تقرير فني تفصيلي

تلبية مُتطلبات الامتثال لأمن الشبكات والبيانات

توصيات لتطبيق إجراءات أمنية على أسطول أجهزة الطباعة

فهرس المحتويات

مخالفة قواعد الامتثال قد تضرّ بأعمالك

يُمكن أن يتسبّب الانتهاك الأمني في خسارة الإيرادات وإلحاق الضرر بسمعة الشركة أو المؤسسة، بالإضافة إلى الغرامات الباهظة والدعاوى القانونية. عندما تشرع في وضع خُطتك الأمنية، تذكّر دائمًا أن شبكتك هي الحلقة الأضعف لديك لذلك يجب تأمينها تمامًا. تتضمّن أجهزة الطباعة والتصوير العديد من نقاط الضعف الأمنية حالها في ذلك حال أجهزة الكمبيوتر المكتبية، ومن الضروري استخدام أجهزة وحلول تُساعدك على تلبية شروط ومتطلبات الامتثال وحماية معلومات الأعمال من التهديدات الأمنية.

ما هي المخاطر؟

إن عدم التوافق والامتثال تنظيمًا وقانونًا تترتب عليه تداعيات مالية جسيمة بالنسبة للشركات الدولية، بما في ذلك الغرامات المالية وفقدان الصفقات والأعمال والطعن في السمعة والدعاوى الجماعية التمثيلية.

كما أن النقاط غير المحمية أو المحمية بشكل غير كافٍ تفتح الباب على مصراعيْه أمام جرائم الإنترنت. جرت شركة Ponemon مؤخرًا استطلاعًا في إطار دراسة لها حيث قررت الشركات التي شاركت في الاستطلاع أنها كانت قد خضعت لمعدل يبلغ هجومين أسبوعيًّا في العالم 2016، حيث يمثل هذا العدد زيادة بواقع 23% نسبة إلى السنة القادمة، وتسببت هذه الزيادة للشركات خسارة بمعدل 9.5 مليون دولار أمريكي سنويًّا في محاربة ومكافحة جرائم الإنترنت.[1] هذا وفي السنة الماضية وحدها تم العبث في ما يزيد عن 4 مليار سجل للبيانات على مستوى العالم، وهو ما يمثل زيادة بنسبة 400% مقارنة بالسنتين الماضيتين.[2]

وعلى الرغم من قيام العديد من إدارات تكنولوجيا المعلومات بتطبيق إجراءات أمنية مشدّدة على الكمبيوترات والشبكة، إلا أنه عادةً ما يتم غضّ النظر عن أجهزة الطباعة والتصوير. ولكن قد تكون الطابعات نقطة الدخول إلى شبكتك، وتأمينها لا يقل أهمية عن تأمين الأجهزة الأخرى. فمن جميع الانتهاكات الخطيرة للبيانات التي أبلغ عنها مديرو تكنولوجيا المعلومات، كان ما نسبته 26% يتعلّق بالطابعات[3].

للمساعدة في التصدي للخطر المتزايد، تقوم الحكومات على مختلف أرجاء العالم بتطبيق تنظيمات أمنية صارمة جديدة والتي تطالب الشركات بتحسين حماية معلومات العملاء. على سبيل المثال يعد نظام EU General Data Protection Regulation (GDPR) واحدًا من التنظيمات الإلزامية الأساسية والذي سيكون ساريَ المفعول اعتبارًا من العالم 2018. يتضمن الـ GDPR متطلبات أكثر شدةً لحماية البيانات من قبل المؤسسات التجارية المختلفة. لذا نوصي بالتحقق من أن جميع الأجهزة المتصلة بشبكتك — من الكمبيوترات إلى الطابعات والأجهزة المحمولة — محمية. هذا النظام الإلزامي لا يسري على بلدان الاتحاد الأوروبي فحسبُ بل يؤثر أيضًا على المؤسسات التجارية العالمية فعليها أيضًا امتثال هذا النظام في حالة تجميعها البيانات واستخدامها من المقيمين في مناطق الاتحاد الأوروبي. سيتعين على الشركات مراقبة الأجهزة كل على حدة وتقييم كل منها بغرض اكتشاف انتهاكات الأمان ورفع التقارير عنها في غضون 72 ساعة من المعرفة بالحادث. إذا اكتشفت تدقيقات الامتثال أنه كانت هناك انتهاكات لم تخضع للمراقبة أو لم يرفع أي تقرير عنها فقد تدفع الشركة محل الحادثة غرامات مالية تصل إلى 20 مليون يورو أو 4% من حجم المبيعات السنوي للشركة.

الاستفادة من الإجراءات الأمنية الشائعة لتحسين الامتثال والارتقاء به

إن مُجاراة لوائح أمن المعلومات والالتزام بها ليس مسألة سهلة على الإطلاق، ولحسن الحظ، فقد وضع مركز أمن الإنترنت (CIS) مجموعة من الإجراءات الأمنية الشائعة لتبسيط توصيات أمن الإنترنت. تتمثل الإجراءات الأمنية الرئيسية لمركز أمن الإنترنت في 20 إجراء يُمكن أن يُسهم اتباعها في التصدي للهجمات الإلكترونية عبر الإنترنت. (للاطلاع على التفاصيل، يُرجى زيارة https://www.cisecurity.org/critical-controls.cfm.) تتفق الإجراءات المذكورة مع العديد من اللوائح الأخرى، مثل توصيات PCI-DSS و27001 ISO وUS CERT وHIPAA وFFIEC وNIST. لا تستهدف هذه الإجراءات أن تحل محل أي من أطر الأعمال الأخرى، ولكن عادة ما تستخدمها الشركات لجعل أطر العمل الأخرى ذات جدوى.

تُولي الإجراءات الأمنية الرئيسية لدى مركز أمن الإنترنت الأولوية لعددٍ بسيط من الأعمال والتي تؤتي بثمارها في تأمين الأجهزة على أكمل وجه. حيث تتعامل مع معظم أشكال التهديدات الشائعة من تقارير التهديدات التي تتعرض لها الأجهزة. ساهم نُخبة من خبراء أمن الإنترنت، من بينهم أشهر المنظمات المعنية بالاستجابة للحوادث والجرائم، في وضع هذه الإجراءات والضوابط. إضافةً إلى ذلك، يتم تحديث الإجراءات بشكل مستمر تجاوبًا مع تزايد التهديدات والهجمات.

استخدام الإجراءات الأمنية الرئيسية التي أعدها مركز أمن الإنترنت للمساعدة على تنسيق خطة الإجراءات الأمنية وتلبية متطلبات الالتزام. يستعرض هذا التقرير التفصيلي الخطوات المقترحة لكل من الإجراءات الـعشرين للمساعدة على تأمين أجهزة الطباعة والبيانات والمستندات كجزء من خطة الأمان الشاملة. تتناول الضوابط رقم 4 و6 و8 و12 و13 و15 خصيصًا أنشطة حماية البيانات ومراقبتها فيما يتعلق بمتطلبات GDPR الجديدة.

الإجراءات الأمنية الرئيسية لمركز أمن الإنترنت والتوصيات

الإجراء الأمني الأول: إجراء جرد للأجهزة المعتمدة وغير المعتمدة

الإجراء – الإدارة الفعّالة (جرد وتتبع وتصحيح) لجميع الأجهزة الموجودة على الشبكة بحيث يقتصر إعطاء إمكانية الوصول على الأجهزة المعتمدة فقط، وتحديد الأجهزة غير المعتمدة وغير الخاضعة للإدارة ومنعها من الوصول.

التوصية – التحقق من أن جميع أجهزة الطباعة المتصلة بالشبكة مُسجلة بأسماء مستخدمين ومُدارة بشكلٍ فعالٍ لضمان الامتثال لسياسة الأمن المتبعة في الشركة. تستطيع الأداة الفعالة لإدارة أمان الطباعة اكتشاف وتقديم الرؤية للشبكة بالكامل وجميع الكمبيوترات المتصلة بها.

الإجراء الأمني الثاني: إجراء جرد للبرامج المعتمدة وغير المعتمدة

الإجراء – الإدارة الفعّالة (جرد وتتبع وتصحيح) لجميع البرامج الموجودة على الشبكة بحيث يقتصر تثبيت البرامج على تلك البرامج المعتمدة فقط، وتحديد البرامج غير المعتمدة وغير المُدارة ومنعها من التثبيت أو التركيب على الأجهزة.

التوصية – التأكد من أن جميع البرامج الثابتة والحلول المُحمّلة على أجهزة الطباعة والتصوير مُحدّثة وموقّعة وتم التحقق من أنها أصلية. اختيار أجهزة طباعة تحتوي على حماية مُدمجة لنظام الإدخال والإخراج الأساسي "BIOS" للتأكد من تحميل الكود الأصلي فقط. يُمكن تثبيت تحديثات البرامج الثابتة كإجراء استباقي على جميع أجهزة الأسطول من خلال حلول إدارة أسطول الطباعة. يجب التحقق من أصالة البرامج (الموجودة على الخادم والموجودة لدى الجهاز العميل).

الإجراء الأمني الثالث: تأمين إعدادات الأجهزة والبرامج على الأجهزة المتنقلة والكمبيوترات المحمولة ومحطات العمل والخوادم

الإجراء – إنشاء وتطبيق وإدارة (تتبع وإبلاغ وتصحيح) إعدادات الأمان بفعالية على الكمبيوترات المحمولة والخوادم ومحطات العمل باستخدام عملية صارمة لإدارة الإعدادات وعملية التحكم في التغيير من أجل منع المهاجمين من استغلال الخدمات والإعدادات الضعيفة في الأجهزة.

التوصية – ينبغي ضبط إعدادات الطابعات بأمان شأنها في ذلك شأن جميع الأجهزة الأخرى المتصلة بالشبكة. ينبغي استخدام ونشر سياسة أمن محددة في جميع أجهزة الطباعة والتعامل بفعالية وحزم مع أي انحرافات تحيد عن هذه السياسة. قد تُساعد قوائم فحص الأمان (مثل NIST) أو خدمات الاستشارات الأمنية على تصميم ونشر سياسة أمان طباعة شاملة. وقد تُسهم أداة فعالة لإدارة أمان الطباعة في أتمتة إنشاء السياسة ونشرها وتقييمها وتصحيح إعدادات الأجهزة في جميع الأجهزة المتصلة بأسطول الطباعة. تحتوي الطابعات متعددة المهام الخاصة بالشركات على أكثر من 250 إعدادًا أمنيًا، وبالتالي فإن أتمتة هذه العملية سيوفر وقتًا طويلًا.

الإجراء الأمني الرابع: التقييم والمعالجة المستمرة لنقاط الضعف

الإجراء – الاستمرار في تقييم الإجراءات واتخاذها بشأن المعلومات الجديدة من أجل تحديد نقاط الضعف والتعامل مع فرص اختراق المهاجمين والحد منها.

التوصية – تستطيع حلول معلومات الأمان وإدارة الأحداث (SIEM) مثل ArcSight أو Splunk أو SIEMonster مراقبة الأنشطة الجارية على الشبكة في الحال وإبلاغ المسؤولين في حال وقوع أي حادث. فهذه المسألة مهمة للغاية لمراقبة أجهزة الطباعة تمامًا مثل أجهزة الكمبيوتر، بالإضافة للتأكد من قدرة طابعاتك على إرسال رسائل سجل النظام إلى أداة معلومات الأمان وإدارة الأحداث.

اختيار أجهزة الطباعة المزوّدة بمزايا يُمكنها اكتشاف الهجمات في الحال والاستعادة بشكل تلقائي، لزيادة وقت تشغيل الأجهزة وتقليل تدخلات فريق تكنولوجيا المعلومات من أجل إجراء الإصلاحات اللازمة.

ومن أجل الحد من نقاط الضعف، يُوصى باستخدام أداة إدارة أمن الأسطول التي تستطيع التعرّف على الطابعات الجديدة وتطبيق إعدادات سياسة الأمن الخاصة بالشركة تلقائيًا بمجرد توصيل الأجهزة بالشبكة. إجراء تقييمات وإصلاحات دورية لضمان استمرارية امتثال أسطول الطباعة بأكمله بالسياسة.

الإجراء الأمني الخامس: الاستخدام المُحكم للمزايا الإدارية

الإجراء – تتبع ومراقبة ومنع وتصحيح استخدام وتخصيص وتهيئة المزايا الإدارية على أجهزة الكمبيوتر والشبكات والتطبيقات.

التوصية – اختيار أجهزة وحلول الطباعة ذات القدرة على مصادقة المستخدمين والتحكم في إمكانية الوصول للوظائف بناءً على دور الشخص ومهامه، بحيث لا يستطيع أحد سوى فريق تكنولوجيا المعلومات أو الموظفين المعتمدين الآخرين ضبط إعدادات الجهاز وتهيئتها. استخدام برامج إدارة أمن الأسطول لنشر كلمات المرور الخاصة بالمسؤولين عبر الأسطول.

الإجراء الأمني السادس: صيانة سجلات التدقيق ومراقبتها وتحليلها

الإجراء – جمع سجلات تدقيق الأحداث وإدارتها وتحليلها والتي من شأنها المساعدة على اكتشاف الهجوم وفهمه والتعامل معه.

التوصية – ينبغي أن يكون لدى أجهزة الطباعة القدرة على إنشاء رسائل الأحداث الخاصة بسجل النظام، بحيث يستطيع فريق الأمن مراجعة سجلات التدقيق بشكل دوري لاكتشاف المشاكل وحلها. اختيار الأجهزة التي يُمكنها إرسال هذه الرسائل إلى حلول إدارة أمن الأسطول وأدوات أمان المعلومات وإدارة الأحداث لكل من المراقبة الفورية والقدرة على إنشاء التقارير من أجل عمليات التدقيق أو متطلبات الامتثال الأخرى.

الإجراء الأمني السابع: وسائل حماية البريد الإلكتروني ومتصفّح مواقع الإنترنت

الإجراء – الحد من احتمالات الهجوم وتقليل الفرص المتاحة أمام المخترقين للتلاعب، مُستغلين استخدام العاملين لمتصفحات الويب وأنظمة البريد الإلكتروني.

التوصية – عادةً ما تكون الطابعات متعددة المهام متصلة بالإنترنت، وبالتالي يُمكنها إرسال الصفحات التي يتم مسحها ضوئيًا عبر البريد الإلكتروني. التحقق من تشفير البيانات الممسوحة ضوئيًا والمرسلة عبر البريد الإلكتروني من أجل حماية البيانات الحساسة. استخدام الأجهزة والحلول التي تستطيع مصادقة المستخدمين مع إمكانيات التحكم في الوصول إلى الموارد داخل الجهاز (مثل خوادم الويب أو وظائف البريد الإلكتروني) بناءً على دور الشخص المعني. إنشاء قائمة تضم "المواقع الموثوقة" للطابعات متعددة المهام وإدارة هذه القائمة بشكل مناسب لضمان أن المواقع الموثوقة فقط هي التي يُمكن الوصول إليها من الجهاز. دمج العديد من وسائل المصادقة (مثل PIN/PIC أو LDAP أو Kerberos للمصادقة) في Active Directory من أجل تيسير الإدارة وزيادة الأمن. ينبغي أن تحتوي أجهزة الطباعة المتصلة بالشبكة على حماية مدمجة من البرامج الخبيثة والفيروسات، كما ينبغي تحديث البرامج الثابتة بصورة دورية لضمان استخدام أحدث إصدار من الحماية على الجهاز.

الإجراء الأمني الثامن: الحماية من البرامج الخبيثة

الإجراء – السيطرة على تثبيت الكود الخبيث ونشره وتركيبه في عدة نقاط في المؤسسة، بالإضافة إلى تحسين استخدام الأتمتة لتمكين التحديث السريع للإجراءات الدفاعية والتصحيحية وجمع المعلومات.

التوصية – اختيار أجهزة الطباعة التي لا تُحمّل سوى الأكواد المحققة والموقّعة والتي تحتوي على مزايا مدمجة لمكافحة البرامج الخبيثة من أجل مراقبة ذاكرة الجهاز بفعالية وإعادة التشغيل في حال تعرّض الجهاز للهجوم. وقد تُسهم أداة فعالة لإدارة أمان الطباعة في تقييم إعدادات الجهاز وتصحيحها تلقائيًا في جميع الأجهزة المتصلة بأسطول الطباعة. كما يتعين التأكّد من أن جميع حلول برامج الطباعة موقّعة ومعتمدة وأصلية.

الإجراء الأمني التاسع: تقييد منافذ الشبكة والبروتوكولات والخدمات والتحكم بها

الإجراء – إدارة (تتبع وتحكّم وتصحيح) الاستخدام التشغيلي المُستمر للمنافذ والبروتوكولات والخدمات الموجودة على أجهزة الشبكة من أجل الحد من نوافذ نقاط الضعف التي يُمكن أن يستغلها المخترقون.

التوصية – إذا لم تكن النوافذ غير المستخدمة والبروتوكولات غير المُؤمّنة (مثل FTP أو Telnet) مُعطّلة بالفعل، فيجب تعطيلها، فقد يستخدمها المخترقون للوصول إلى الجهاز. توفير وقت فريق تكنولوجيا المعلومات من خلال استخدام أداة إدارة أمان الطباعة لإبقاء إعدادات الجهاز متوافقة بشكل تلقائي في جميع أجهزة الأسطول. استخدام كلمات مرور المسؤولين والمصادقة وإجراءات الوصول بحسب الدور للحد من الوصول إلى وظائف الجهاز وإعداداته.

الإجراء الأمني العاشر: إمكانية استعادة البيانات

الإجراء – إنشاء نُسخة احتياطية من المعلومات المهمة بالشكل المناسب مع وجود آلية ثابتة للاستعادة في الوقت السليم.

التوصية – لا ينطبق الإجراء الأمني هذا على الطابعات في الوقت الحالي.

الإجراء الأمني الحادي عشر: تأمين التهيئات والإعدادات للأجهزة المتصلة بالشبكة مثل جدران الحماية وأجهزة التوجيه (الراوتر) والمحولات

الإجراء – إنشاء وتطبيق وإدارة (تتبع وإبلاغ وتصحيح) إعدادات الأمان بفعالية على أجهزة البنية التحتية للشبكة باستخدام عملية صارمة لإدارة الإعدادات وعملية التحكم في التغيير من أجل منع المهاجمين من استغلال الخدمات والإعدادات الضعيفة في الأجهزة.

التوصية – ينبغي الاعتناء بضبط إعدادات الطابعات المتصلة بالشبكات شأنها في ذلك شأن جميع الأجهزة الأخرى المتصلة بالشبكة. وقد تُسهم أداة فعالة لإدارة أمان الطباعة في أتمتة نشر السياسة وتقييمها وتصحيح إعدادات الأجهزة في جميع الأجهزة المتصلة بأسطول الطباعة للمساعدة على إبقاء الشبكة آمنة، مع توفير وقت فريق تكنولوجيا المعلومات.

الإجراء الأمني الثاني عشر: حماية الحدود

الإجراء – اكتشاف ومنع وتصحيح تدفق المعلومات المنقولة عبر الشبكات ذات مستويات الثقة المتفاوتة مع التركيز على البيانات المُدمرة للأمن.

التوصية – استخدام التشفير لحماية البيانات المنقولة (مهام الطباعة أو المسح الضوئي المنقولة من الطابعة أو إليها) والمخزّنة على القرص الصلب بالجهاز. اختيار أجهزة وحلول الطباعة ذات القدرة على مصادقة المستخدمين والتحكم في الوصول إلى الوظائف بحسب دور الشخص، على سبيل المثال، لا يستطيع أحد سوى المستخدمين المصادقين والمعتمدين فقط إرسال مهام مسح ضوئي عبر البريد الإلكتروني أو إرسال ملفات إلى الشبكات السحابية. تسجيل مواقع الويب الموثوقة في قائمة "المواقع الموثوقة" على الجهاز لمنع الوصول إلى المواقع الخبيثة والضارة. تستطيع حلول الطباعة المتنقلة الآمنة تسهيل الأمور على المستخدمين بحيث يُمكنهم الطباعة من أجهزتهم المتنقلة أثناء حماية الشبكة.

الإجراء الأمني الثالث عشر: حماية البيانات

الإجراء – منع استخلاص البيانات وتخفيف آثار البيانات المُستخلصة والتحقق من الخصوصية وسلامة المعلومات الحساسة.

التوصية – استخدام التشفير لحماية البيانات المنقولة (مهام الطباعة أو المسح الضوئي المنقولة من الطابعة أو إليها) والمخزّنة على القرص الصلب بالجهاز. استخدام جميع حلول الطباعة بطريقة السحب من أجل تلافي ترك المستندات الحساسة في أدراج الورق المطبوع. التأكد أن البيانات المُخزّنة على الأقراص الصلبة للأجهزة قد تم إزالتها بأمان قبل إعادة الأجهزة المُستأجرة أو إعادة تدويرها عند انتهاء استخدامها.

الإجراء الأمني الرابع عشر: الوصول الخاضع للتحكّم بحسب الحاجة للمعرفة

الإجراء – تنفيذ عمليات التتبّع والمنع والتصحيح وتأمين الوصول إلى الأصول المهمة (مثل المعلومات والموارد والأنظمة) وفقًا للتحديد الرسمي للأشخاص وأجهزة الكمبيوتر والتطبيقات التي تحتاج ويحق لها الوصول إلى هذه الأصول المهمة بناءً على تصنيف مُعتمد.

التوصية – اختيار أجهزة وحلول الطباعة ذات القدرة على مصادقة المستخدمين والتحكم في إمكانية الوصول للوظائف بناءً على دور الشخص. دمج العديد من وسائل المصادقة (مثل PIN/PIC أو LDAP أو Kerberos للمصادقة) في Active Directory من أجل تيسير الإدارة وزيادة الأمن. قد تُسهم حلول الطباعة بطريقة السحب في حماية المستندات الحساسة من الوقوع في الأيدي الخاطئة.

الإجراء الأمني الخامس عشر: التحكم في الدخول إلى الشبكات اللاسلكية

الإجراء –التتبع والتحكّم والمنع والتصحيح للاستخدام الآمن لشبكات المنطقة المحلية اللاسلكية ونقاط الوصول وأنظمة العميل اللاسلكية.

التوصية – وقد تُسهم أداة فعّالة لإدارة أمان الطباعة في أتمتة نشر إعدادات الأجهزة وتقييمها وتصحيحها بما في ذلك الإعدادات اللاسلكية في جميع الأجهزة المتصلة بالأسطول. استخدام حلول التحكّم في الوصول للحد من إمكانية الوصول إلى وظائف الجهاز مثل المسح الضوئي إلى البريد الإلكتروني بناءً على دور المستخدم. تستطيع حلول الطباعة المتنقلة الآمنة تسهيل الأمور على المستخدمين بحيث يُمكنهم الطباعة من أجهزتهم المتنقلة أثناء حماية الشبكة. على سبيل المثال، تقوم الأجهزة التي تدعم الطباعة اللاسلكية بطريقة النظير إلى النظير بالسماح لمستخدمي الجهاز المتنقل بطباعة مباشرةً إلى إشارة لاسلكية مميزة من الطابعة، من دون الوصول إلى شبكة الشركة أو الخدمة اللاسلكية.

الإجراء الأمني السادس عشر: مراقبة الحساب والتحكّم به

الإجراء – الإدارة الفعالة لنظام دورة حياة حسابات الأنظمة والتطبيقات والتي تشمل إنشاءها واستخدامها وإدخالها في وضع السكون وحذفها، من أجل تقليل فرص استغلال المخترقين لها.

التوصية – اختيار أجهزة وحلول الطباعة ذات القدرة على مصادقة المستخدمين والتحكم في إمكانية الوصول للوظائف بناءً على دور الشخص. دمج المصادقة مع Active Directory من أجل الإدارة المركزية وزيادة الأمان. مراجعة حسابات المستخدمين بشكلٍ دوري وتعطيل الحسابات غير الضرورية واستخدام حلول التتبع لمراقبة استخدام الحساب. تشفير أسماء مستخدمي الحسابات وبياناتٍ المصادقة، سواء أثناء التنقل أو تخزينها على الجهاز. يستطيع مستشارو الأمان مساعدتك على وضع خطة شاملة لأمان الطباعة للمساعدة على تقليل المخاطر، ليس هذا فحسب، بل إنهم يستطيعون إدارة الأمن بما في ذلك مراقبة الحسابات والتحكم بها.

الإجراء الأمني السادس عشر: تقييم المهارات الأمنية وتقديم التدريب المناسب لسد الفجوات

الإجراء – الوقوف على المعرفة والمهارات والقدرات المحددة اللازمة لدعم حماية المؤسسة؛ وضع وتنفيذ خطة مُتكاملة الأركان لتقييم الفجوات وتحديدها والتعامل معها من خلال برامج السياسة والتخطيط التنظيمي والتدريبية والتثقيفية لجميع الأدوار الوظيفية في المؤسسة.

التوصية – امتلاك مستشاري أمان الطباعة المعرفة المُتخصصة لمساعدتك على تقييم المخاطر الأمنية ووضع سياسة أمان شاملة ووضع خطة شاملة وتنفيذ الحلول والتوصيات التكنولوجية. كما تستطيع بعض خدمات الأمان أيضًا إدارة الالتزام بأمان الطباعة نيابةً عنك.

الإجراء الأمني الثامن عشر: أمن البرامج والتطبيقات

الإجراء – إدارة دورة حياة الأمن لجميع البرامج الداخلية المُطورة المُشتراة من أجل منع نقاط الضعف الخاصة بالأمان واكتشافها وتصحيحها.

التوصية – الالتزام بتطوير أفضل الممارسات لجميع حلول الطباعة. اختيار الحلول البرمجية التي تم توقيعها ومصادقتها واعتبارها أصلية.

الإجراء الأمني التاسع عشر: الاستجابة للحوادث وإدارتها

الإجراء الأمني – حماية معلومات المؤسسة وسمعتها من خلال تطوير وتفعيل بنية تحتية للاستجابة للحوادث (مثل، مراقبة الخطط والأدوار المحددة والتدريب والاتصالات والإدارة المُحكمة)

التوصية – التأكد من اشتمال خطة الاستجابة للحوادث على بيئة الطباعة.

الإجراء الأمني العشرين: اختبارات الاختراق وتمارين الفريق الأحمر (المعني بالارتقاء بكفاءة المؤسسة)

الإجراء - اختبار القوة الكُلية لدفاعات المؤسسة (التكنولوجيا والعمليات والموظفين) من خلال محاكاة أهداف المخترِق وأعماله.

التوصية – إدخال بيئة الطباعة عند إجراء اختبارات الاختراق. تقييم بيئة الطباعة بشكل دوري لمعرفة ما إذا كان بها نقاط ضعف وتحديث خطة الأمن بحيث تُعالج تلك النقاط.

بادر باتخاذ الخطوة التالية

إن الأخذ بالتوصيات المذكورة في هذا التقرير التفصيلي يُساعدك على تعزيز أمان الطباعة لديك وتلبية متطلبات الامتثال. هل تحتاج لمساعدة؟ تستطيع خدمات إدارة أمان الطباعة والخدمات الاستشارية مساعدتك على وضع خطة واستخدام العمليات والتكنولوجيا لتعزيز أمان أجهزة الطباعة والبيانات والمستندات.

الملحق أ: مزايا وحلول وخدمات أمان الطباعة من HP

تُساعدك مزايا الأمان المُدمجة في أجهزة HP بالإضافة إلى حلول وخدمات البرامج الرائدة في هذا المجال على تلبية شروط الامتثال التنظيمية والقانونية وحماية معلوماتك التجارية من التهديدات الأمنية.

تعمل مزايا الأمان المدمجة في طابعات HP العادية والطابعات متعددة الوظائف للشركات على الحماية من البرامج الخبيثة وتستطيع اكتشاف الهجوم والتعامل معه تلقائيًا. تتفرّد مزايا أمان الطباعة لدى HP بتقديم اكتشاف فوري للهجمات ومراقبة أوتوماتيكية وتحقق من البرامج الثابتة المدمجة للتصدي لأي تهديدات بمجرد ظهورها[4]. تُساعد على تلبية مُتطلبات الإجراء الثاني والرابع والسادس والثامن.) hp.com/go/PrintersThatProtect

توفر حلول **HP Access Control** مجموعة مُتنوعة من إجراءات المصادقة والوصول بحسب الأدوار للمساعدة على تقليل الانتهاكات الأمنية المحتملة، بالإضافة إلى تتبع المهام وتحمّل المسؤولية. (تُساعد على تلبية الإجراء الخامس والسابع والعاشر والثاني عشر والثالث عشر والرابع عشر والخامس عشر والسادس عشر) hp.com/go/hpac

تُسهم حلول التشفير وHP JetAdvantage Workflow في حماية البيانات سواء عند تخزينها على أجهزة HP Enterprise وأثناء نقلها من أجهزة الطباعة وإليها أو على السحابة. (تُساعد على تلبية الإجراءيْن الثاني عشر والثالث عشر.) hp.com/go/upd, hp.com/go/documentmanagement

تعمل حلول HP للطباعة بطريقة السحب على حماية المستندات السرية من خلال تخزين وظائف الطباعة على خادم محمي أو في الشبكة السحابية أو على الكمبيوتر المكتبي. يقوم المستخدمون بالمصادقة في مكان الطباعة المختار لسحب مهامهم وطباعتها. (تُساعد على تلبية متطلبات الإجراءين الثالث عشر والرابع عشر.) hp.com/go/hpac، hp.com/go/JetAdvantageSecurePrint

تقوم **HP JetAdvantage Connect** بإعطاء مستخدمي الأجهزة المتنقلة إمكانية وصول للطباعة من الهواتف الذكية والأجهزة اللوحية مع الاحتفاظ بالأمان والتحكّم الإداري الذي تُريده. (تُساعد على تلبية متطلبات الإجراءين الثاني عشر والخامس عشر.) hp.com/go/JetAdvantageConnect

يُمكن إرسال بيانات الأحداث الخاصة بالطابعة إلى أدوات SIEM مثل ArcSight أو Splunk أو SIEMonster. يستطيع فريق الأمان مشاهدة النقاط المُتصلة بالطابعة بسهولة وذلك كجزء من النظام البيئي الأشمل لتكنولوجيا المعلومات ويُمكن اتخاذ إجراءات تصحيحية. (تُساعد على تلبية متطلبات الإجراءين الرابع والسادس.)

يُعتبر HP JetAdvantage Security Manager الأداة الوحيدة للامتثال لأمان الطباعة القائم على سياسة محددة،[5] حيث يُساعد على وضع سياسة أمنية لجميع الأجهزة في الأسطول التقني، وأتمتة تصحيح إعدادات الجهاز تلقائيًا، وتثبيت وتجديد الشهادات الفريدة بالإضافة للحصول على التقارير اللازمة للتحقّق من الامتثال. تعمل ميزة Security-Instant on تلقائيًا على تهيئة الأجهزة الجديدة عند إضافتها إلى الشبكة أو بعد إعادة التشغيل. (تُساعد على تلبية متطلبات الإجراء الأول والثاني والثالث والرابع والخامس والسادس والثامن والتاسع والحادي عشر والخامس عشر.) hp.com/go/securitymanager

توفّر خدمات الطباعة المدارة الآمنة من HP أقوى وأشمل حماية في مجال أمان الطباعة على الإطلاق.[6] قد يكون أمان الطباعة مسألة معقّدة. دع HP تُدير أمان الطباعة بدءًا من تهيئة الأجهزة إلى حلول الأمن المُتقدمة التي تتعامل مع متطلبات الأشخاص والعمليات والامتثال. (تُساعد على تلبية متطلبات الإجراء الثاني والثالث والثاني عشر والسادس عشر والسابع عشر والثامن عشر والتاسع عشر) hp.com/go/SecureMPS

توفّر **HP Print Security Professional Services** خُبراء الأمان لمساعدتك على تقييم بيئة الطباعة لديك، ووضع سياسات الأمان مقدمًا وتحديث الأمان لديك أولًا بأول. كما يُمكننا أيضًا إدارة الالتزام بأمان الطباعة نيابةً عنك. (تُساعد على تلبية متطلبات الإجراء الثاني والثالث والثاني عشر والسادس عشر والسابع عشر والتاسع عشر) hp.com/go/SecureMPS

ملاحظات

[1] دراسة معهد بونيمون برعاية HPE "تكلفة عام 2016 لدراسة الجرائم الإلكترونية ومخاطر الابتكارات في مجال الأعمال"، عام 2016.

[2] تقرير The 2016 Year End Data Breach QuickView الذي أعدته RiskBased Security يناير عام 2017.

[3] تعرّض 26.2% من المشاركين في أحد الاستبيانات لانتهاك أمني تقني خطير اقتضى اتخاذ إجراء لمعالجته، كما أن أكثر من 26.1% من هذه الحوادث اشتملت على الطباعة. شركة البيانات الدولية: "استبيان 2015 لتكنولوجيا المعلومات وأمان الطباعة، شركة البيانات الدولية رقم US40612015، سبتمبر 2015.

[4] يسري على أجهزة HP من فئة الشركات والمطروحة في بداية 2015 وبناءً على مراجعة HP لمزايا الأمان المنشورة والمدمجة في الطابعات المنافسة من نفس الفئة لسنة 2016. تتفرّد HP دون غيرها بتقديم مجموعة متنوّعة من المزايا الأمنية لفحص سلامة الأجهزة وصولًا إلى نظام الإدخال والإخراج الأساسي (BIOS) مع إمكانيات المعالجة الذاتية. قد يُطلب تحديث باقة خدمات FutureSmart لتفعيل المزايا الأمنية. للاطلاع على قائمة المنتجات المتوافقة، انظر hp.com/go/PrintersThatProtect. لمزيد من المعلومات، يُرجى زيارة hp.com/go/printersecurityclaims.

[5] يجب شراء HP JetAdvantage Security Manager بشكل منفصل. لمعرفة المزيد، تفضّل بزيارة hp.com/go/securitymanager. الحساب التنافسي بناءً على أبحاث HP الداخلية بشأن عروض المنافسين (مقارنة أمان الأجهزة، يناير 2015) وتقرير الحلول على HP JetAdvantage Security Manager 2.1 من شركة Buyers Laboratory LLC، فبراير 2015.

[6] تشمل الجهاز والبيانات وقدرات تأمين المستندات من خلال رواد مقدمي خدمات الطباعة المدارة. بناءً على مراجعة HP للمعلومات المتاحة لعموم الجمهور من عامي 2015-2016 والخاصة بخدمات الأمان وبرامج الأمن والإدارة ومزايا الأمان المدمجة في الجهاز للطابعات المنافسة من الفئة ذاتها. لمزيدٍ من المعلومات، يُرجى زيارة hp.com/go/MPSsecurityclaims أو hp.com/go/mps.

اشترك للحصول على الأخبار الجديدة
hp.com/go/getupdated

المشاركة مع الزملاء

4AA6-8821ARE، يونيو 2017، المراجعة 1