والقضاء عليه بسرعة."

فالي علي
كبير متخصصي التكنولوجيا
لدى شركة HP

الخطر على حدود الشبكة

تمتلك بعض الشركات من فئة المؤسسات الموارد اللازمة لتوسيع نطاق الحماية لتشمل الحدود الخارجية لشبكاتها. لكن العديد من الشركات والمؤسسات متوسطة الحجم لم تخضع جميع هواتفها الذكية وأجهزة الماسحات الضوئية والطابعات وأجهزة إنترنت الأشياء لديها لأنظمة الأمان.[٣٠] وتقول "أولبرايت" التي تعمل لدى شركة HP إن محادثاتها مع العملاء غالبًا ما تكشف عن عدم اهتمام غير متوقع بتأمين الأجهزة الطرفية للشبكات المتطورة.

وأضافت قائلة "إن ما يثير الدهشة بالنسبة لي هو أن الكثير من العملاء يدركون تمامًا أن أجهزة الكمبيوتر والخوادم وأجهزة الشبكات، مثل المحوّلات والموجّهات معرّضة للخطر، ولكنهم لا يقلقون عادةً بشأن الطابعات أو أجهزة إنترنت الأشياء الأخرى. وهذا هو المكان الذي نحاول فيه زيادة الوعي والتعليم – أن أي جهاز طرفي مكشوف أو غير مؤمّن على شبكتك، يمكن أن يعرض البنية الأساسية بأكملها للخطر."

ولكن أولاً، يتعين على أقسام تكنولوجيا المعلومات التأكد من أنها تغطي الأساسيات التالية: ١) تطوير بروتوكولات الأمان الصارمة والالتزام بها، بما في ذلك طلب تغيير كلمات المرور المعينة في المصنع ورموز الوصول إلى الصيانة على الفور على جميع الأجهزة؛ ٢) الالتزام بجداول تصحيحات وتحديثات الأمان في الوقت المناسب لجميع الأجهزة المتصلة بالشبكات؛ و ٣) ضبط التحديث التلقائي أو العاجل لأنظمة التشغيل والتطبيقات وجدران الحماية وتعريفات الفيروسات. يتعين أيضًا على الشركات الاجتهاد سعيًا للحفاظ على تحديث سجلات الموظفين لديها ومنع وصول الأفراد الذين لم يعودوا يعملون لديها.

ويقول "علي" إنه من الضروري أيضًا مزج الفهم الحديث مع سبل تطور المكتب العصري. إذ يتوقع الموظفون بشكل متزايد أن يكونوا قادرين على العمل من أي مكان في أي وقت، وأن يحدث تبادل بين أماكن العمل واللعب بحيث يمكن ممارسة العمل على الشاطئ وقضاء ساعات المرح في العمل. ويقول علي "إن مكاتب المستقبل تتمتع بحدود مفتوحة". وأضاف "إنها بيئة متواصلة على مدار الساعة طوال أيام الأسبوع تختلط فيها حياتك الشخصية بحياتك العملية." ويجب أن تواكب بنية الشبكة والأجهزة والتقنيات هذا التحول.

يتعين على أقسام تكنولوجيا المعلومات التأكد من أنها تغطي الأساسيات التالية:

١ **تطوير بروتوكولات الأمان الصارمة والالتزام بها**

... بما في ذلك طلب تغيير كلمات المرور المعينة في المصنع ورموز الوصول إلى الصيانة على الفور على جميع الأجهزة.

٢ **الالتزام بجداول تصحيحات وتحديثات الأمان في الوقت المناسب لجميع الأجهزة المتصلة بالشبكة**

٣ **ضبط التحديث التلقائي أو العاجل**

... لأنظمة التشغيل والتطبيقات وجداران الحماية وتعريفات مكافحة الفيروسات.

ويشير باحث الأمان "جريفين" إلى أن محترفي الأمان الإلكتروني يشاركون في حرب غير متكافئة يجب عليهم فيها النجاح كل يوم، لكن العدو يحتاج إلى النجاح مرة واحدة فقط. وقد قدم أفضل سبع ممارسات من شأنها تعزيز الأمان الإلكتروني على المدى الطويل:

١. إعداد عمليات سهلة التنفيذ ليست معقدة للغاية أو تبدو في غاية السهولة.
٢. تقديم نصائح بسيطة ومتسقة للمستخدمين.
٣. استخدم المصادقة الثنائية كلما كان ذلك ممكنًا نظرًا لوجود العديد من المشكلات المتعلقة بكلمات المرور وسياسات كلمات تامرور بالشركات.
٤. عدم الشراء استنادًا إلى السعر وحده. تحويل سياسات الأمان الجيدة إلى منتجات أمان جيدة بقرارات شراء أمان جيدة.
٥. عدم الاعتماد على "منظومة الأمان" وحدها والتوقف عن التعامل مع المهام كإجراءات يجب إنهاؤها عند وضع سياسات الأمان لشركتك. التأكد من أن ميزات الأمان التي تدفع مقابلها تجعل شركتك آمنة بالفعل.
٦. إنشاء تقارير أكثر عمقًا ومعنى عن طريق الحصول على أدوات تحليلية لا توضح فحسب عدد الهجمات والفيروسات التي توقفت فيها أنظمة الأمان خلال شهر معين، بل أيضًا عدد تلك الفيروسات الجديدة والفريدة من نوعها.
٧. يجب على مصنعي أجهزة إنترنت الأشياء بناء الأمان في منتجاتهم منذ البداية وأن يتأكدوا من أنهم آمنون دائمًا.

أهمية تعليم الموظفين

أدى تلاشي جدران المكاتب في العصر الحديث إلى تفاقم مشكلة كانت متركزة في هفوات بنظام الأمان نتيجة لسلوك بشري. إذ يتخلى الموظفون عن بروتوكولات الأمان المزعجة من أجل زيادة الإنتاجية، وغالبًا ما يكونوا غير مدركين أن بعض سلوكياتهم عبر الإنترنت تكون في غاية الخطورة. لهذا السبب، فإن حالات السهو البسيطة والممارسات غير السليمة على الإنترنت تكون غالبًا السبب في الشبكات المحطمة أو انتهاك الملكية الفكرية أو سرقة بيانات العملاء الحساسة والسيطرة الأجهزة الطرفية بواسطة شبكات الروبوت (شبكات الاختراق). تقول أولبرايت "عادة ما يقوم شخص بالنقر فوق ارتباط ضار في رسالة بريد إلكتروني".

تشير إحدى شركات مكافحة البرامج الضارة المعروفة إلى أن ٣ بالمائة فقط من البرامج الضارة التي يرونها تستهدف عيوبًا تقنية.[٣١] وهذا يعني أن ٩٧ بالمائة من هؤلاء المخترقين يستخدمون الهندسة الاجتماعية للوصول إلى ضحايا غير مرتابين للنقر فوق ارتباط في رسالة بريد إلكتروني للتصيد الاحتيالي أو كشف حساسية البيانات، مثل كلمات المرور وأرقام الحسابات المصرفية.

وهذا هو سبب أهمية المبادرات التعليمية لكل من موظفي تكنولوجيا المعلومات في التطوير والحفاظ على بروتوكولات وإجراءات أمان قوية للمعلومات، والموظفين غير العاملين في تكنولوجيا المعلومات لتقليل سلوك المستخدم غير المنضبط الذي يخلق ثغرات أمان كبيرة.

تشمل النقاط الأساسية لتدريب الموظفين غير الأعضاء في مجال تكنولوجيا المعلومات ما يلي:

- عدم استخدم كلمة المرور نفسها عبر مواقع شخصية ومواقع عمل مختلفة.
- عدم ترك المطبوعات الحساسة على الطابعات.
- تأمين أجهزة الكمبيوتر والأجهزة الخاصة بك عند الابتعاد عنها.
- استخدم شاشات الجهاز التي تمنع الآخرين من رؤية المعلومات على جهاز الكمبيوتر لديك.
- عدم النقر مطلقًا فوق الارتباطات دون التفكير بشأنها.

كيف يمكن للمصممين والمهندسين والمنشئين لأفضل النظم الاعتماد على السلوك البشري لتحسين كيفية تأمين الشركات لشبكاتها وأصولها؟

أسلحة المستقبل العصرية

يشير "علي" وباحث الأمان "جريفين" إلى عدد من ابتكارات HP المتوفرة حاليًا للجمهور التي لا تعرقل إنتاجية المستخدمين، مما يحثهم على عدم تجاهلها أو تعطيلها.

وأحد هذه الابتكارات المتطورة هو HP Secure، فهو عبارة عن مجموعة من أدوات حماية الكمبيوتر تتضمن Sure View وSure Click وSure Start.

HP Sure View هي شاشة خصوصية مدمجة تعمل على منع الآخرين من قراءة البيانات على شاشات المستخدمين. يقول جريفين "إن هذه ميزة أمان رائعة". وأضاف "إنها سهلة الاستخدام وأنهم يعلمون ما تقدمه هذه الشاشة."

HP Sure Click هو معيار أمان يطبق على مستوى الأجهزة لمستعرضات الويب يعزل البرامج الضارة على جهاز افتراضي لمنع إصابة النظام بها. يقول على متسائلاً "كم عدد المرات التي نقرت فيها على ارتباط وقلت على الفور "أوه! هذا هراء، لم يكن ينبغي لي النقر فوقه؟". وأضاف "بفضل استخدام Sure Click، لم تعد هناك برامج ضارة في جهازك فعليًا. وإذا تم تنزيل برنامج ضار عن طريق الخطأ، فما على المستخدمين سوى إغلاق علامة التبويب وسيختفي كل شيء. إنه لأمر رائع، لأننا لن نطلب من المستخدمين تغيير سلوكهم لجعل التصفح أكثر أمانًا."

هذا النوع من تصميم الأمان الإلكتروني الذي يتجاوز خطأ المستخدم سيقطع شوطًا طويلاً نحو الحد من العامل البشري الكبير المؤثر في عمليات الاختراق الشبكة.

شاشة الخصوصية HP Sure View المدمجة ميزة اختيارية يجب تكوينها وقت الشراء. وهي متوفرة على أجهزة كمبيوتر محمولة محددة من HP فقط.

يتوفر HP Sure Click في أنظمة أساسية مختارة من شركة HP ويدعم المستعرضين Microsoft® Internet Explorer و Chromium™.
تحقق هنا للإطلاع على جميع الأنظمة الأساسية المتوافقة بمجرد توافرها.

تتوفر تقنية **HP Sure Start Gen٤** على منتجات HP Elite وHP Pro ٦٠٠ المزوّدة بمعالجات Intel® أو AMD من الجيل الثامن.

HP Sure Start عبارة عن إعادة تصور للحماية من البرامج الضارة عن طريق تحليل البرنامج الثابت لنظام BIOS، وهو الجزء الأساسي في نظام تشغيل الكمبيوتر – إذن إنها منطقة معرّضة بشكل متزايد للهجمات لأنه من الصعب للغاية اكتشاف اختراقها. بدون وجود حماية مناسبة، تكون البرامج الضارة المثبتة على BIOS غير مرئية، مما يسمح للمهاجمين بالوجود المستمر على الشبكة. وقد كشفت دراسة "تقرير تحقيقات اختراقات البيانات في Verizon لعام ٢٠١٦" أن هذا النهج يتبناه المهاجمون بشكل متزايد على النحو التالي: لاحظ المحللون ارتفاعًا بنسبة ١٣٢ بالمائة في الحوادث التي تستهدف أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر المكتبية خلال العام المنصرم.[٣٢]

فبرنامج HP Sure Start يمنع المحتالين من التواجد على نظام BIOS. وبمجرد تشغيل جهاز الكمبيوتر، تتحقق الميزة المضمّنة من خلو BIOS من البرامج الضارة. وإذا لم يكن الأمر كذلك، يستعيد HP Sure Start التعليمات البرمجية إلى إصدار سليم تلقائيًا دون تدخل المستخدم أو الحاجة إلى قسم تكنولوجيا المعلومات. يقول علي "إن هذا الإجراء يجعل الجهاز آمن دائمًا".

القسم ٣:

إلقاء نظرة دقيقة: تعلم الآلة والذكاء الاصطناعي

الحفاظ على السلامة الرقمية للأجهزة والشبكات المتصلة بدأت في الحصول على بعض المساعدة من الذكاء الاصطناعي من خلال تعلم الآلة.

وعلى الرغم من أن أفضل الممارسات الحالية في مجال الحماية الإلكترونية تتضمن تقنيات متعددة الطبقات، وعمليات تسجيل دخول باستخدام القياسات الحيوية (من جسم الإنسان)، ومراقبة الشبكة، إلى جانب تثقيف الموظفين بشأن الممارسات السليمة على الإنترنت، فإن الحفاظ على السلامة الرقمية للأجهزة والشبكات المتصلة بدأت في الحصول على بعض المساعدة من الذكاء الاصطناعي من خلال تعلم الآلة.

وهناك برامج أخرى متطورة من HP يمكنها سد ثغرات الطابعات الطرفية المتصلة بالشبكات. تم تطوير HP Connection Inspector في HP Labs وهو متاح حاليًا، إذ أنه عبارة عن ميزة أمان مضمّنة تتعرف على شكل سلوك الشبكة العادي للطابعة، ثم تراقب التغييرات المشكوك فيها. وعندما تكتشف أن البيانات الصادرة غير معتادة، تنبه المسؤولين وتوقف الاتصالات المشكوك فيها، ثم تفرض إيقاف التشغيل للإصلاح الذاتي لإزالة البرامج الضارة وإيقاف الهجوم.

هذه التطورات تعطي "كينت" الذي يعمل لدى شركة NAES مقياسًا للتفاؤل الحذر. فهو ينتظر اليوم الذي يستطيع فيه الفنيون توصيل جهاز بالشبكة لمراقبة التهديدات غير المرئية داخل تيارات اتصالات البيانات وإغلاق تبادل البيانات على الفور في حالة اكتشاف اختراق ثم يدرس تفاصيل الهجوم ليضع نموذجًا لما سيكون عليه هجوم مماثل إذا ما جاء في المستقبل. فهو يقول "إنه بمثابة صندوق ذكاء اصطناعي يراقب كل شيء ويوقف التهديد تلقائيًا بمجرد ظهوره – وسيكون ذلك رائعًا".

إدخال أجهزة إنترنت الأشياء تحت مظلة الدفاع

إن تضمين المعالجات ووصول الإنترنت في منظِمات الحرارة وأجهزة استشعار الحركة والإضاءة والأنظمة الأخرى يتيح للمبنى الذي يوجد به المكتب التمكن من توفير الطاقة بشكل كبير تلقائيًا استنادًا إلى الوظيفة ووقت اليوم وحتى الطقس.[٣٣] فتوربينة الرياح تبلغ المدير بأن التروس داخل هيكل المحرك تهتز بشدة وتحتاج إلى الانتباه[٣٤]. إذ يعمل المحرك التجاري النفاث وكمبيوتر الطيران معًا على إجراء تغييرات دقيقة تقلل من احتراق الوقود وتوفير الوقت.[٣٥]

تأتي هذه الأجهزة الذكية أيضًا إلى منازلنا في شكل منظمات حرارة ذكية ومبردات ذكية ومصابيح ذكية ومساعدات رقمية مدعومة بالذكاء الاصطناعي. وفي المستقبل، ستتوفر

لدينا أيضًا أذرع صناعية وزراعات شبكية ستندمج مع المعالجات الصغيرة وتعزز الاتصال بالإنترنت. ولكن ماذا يحدث إذا استهدفها المخترقون؟

يقول علي كبير التقنيين في HP "فكر في زراعة شبكية أو شخص عنده بتر ولديه ساق مصنوعة بتقنية الطباعة ثلاثية الأبعاد وتخيل إذا حدث هجوم على البرنامج الثابت لهذا العضو الاصطناعي أو أصيب ببرنامج طلب الفدية". وتساءل "ما الذي سيبدو عليه الوضع؟ وماذا سيفعل الأشخاص إذا فقدوا أبصارهم فجأة وتلقوا رسالة تطلب منهم الدفع، وإلا لن يتمكنوا من الرؤية؟"

وهذا هو الحيز الذي نحتاج فيه إلى المرونة للسماح للأجهزة المصابة بالتخلص من البرامج الضارة بسرعة والعودة إلى العمل في حالة سليمة. وأضاف على "بمجرد أن تصاب زراعة شبكية ببرنامج ضار أو برنامج طلب فدية، فما عليك فعله هو فتح العينين وإغماضهما وستختفي البرامج الضارة وستستعيد الرؤية".

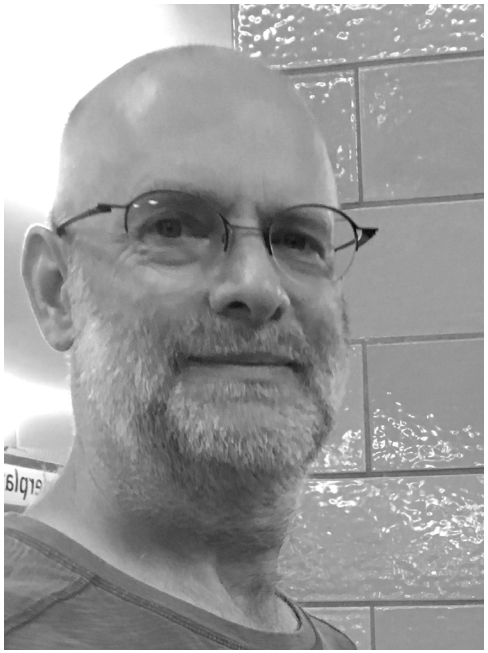
وأضاف "للقيام بذلك، سيحتاج مصنّعو إنترنت الأشياء أن يتعلموا ما تعلمته باقي قطاعات التكنولوجيا على مدى عقود من التركيز غير الكافي على الأمان: إذ تحتاج أجهزة إنترنت الأشياء إلى دمج نظام الأمان بها في الأساس. وإذا تعرض مصباح ذكي إلى برنامج ضار، فمن المفترض أن يتم إيقافه وإعادة تشغيله والتخلص من التعليمة البرمجية الضارة وبدء الإنارة مرة أخرى.

سهولة الاستخدام تحمي من السلوك السيئ

يقول جريفين "إذا اضطررت إلى وضع مفتاح في بابي، وتعين عليّ انتظار رسالة نصية قصيرة للتحقق من أنني كنت أحاول الدخول إلى منزلي، فلن أقبل ذلك". وأضاف "يجب ألا أعيق الطريق كي أتمكن من مواصلة حياتي."

لمعالجة هذه المشكلة التي استمرت لفترة طويلة، ظل المهندسون يعملون على إدخال تحسينات على تسجيل الدخول لسنوات باستخدام ميزة التعرف على الوجه المعتمدة على النظر وبصمات الأصابع، أو تحديات القياسات الحيوية الشبكية سعيًا لاستبدال كلمات المرور الأبجدية الرقمية القديمة بشكل تدريجي.[٣٦]

"إنه سباق تسلح، ومن الصعب دائمًا معرفة الطريق الذي سيسلكه المهاجمون بعد ذلك."



جوناثان جريفين،
باحث أمان كبير في HP Labs

هناك حل آخر يتمثل في تقنية HP WorkWise، فهي عبارة عن تطبيق مجاني متوفر على Google Play ينشئ ارتباطًا مشفرًا آمنًا بين الهاتف الذكي للموظف والكمبيوتر. وباستخدام هذا الارتباط، يمكن للكمبيوتر معرفة وقت ابتعاد المستخدم عنه، مما يتسبب في تأمين جهاز الكمبيوتر تلقائيًا كي لا يتمكن الآخرون من الوصول إليه. وعندما يعود المستخدم، يتعرف الكمبيوتر عليه ويسجل دخوله مرة أخرى دون الحاجة إلى كلمة مرور. فهذه التقنية تُستخدم لتسجيل الخروج ومساعدة المستخدمين على البقاء في أمان دون مطالبتهم بفعل أي شيء إضافي.

يقول علي "يوجد نوعان من التكنولوجيا. النوع الذي يرغب المستخدمون في استخدامه والنوع المزعج الذي يتعين عليهم استخدامه. وإذا كان نوع الأمان مزعجًا ويضطرون إلى استخدامه، فسيجدون في النهاية طريقة لتجاوزه."

تعلم الآلة هو سلاح ذو حدين

لقد ولت تلك الأيام التي كان يتم فيها فحص البرامج الضارة كأداة رئيسية ضد المهاجمين.[٣٧] لذا، يتعين تحديث برنامج مكافحة البرامج الضارة بتعليمات برمجية خاصة بالبرامج الضارة المعروفة من أجل التعرُف على ما يبحث عنه البرنامج. وهذا لا يكون مساعدًا عندما يتم إطلاق تعليمات برمجية ضارة جديدة على الويب، وهو ما يحدث بسرعات تفاجئ الباحثين.

ومن جانب المدافعين، بدأ استخدام البيانات بالإضافة إلى تعلم الآلة لتغذية التحليل التلقائي للشبكة، وهذا يعمل على تجميع البيانات من التدفق الثابت المستمر الداخل إلى شبكة الشركة والخارج منها بحثًا عن الحالات الشاذة. فلا شك أن إمكانيات الكمبيوتر هذه ستراقب في يوم من الأيام الارتفاع في نشاط المعالج على سبيل المثال، مما قد يشير إلى أن المشكلة قد بدأت. ومن جانب المهاجمين، يمكن بالتأكيد استخدام التعلم الآلي لأتمتة فحص الشبكة ومسحها وتنقيحها.

يقول جريفين الذي يعمل لدى HP بأن التعلم الآلي وأشكال أخرى من الذكاء الاصطناعي تمنح المدافعين ميزة فعليًا. لكنه يحذر من أن أدوات، مثل تعلم الآلة ليست علاجًا شاملاً. ولكن في الواقع، من المرجح أن يوفر تعلم الآلة بيئة هجوم جديدة للمخترقين الذين يبحثون عن نقاط ضعف في وسائل الحماية المستندة إلى تعلم الآلة وباستخدام تعلم الآلة/الذكاء الاصطناعي ذاته لإعداد هجمات أرخص وأكثر فعالية. وأضاف "إنه سباق تسلح، ومن الصعب دائمًا معرفة الطريق الذي سيسلكه المهاجمون بعد ذلك".

هل سيحل الذكاء الاصطناعي مشكلة الأمان الإلكتروني أم أنه سيزيدها سوءًا؟

في وقت ما من المستقبل القريب، سوف تتطور الخوارزميات المتقدمة التي تُستخدم بشكل أساسي في حل مشاكل تعلم الآلة إلى أنظمة ذكاء اصطناعي أكثر قوة. وسوف يستخدم المهاجمون المدعومون بالموارد الذكاء الاصطناعي في اختبار الشبكات ومهاجمتها. وستتيح لهم التكنولوجيا القوية تطوير الحيل الهندسية التي يستخدمونها لزيادة صعوبة تمييز هجمات التصيد الاحتيالي والبرامج الضارة عن الرسائل الإلكترونية والمواقع الإلكترونية العادية. فكل من المهاجمين والمدافعين سينشر الذكاء الاصطناعي لإعادة توجيه تدفقات بيانات الشبكة بشكل ذكي خلال هجمات "حجب الخدمات الموزّع" لزيادة الضرر أو الحد منه.

يقول علي "إننا سنعيش في عالم من الهجمات الذكية التي يدعمها الذكاء الاصطناعي". وأضاف "ربما حدث ذلك بالفعل، لكن النظام ذكي بدرجة كافية لم تمكن أحدًا من اكتشافه."

ويجب على المهندسين في المستقبل تطوير إمكانيات التعلم الديناميكي للذكاء الاصطناعي بما يكفي لتمكين أنظمة المدافعين من استخدام البيانات العامة والاتجاهات الحالية للمساعدة في التنبؤ بالهجمات أو إحباطها أو احتوائها، وربما حتى تعقب مواقع الجهات الإجرامية الفاعلة.

أما في الوقت الحالي، فقد بدأت الشركات المصنّعة في الاهتمام بإنتاج أجهزة مثل تلك التي يحلم بها "كينت" الذي يعمل لدى شركة NAES مثل: جهاز يتضمن تقنيات الذكاء الاصطناعي. فكانت الخطوة الأولى هي وضع الأمان في قلب المنتجات منذ بداية عملية التصميم.

الفوز في معركة لا تنتهي ضد الشر

تشتد الحرب الطاحنة بين الأخيار والأشرار والتي تكون فيها النتائج متفاوتة في كل صناعة. ونظرًا لبذل العناصر الإجرامية والسياسية قصارى جهدها لاختراق الشبكات وتعطيلها، فقد كانت المخاطر هائلة، ولم تكن هناك إمكانية للتخلص من التهديدات.

إذ تعتبر حماية موثوقية الأنظمة الرقمية التي تدعم البنية الأساسية والمؤسسات

> هناك معركة مستمرة بين الأخيار والأشرار. إنها معركة لا يمكن أن نخسرها، كأشخاص طيبين. إنها معركة يجب ألا نخسرها. فنحن في HP ملتزمون بما يلي: هذه معركة لن نخسرها.

الحكومية بالغة الأهمية، فضلاً عن الشركات الكبيرة والصغيرة أمرًا أساسيًا للحياة العصرية وسبل العيش والمجتمع. يقول علي الذي يعمل لدى HP "نحن نعتقد أنه عالم مخيف، ولكن هناك أيضا الخير". وأضاف "هناك معركة مستمرة بين الأخيار والأشرار. إنها معركة لا يمكن أن نخسرها، كأشخاص طيبين. إنها معركة يجب ألا نخسرها. فنحن في HP ملتزمون بما يلي: هذه معركة لن نخسرها."

التعليقات الختامية

١. Robotics Business Review، "Robot Investments Weekly: الذكاء الاصطناعي والأتمتة الاصطناعية والإنفاق المحفز للأجهزة المحمولة،" https://www.roboticsbusinessreview.com/financial/robot-investments-weekly-ai-industrial-automation-mobility-market-drive-spending/ (تم الوصول إليه في ٢٦ فبراير ٢٠١٨)

٢. TechEmergence، "تطبيقات اكتشاف العقاقير من خلال تعلم الآلة" – Pfizer وRoche وGSK وغيرها، https://www.techemergence.com/machine-learning-drug-discovery-applications-pfizer-roche-gsk/ (تم الوصول إليه في ٢٦ فبراير ٢٠١٨)

٣. Popular Mechanics، "الجراح سيحدثك الآن على Skype،" https://www.popularmechanics.com/science/health/a19208/the-surgeon-will-skype-you-now/ (تم الوصول إليه في ٢٦ فبراير ٢٠١٨)

٤. CFO، "هبوط الأسهم الرئيسية بسبب الهجمات الإلكترونية،" http://ww2.cfo.com/cyber-security-technology/2017/04/cyber-attacks-stock-drops/ (تم الوصول إليه في ٢٦ فبراير ٢٠١٨)

٥. Kaspersky، "خريطة التهديدات الإلكترونية في الوقت الحقيقي: الإصابات المحلية في الأسبوع الماضي،" https://cybermap.kaspersky.com/stats/ (تم الوصول إليه في ٢٦ فبراير ٢٠١٨)

٦. Anti-Phishing Working Group، "استطلاع التصيد الاحتيالي العالمي،" https://apwg.org/resources/apwg-reports/domain-use-and-trends

٧. G DATA Security Blog، "اتجاهات البرامج الضارة لعام ٢٠١٧،" https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017

٨. خريطة الهجمات الرقمية، ما المقصود بهجوم "حجب الخدمات الموزّع؟" http://www.digitalattackmap.com/understanding-ddos/

٩. خريطة الهجوم الرقمي، "أعلى الهجمات اليومية لحجب الخدمات الموزّع،" http://www.digitalattackmap.com/

١٠. وزارة الدفاع الأمريكية، "DISA Director Warns ،Terabyte of Death' Cyberattack Against DoD Looms" https://www.defense.gov/News/Article/Article/1414146/

١١. HP، دراسة أجرتها HP تكشف عن أن ٧٠ بالمائة من أجهزة إنترنت الأشياء تتعرض للهجوم، http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

١٢. Greenfield Daily Reporter، "ضحايا سقوط المستشفيات في هجوم المخترقين؛ عدم وجود سجلات مرضى مخترقة،" http://www.greenfieldreporter.com/2018/01/12/hospital-falls-victim-to-hacker-attack-no-patient-records-compromised-officials-said/

١٣. Black Hills Pioneer، "اختراق خوادم مدينة بيل فورش،" http://www.bhpioneer.com/local_news/belle-fourche-city-servers-hacked/article_7254ad36-f576-11e7-8ed7-e31c3ee0da87.html

١٤. Columbia Daily Herald، "معاناة MCPS من الهجمات الإلكترونية،" http://www.columbiadailyherald.com/news/20180105/mcps-experiences-cyber-attack

١٥. Bloomberg Technology، "لا يمكن أن يكون هذا حقيقيًا. من داخل انهيار صناعة أشباه الموصلات،" https://www.bloomberg.com/news/articles/2018-01-08/-it-can-t-be-true-inside-the-semiconductor-industry-s-meltdown

١٦. The Economic Times of India، "اختراق ٣,٢ مليون بطاقة مدين بنكية؛ SBI وبنك HDFC وICICI وYES Bank وAxis Worst Hit،" (Paywall) https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms

١٧. CNBC، "الابتزاز الافتراضي عمل كبير لمجرمي الإنترنت،" https://www.cnbc.com/2016/02/17/ransomware-is-targeting-us-companies-of-all-sizes.html

١٨. Cybersecurity Ventures، "تقرير الجرائم الإلكترونية،" https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

١٩. مقابلة تليفونية مع "جيسون أوكيفي" لدى HP (في ١٤ ديسمبر ٢٠١٧)

٢٠. مقابلة تليفونية مع شيفان أولبرايت لدى HP (في ١٥ ديسمبر ٢٠١٧)

٢١. CoinDesk، "شبكة روبوت للاختراق تصيب نصف مليون خادم من أجل تعدين آلاف من عملة المونيرو،" https://www.coindesk.com/botnet-infects-half-million-servers-mine-thousands-monero/

٢٢. مقابلة تليفونية مع دانيال كلاي بشركة Shieldly (في ١٠ يناير ٢٠١٨)

٢٣. فاينانشيال تايمز، "الخدمات الأساسية تواجه غرامات بسبب ضعف الأمان الإلكتروني،" (Paywall) https://www.ft.com/content/f2faf8cc-7b79-11e7-ab01-a13271d1ee9c

٢٤. Houston Chronicle، "عواقب الأمان السيئ في الشركات،" http://smallbusiness.chron.com/consequences-poor-security-company-70227.html

٢٥. IBM وPonemon Institute، "دراسة تكلفة اختراق البيانات في Ponemon Institute لعام ٢٠١٧،" https://www.ibm.com/security/data-breach

٢٦. مقابلة تليفونية مع جوناثان جريفين لدى HP (في ٢١ ديسمبر ٢٠١٧)

٢٧. مقابلة تليفونية مع ألن كينت لدى NAES (في ١٥ يناير ٢٠١٨)

٢٨. مقابلة تليفونية مع فالي علي لدى HP (في ١٥ ديسمبر ٢٠١٧)

٢٩. Keeper Security، "حالة الأمان الإلكتروني في الشركات الصغيرة والمتوسطة عام ٢٠١٧،" https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html

٣٠. Digital Guardian، "هجمات الهندسة الاجتماعية: التقنيات الشائعة وكيفية منع هجوم،" https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

٣١. Verizon، "تقرير تحقيقات اختراق البيانات لعام ٢٠١٦،" http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

٣٢. Intel، "خفض تكاليف الطاقة والتأثير الكربوني عن طريق الإدارة الذكية للمباني،" https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/iot-ecs-tatung-reduce-carbon-footprint-solution-brief.pdf

٣٣. Industrial Internet Consortium، "فوائد تحليلات إنترنت الأشياء للطاقة المتجددة،" https://www.iiconsortium.org/case-studies/ParStream_Envision_Energy_Case_Study.pdf

٣٤. Aviation Week، "إنترنت الطيران: مجموعة صناعية للتحول،" http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed

٣٥. Global Cyber Alliance، "كيف يمكن للقياسات الحيوية استبدال كلمات المرور،" https://www.globalcyberalliance.org/how-biometrics-can-replace-passwords.html

٣٦. Wall Street Journal، "حدود برامج مكافحة الفيروسات،" (Paywall) https://www.wsj.com/articles/the-limits-of-antivirus-software-1505700000

لمعرفة المزيد، تفضل بزيارة
www.hp.com/go/explorehpsecure

4AA7-3259ARE