مستند فني

أبواب بدون أقفال

تبين الدراسات أن الطابعات تبقى مكشوفة أمام هجمات القراصنة

بينما تركز طواقم تقنية المعلومات على نقاط طرفية أخرى، تبقى حماية طابعات الشركات متخلفة

تعد الطابعات أهدافًا سهلة: ذلك أن عددًا كبيرًا جدًّا من الطابعات المتصلة بالشبكة ليست محمية بأية قيود فتأمينها دون المستوى اللازم.

هذا مع أن الخطر واقعي لا يستحق التجاهل. لقد تطورت طابعات الشركات فأصبحت أجهزة متصلة قوية ذات نفس نقاط الضعف مثل أي جهاز طرفي متصل آخر. ونظرًا لعدم توفير الحماية لتلك المداخل إلى الشبكة في معظم الحالات، فهجمات القراصنة تصير خطرًا وقعيًّا جدًّا؛ علاوة على ذلك قد تتيح الأجهزة المذكورة الوصول إلى بيانات شركتك المالية والخصوصية مما قد يؤدي إلى تداعيات خطيرة جدًّا على أعمالك.

وبما يتناقض تمامًا مع هذه المعطيات فإن دراسة أجريت من قبل شركة Spiceworks مؤخرًا والتي شملت أكثر من ٣٠٠ من ذوي النفوذ في مجال تقنية المعلومات في مختلف الشركات أظهرت أن ١٦٪ فقط من أجاب على السؤال اعتقدوا أن الطابعات تمثل ثغرة أمنية أو خطرًا أمنيًّا كبيرًا. وهو معدل قليل جدًّا بالنسبة إلى الآراء الشائعة بخصوص أجهزة الكمبيوتر المكتبية أو المحمولة والأجهزة المحمولة الأخرى.[1] وكان هذا الاعتقاد هو الذي أضفى الصبغة السائدة على نظرية طواقم تقنية المعلومات تجاه أمان الشبكات. ومع أن معدل الشركات التي تحمي طابعاتها بشكل أو بآخر يبلغ ثلاث من ضمن كل خمس شركات، إلا أن هذا المعدل يعد أقل بكثير نسبة إلى النقاط الطرفية الأخرى — مما يترك الطابعات ضعيفة. بالرغم من وجود حلول سهلة لمعالجة هذا النوع المعين من نقاط الدخول إلى الشبكة.

ويقدم هذا المستند الفني المعلومات عن أمان الطابعات استنادًا إلى استطلاع الرأي المذكور لشركة Spiceworks، إلى جانب تداعيات الثغرات الأمنية وبعض ميزات الأمان الحديثة المدمجة المصممة لحماية الطابعات ضد هجمات القراصنة.

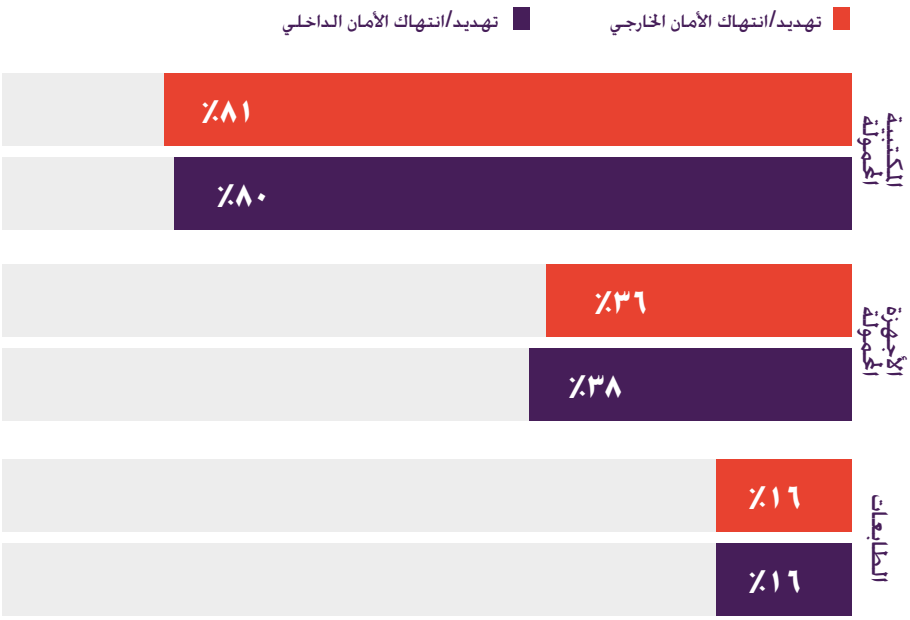
١٦٪ فقط من أجاب على السؤال اعتقدوا أن الطابعات تمثل ثغرة أمنية أو خطرًا أمنيًّا كبيرًا.[1]

أبواب مفتوحة للهجمات

في استطلاع الرأي لشركة Spiceworks، أجاب ٧٤٪ ممن رد على السؤال (صافي) أن شركتهم كانت قد تعرضت لنوع واحد على الأقل من انتهاكات أو تهديدات تقنية المعلومات الخارجية في السنة المنصرمة. بينما تعرض ٧٠٪ منهم (صافي) لانتهاكات أو تهديدات على أمان تقنية المعلومات كان مصدرها داخل المؤسسة، والتي كانت من بين أسبابها الشائعة أخطاء المستخدمين أو استخدام أجهزة شخصية لأغراض العمل أو استخدام الموظفين الشبكات المنزلية أو العمومية لأغراض العمل.[1]

أبرز تهديدات/انتهاكات أمان تقنية المعلومات الخارجية شوهدت

وكانت أغلبية التهديدات قد نتجت وتجسدت عبر استخدام الكمبيوترات المكتبية والمحمولة، بينما نجمت الأخرى عن الأجهزة المحمولة والطابعات.١ (ويعد معدل ١٦٪ وهو نسبة التهديدات التي نفذت عبر الطابعات أعلى بكثير من المعدل الذي وجدته دراسة مشابهة أجرته شركة Spiceworks عام ٢٠١٤ **والذي لم يبلغ أكثر من ٤٪**). ومن المحتمل أيضًا أن عدد الهجمات التي يتم تنفيذها عبر الطابعات لا ينال القدر اللازم من الاهتمام لأن الطابعات لم تتم مراقبتها بشكل كثيف مثل أجهزة الكمبيوتر والأجهزة المحمولة.



إننا نهمل طابعاتنا

كانت الحالة مهما كانت، تبين دراسة Spiceworks أن حماية الطابعات لم ننتبه إليها عادة إلا بعد حدوث المشكلة.

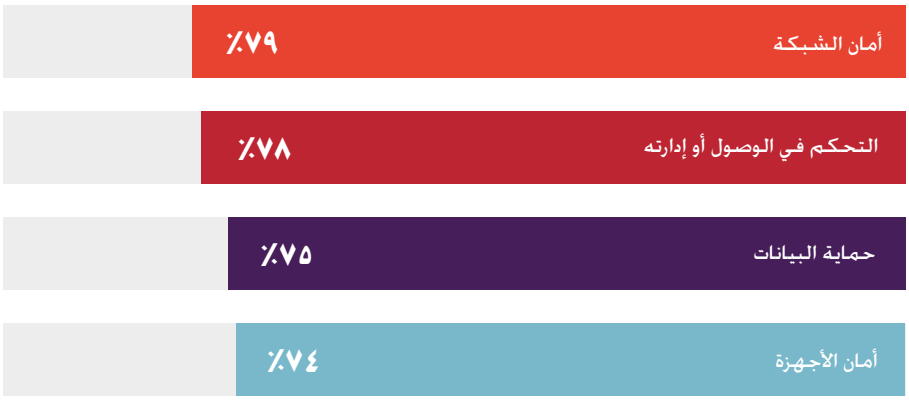
وتكترث الشركات اكتراثًا خاصًّا بأهمية حماية الشبكة والنقاط الطرفية والبيانات. فقد تبين أن أكثر من ثلاثة أرباع ممن أجاب على السؤال يستخدمون وسائل حماية الشبكة أو التحكم في الوصول وإدارته أو حماية البيانات أو حماية النقاط الطرفية أو حلولاً تدمج بين التقنيات المذكورة.[1]

ولكن هذه الحلول لا تجد طريقها إلى الطابعات في معظم الحالات. ومع أن ٨٣٪ من المجيبين يستخدمون وسائل حماية الشبكات على أجهزة الكمبيوتر المكتبية/المحمولة و ٥٥٪ على الأجهزة المحمولة، لا يطبقها على الطابعات سوى ٤١٪ منهم.[1]

وتكون هذه الفجوة بالنسبة للنقاط الطرفية أوسع:

علاوة على ذلك، لا يطبق شهادات الأمان على الطابعات سوى أقل من ثلث المجيبين (٢٨٪)، مقارنة بنسبة ٧٩٪ لأجهزة الكمبيوتر و ٥٤٪ للأجهزة المحمولة.١

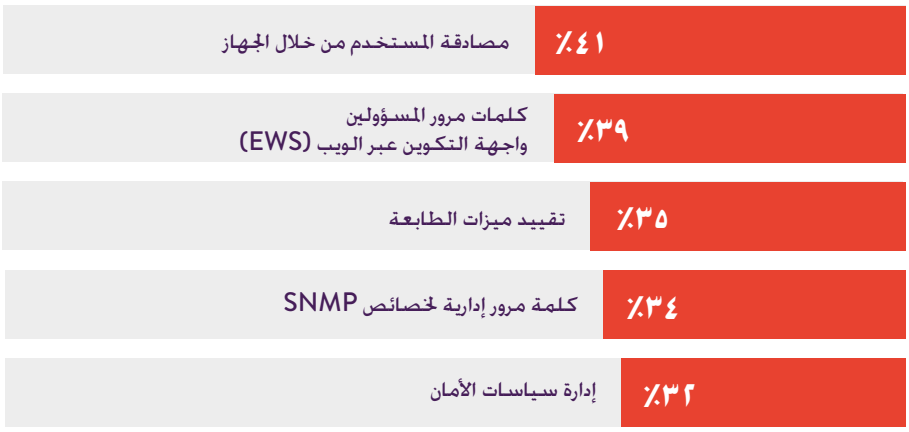
أبرز ممارسات الحماية الخاصة بالنقاط الطرفية



ومن وسائل الحماية المستخدمة بالنسبة للأجهزة الطرفية العامة كانت أكثر وسائل الحماية تطبيقًا على الطابعات حماية المستندات، وحماية الشبكة، والتحكم في الوصول، ولكن نسبة أقل من نصف المجيبين أفادوا بأن شركاتهم تطبق أية الوسائل المذكورة على طابعاتها.[1]

ومع أن بعض الشركات تطبق ممارسات الأمان الخاصة بالطابعات بالفعل، إلا أن الممارسات المذكورة تتفاوت بشكل كبير بين الشركات المختلفة. ٤٠٪ من الشركات فقط أو ما يزيد عنها بقليل كانت قد طبقت مصادقة المستخدم، وأقل من ٤٠٪ منها كانت تستخدم كلمات مرور المسؤول على واجهة التكوين عبر الويب.[1] حيث أنه للحصول على دفاع يمكن اعتباره قوي، على كل شركة أن تستخدم مزيجًا من تلك الاتجاهات — وأكثر.

أبرز ممارسات الحماية الخاصة بالطابعات



وبما يخص امتثال النقاط الطرفية وممارسات التدقيق، فوسائل التحكم في الطابعات تتخلف وراء جميع ممارسات النقاط الطرفية تقريبًا. فمع أن نسبة ٩٠٪ من الشركات تتمتع بتطبيق سياسة أمان، لا تجد تلك السياسات طريقها إلى الطابعات عادةً، كما ذكرنا. وعلى سبيل المثال، بينما قال ٥٧٪ من المجيبين أنهم يطبقون وسائل مكافحة البرنامج الضارة على أجهزة الكمبيوتر، لم يطبقها على الطابعات سوى ١٧٪ منهم.[1]

٩ من ١٠ أخصائي تقنية المعلومات تفيد بأن لشركتهم سياسة متعلقة بأمان المعلومات للأسباب الآتية:

من الواضح أن الشركات لم تكرس المستوى اللازم من الاهتمام للطابعات — فيجب أن تفعل بلا أدنى شك.

"هناك العديد من الطابعات التي لم تزل لديها كلمات المرور الافتراضية أو أنها لم تكن محمية بكلمة مرور على الإطلاق، أو يستخدمها عشرة مستخدمين بنفس كلمة المرور". هكذا قال مايكل هوارد، مستشار الأمان الرئيسي لدى HP، لمجلة Computerworld في شهر يونيو. "تعد الطابعات غير المحمية بكلمات مرور منجمَ ذهب بالنسبة للقراصنة، ومن الانتهاكات الشائعة جدًّا هجوم بواسطة عامل وسيط حيث تتم السيطرة على الطابعة وتحويل [المستندات الواردة] إلى الكمبيوتر المحمول قبل أن تصل مرحلة الطباعة. هكذا يمكنهم مشاهدة جميع ما يطبعه الرئيس التنفيذي."[٢]

التأثير المحتمل لاختراق الطابعات

وفقًا لما أفاد به أحد كبار الخبراء في مجال تحليل التهديدات الإلكترونية في شركة Bitdefender، بوغدان بوتزاتو، تمثل الطابعات ثغرة أمنية محتملة كبيرة. "إننا نتلقىالعديد من المعلومات والمعطيات في مختبراتنا المخصصة لتقييم نقاط الضعف. وتفيد هذه المعلومات أن الموجهات لم تعد أسوأ جهاز على شبكة الإنترنت. فاليوم إنها الطابعات التي احتلت هذا الدور."[٣]

وقد تؤثر نقطة الضعف هذه على الشركات بشكل خطير، ذلك أن طابعة واحدة غير محمية تكفي لتعريض كامل شبكة الأجهزة المتصلة الخاصة بك للهجمات المختلفة، مانحةً القراصنة القدرة على التجسس على أجهزتك المتصلة — إلى جانب الطعن في أمان الشبكة بأسرها.

١. عدد متزايد من المكالمات مع مكتب المساعدة وزيادة الوقت المكرّس لعمليات الدعم

٢. تقليل الإنتاجية/الفاعلية

٣. زيادة وقت تعطيل الأنظمة

٤. زيادة الوقت المخصص لمكالمات الدعم

٥. زيادة الأنشطة التطبيقية لسياسات المستخدم النهائي

لقد شاهدنا جميعًا تأثيرات انتهاكات الأمان. ففي استطلاع الرأي لشركة Spiceworks سرد المجيبون أبرز التأثيرات الخمس للانتهاكات هي:[١]

علمًا بأن انتهاكات الأمان الناجمة عن الطابعات قد تكون أكثر جسامة منها جميعًا، وبخاصة إن كنت تستخدم طابعة متعددة الوظائف قادرة على تخزين البيانات المطبوعة إلكترونيًّا. فمهام

الطباعة المخزنة في التخزين المؤقت للطابعة قد تتيح للقراصنة الوصول إلى معلومات شخصية أو تجارية حساسة.

وهناك مخافة أكثر ألا وهي فتح المجال أمام القراصنة للوصول إلى شبكة الشركة الأوسع عبر الطابعات غير المحمية. وسرقة أشياء مثل أرقام التأمين الوطني، أو المعلومات المالية أو المذكرات والمستندات الداخلية. حيث من المحتمل ألاّ تؤثر المعلومات المسروقة على الأفراد من الموظفين فحسب بل أن يستخدمها المنافسون أو أن تؤدي إلى الطعن في سمعة الشركة بشكل خطير.

الحل البسيط: ميزات الأمان المضمنة

لا شك أن الشركات يلزمها معالجة مسائل الأمان حتى في طابعاتها. تقدم بعض الطابعات الحديثة المعدة للشركات ميزات الأمان المدمجة السهلة الاستخدام والتي تكافح التهديدات على الطابعات. بما في ذلك:

- الاكتشاف التلقائي للهجمات والحماية والاسترداد التلقائيين
- تعقب الاستخدام لتجنب الاستخدام غير المصرح به
- خيارات تسجيل الدخول البسيطة مثلاً أرقام PIN أو البطاقات الذكية
- قارئ بطاقات استشعاري يتيح للمستخدمين إجراء المصادقة السريعة والطباعة الآمنة من عند الطابعة أو باستخدام بطاقات التعريف.
- الطباعة المشفرة الآمنة للمستندات الحساسة

عند اعتبارك شراء طابعتك القادمة، سواء المكتبية أو المتعددة الوظائف، لا تنس التحقق من وجود وسائل أمان مدمجة — كما لا تنس تنشيطها. فمع مثل هذه الميزات البسيطة المكيفة للطابعة، لا يبقى أي سبب للإصرار على تعريض طابعاتك للمخاطر؛ فمع انتشار إنترنت الأشياء هناك نقاط وصول عديدة أخرى تثير القلق — يجب ألاّ تكون طابعاتك منها.

هل تبحث عن طابعة أكثر أمانًا؟

معرفة المزيد ›

المصادر:

١ استطلاع للرأي لشركة Spiceworks شارك فيه ٣٠٩ من أصحاب القرار في مجال تقنية المعلومات في أمريكا الشمالية ومناطق EMEA و APAC، بطلب من HP، نوفمبر ٢٠١٦.

٢ "Printer Security: Is your company's data really safe?" *Computerworld*, June 1, 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

٣ "Printers Now the Least-secure Things on the Internet," *The Register*, September 8, 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/