Technisches Whitepaper

Erfüllen Sie Compliance-Anforderungen für die Netzwerk- und Datensicherheit

Empfehlungen für die Anwendung von Sicherheitsmechanismen für die Druckerflotte

Inhalt

Compliance-Verstöße können Ihrem Unternehmen schaden

Abgesehen von hohen Geldstrafen und Rechtsstreitigkeiten kann eine Sicherheitslücke auch Umsatzeinbußen und Imageschäden zur Folge haben. Wenn Sie Ihren Sicherheitsplan entwickeln, sollten Sie beachten, dass jedes Netzwerk nur so sicher ist wie das schwächste Glied in der Kette. Druck- und Bildverarbeitungsgeräte können häufig dieselben Sicherheitsschwachstellen aufweisen wie PCs. Es ist wichtig, Geräte und Lösungen bereitzustellen, die Ihnen helfen, Compliance-Anforderungen zu erfüllen und Ihre Geschäftsinformationen vor Sicherheitsbedrohungen zu schützen.

Welchen Risiken ist Ihr Unternehmen ausgesetzt?

Verstöße gegen Vorschriften und gesetzliche Bestimmungen verursachen in global agierenden Unternehmen hohe Kosten, die z. B. durch Strafen, entgangene Umsätze, Imageverlust und Rechtsstreitigkeiten entstehen.

Nicht oder nur unzureichend geschützte Endgeräte bilden zusätzliche Einfallstore für Cyberkriminelle. Die im Rahmen einer kürzlich von Ponemon durchgeführten Studie befragten Organisationen hatten 2016 durchschnittlich zwei Angriffe pro Woche zu verzeichnen. Das ist ein Anstieg von 23 % gegenüber dem Vorjahr und bedeutet einen durchschnittlichen Verlust von 9,5 Millionen US-Dollar jährlich im Kampf gegen Cyberkriminalität.[1] Allein letztes Jahr sind weltweit über 4 Milliarden Datensätze in die Hände von Hackern gefallen, was einem Anstieg von 400 % im Vergleich zu den vergangenen zwei Jahren entspricht.[2]

Auch wenn viele IT-Abteilungen mittlerweile strenge Sicherheitsmaßnahmen durchgesetzt haben, um Computer und das Netzwerk zu schützen, fallen die Druck- und Bildverarbeitungsgeräte oft durch das Raster. Aber Drucker können zu Einfallstoren für Angriffe auf Ihr Netzwerk werden, daher sollte ihr Schutz keinesfalls vernachlässigt werden. 26 % aller von IT-Managern gemeldeten schwerwiegenden Verstöße gegen die Datensicherheit sind auf Schwachstellen bei Druckern zurückzuführen.[3]

Um der wachsenden Bedrohung zu begegnen, implementieren Regierungsbehörden auf der ganzen Welt strenge neue Sicherheitsvorschriften, die Organisationen dazu zwingen, Kundeninformationen besser zu schützen. Die neue Datenschutz-Grundverordnung (DSGVO) der EU ist beispielsweise ein zentrale Verordnung, die 2018 in Kraft tritt. Die DSGVO erhöht die an Unternehmen gestellten Anforderungen im Bereich Datenschutz. Daher sollten Sie unbedingt sicherstellen, dass alle in Ihrem Netzwerk befindlichen Geräte – von PCs über Drucker bis zu mobilen Geräten – geschützt sind. Von der neuen Verordnung sind nicht nur EU-Länder betroffen. Auch globale Unternehmen müssen die Vorschriften einhalten, wenn sie Daten von EU-Bürgern erfassen und verwenden. Organisationen müssen jedes einzelne Gerät überwachen und bewerten, um Sicherheitsverletzungen erkennen und innerhalb von 72 Stunden nach Kenntnisnahme melden zu können. Wenn bei Compliance-Audits nicht überwachte oder nicht gemeldete Verstöße offengelegt werden, drohen den betroffenen Unternehmen Bußgelder in Höhe von bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes.

Setzen Sie allgemeine Sicherheitsmaßnahmen zur Verbesserung der Compliance um

Es ist nicht einfach, branchenspezifische Compliance-Anforderungen und Vorschriften zu erfüllen. Doch das Center for Internet Security (CIS) hat eine Reihe allgemeiner Sicherheitsmaßnahmen entwickelt, die die Umsetzung der Empfehlungen für Cybersicherheit erleichtern. Bei den CIS Critical Security Controls handelt es sich um 20 spezifische Maßnahmen zur Abwehr von Cyberangriffen. (Weitere Informationen finden Sie unter https://www.cisecurity.org/critical-controls.cfm.) Die Sicherheitsmaßnahmen sind auf zahlreiche andere branchenspezifische Vorschriften wie PCI-DSS, ISO 27001, US CERT-Empfehlungen, HIPAA, FFIEC und NIST abgestimmt. Sie sind nicht dafür vorgesehen, diese oder andere Sicherheitsframeworks zu ersetzen, werden jedoch häufig von Unternehmen genutzt, um die Richtlinien anderer Frameworks sinnvoll umzusetzen.

Die CIS Critical Security Controls legen den Schwerpunkt auf eine übersichtliche Anzahl von äußerst effektiven Sicherheitsmaßnahmen. Sie zielen auf die am häufigsten auftretenden Angriffsmuster ab, die in maßgeblichen Studien zu Bedrohungen beschrieben werden. Zahlreiche Branchenexperten, darunter Top-Organisationen aus den Bereichen IT-Forensik und Vorfallsreaktion, haben an der Entwicklung dieser Maßnahmen mitgewirkt. Darüber hinaus werden die Maßnahmen fortlaufend im Hinblick auf neu entstehende Bedrohungen und Angriffe aktualisiert.

Nutzen Sie die CIS Critical Security Controls, um Ihr Sicherheitskonzept zu strukturieren und Compliance-Richtlinien einzuhalten. In diesem Whitepaper werden Aktionen zur Umsetzung der 20 Maßnahmen vorgeschlagen, um zum Schutz Ihrer Druckgeräte, Daten und Dokumente im Rahmen Ihres umfassenderen Sicherheitsplans beizutragen. Die Sicherheitskontrollen 4, 6, 8, 12, 13 und 15 befassen sich speziell mit Datenschutzmaßnahmen und Überwachungsaktivitäten in Bezug auf die neuen DSGVO-Anforderungen.

CIS Critical Security Controls und empfohlene Maßnahmen

CSC 1: Inventarisierung der genehmigten und nicht genehmigten Hardware

Maßnahme – Aktives Verwalten (Inventarisieren, Nachverfolgen und Korrigieren) aller Geräte im Netzwerk, sodass nur autorisierte Geräte Zugriff darauf erhalten und nicht autorisierte bzw. nicht verwaltete Geräte erkannt und am Zugriff gehindert werden

Empfehlung – Stellen Sie sicher, dass alle Druckgeräte im Netzwerk berücksichtigt und aktiv verwaltet werden, um die Einhaltung Ihrer Sicherheitsrichtlinie zu gewährleisten. Ein effektives Tool für die Verwaltung der Drucksicherheit ermöglicht die Erkennung von Geräten und sorgt für Transparenz im Hinblick auf alle vernetzten Geräte und Geräte mit PC-Verbindung.

CSC 2: Inventarisierung der genehmigten und nicht genehmigten Software

Maßnahme – Aktives Verwalten (Inventarisieren, Nachverfolgen und Korrigieren) aller Softwareprogramme im Netzwerk, sodass nur autorisierte Software installiert ist und ausgeführt wird und nicht autorisierte bzw. nicht verwaltete Software gefunden wird, um ihre Installation oder Ausführung zu unterbinden

Empfehlung – Stellen Sie sicher, dass sämtliche auf Druck- und Bildverarbeitungsgeräten installierte Firmwareprogramme und Lösungen auf dem neuesten Stand, signiert und gültig sind. Wählen Sie Druckgeräte mit integriertem BIOS- und Firmware-Schutz, um sicherzustellen, dass nur authentischer Code geladen wird. Mithilfe von Flottenverwaltungslösungen lassen sich proaktive Firmware-Updates per Push auf die Geräte der Druckerflotte übertragen. Software (serverbasiert und clientbasiert) sollte signiert und als authentisch validiert worden sein.

CSC 3: Sichere Hardware- und Softwarekonfigurationen für alle mobilen Endgeräte, Laptops, Workstations und Server

Maßnahme – Festlegen, Implementieren und aktives Verwalten (Nachverfolgen, Erfassen in Berichten und Korrigieren) der Sicherheitskonfiguration von Laptops, Servern und Workstations durch konsequentes Konfigurationsmanagement und ein strenges Änderungsüberwachungsverfahren, um zu verhindern, dass Angreifer Dienste und Einstellungen manipulieren

Empfehlung – Drucker sollten wie andere Netzwerkendpunkte auch eine sichere Konfiguration aufweisen. Sie sollten übergreifend für alle Druckgeräte eine Sicherheitsrichtlinie festlegen und implementieren und aktiv jegliche Abweichungen korrigieren. Sicherheitschecklisten (wie NIST) oder Sicherheitsberatungsservices können Ihnen beim Entwickeln und Implementieren einer umfassenden Richtlinie für die Drucksicherheit helfen. Ein effektives Verwaltungstool für die Drucksicherheit kann die Richtlinienerstellung, -implementierung und -bewertung sowie die Korrektur von Geräteeinstellungen für die gesamte Druckerflotte automatisieren. Multifunktionsgeräte (MFPs) der Enterprise-Klasse verfügen über mehr als 250 Sicherheitseinstellungen, sodass sich durch die Automatisierung erhebliche Zeiteinsparungen erzielen lassen.

CSC 4: Kontinuierliche Schwachstellenbewertung und -behebung

Maßnahme – Kontinuierliches Abrufen, Bewerten und Heranziehen von Informationen, um Schwachstellen zu identifizieren und auf diese Weise so wenig Angriffsfläche wie möglich zu bieten

Empfehlung – Lösungen für Sicherheitsinformationen und Ereignismanagement (Security Information and Event Management, SIEM) wie ArcSight, Splunk oder SIEMonster können die Aktivitäten in Ihrem Netzwerk in Echtzeit überwachen und Administratoren über Vorfälle informieren. Die Überwachung Ihrer Druckgeräte ist ebenso wichtig wie die Überwachung von PCs. Daher sollten Sie sicherstellen, dass Ihre Drucker Systemprotokollmeldungen zu Ereignissen an Ihr SIEM-Tool übermitteln können.

Wählen Sie Druckgeräte mit Funktionen zur Angriffserkennung in Echtzeit und automatischen Wiederherstellung, um die Betriebszeit zu optimieren und den Wartungsaufwand zu verringern.

Verwenden Sie ein Verwaltungstool für die Flottensicherheit, das neue Drucker erkennt und sie automatisch mit den Sicherheitseinstellungen entsprechend den Richtlinien Ihres Unternehmens konfiguriert, sobald sie mit dem Netzwerk verbunden werden, um die Anzahl der Schwachstellen zu verringern. Planen Sie regelmäßige Bewertungen/Überarbeitungen, um zu gewährleisten, dass Ihre gesamte Druckerflotte richtlinienkonform ist.

CSC 5: Kontrollierte Nutzung von Administratorrechten

Maßnahme – Nachverfolgen, Kontrollieren, Verhindern und Korrigieren der Nutzung, Zuweisung und Konfiguration von Administratorrechten für Computer, Netzwerke und Anwendungen

Empfehlung – Wählen Sie Druckgeräte und -lösungen, die die Authentifizierung von Benutzern und die rollenbasierte Steuerung des Zugriffs auf Funktionen ermöglichen, sodass nur IT-Mitarbeiter und andere autorisierte Benutzer Geräteeinstellungen einrichten und konfigurieren können. Setzen Sie Software zur Verwaltung der Flottensicherheit ein, um flottenweit Administrator-Kennwörter festzulegen.

CSC 6: Erstellung, Überwachung und Analyse von Audit-Protokollen

Maßnahme – Erstellen, Verwalten und Analysieren von Audit-Protokollen von Ereignissen, mit denen sich Angriffe erkennen und nachvollziehen und Wiederherstellungen nach Angriffen durchführen lassen

Empfehlung – Druckgeräte sollten eine Funktion zum Erstellen von Systemprotokollmeldungen zu Vorfällen aufweisen, sodass Ihr Sicherheitsteam regelmäßig Audit-Protokolle auswerten kann, um Probleme zu erkennen und zu beheben. Wählen Sie Geräte, die diese Meldungen an Verwaltungslösungen für Flottensicherheit und SIEM-Tools senden können, um eine Überwachung in Echtzeit und die Berichterstellung zu Audit- oder anderen Compliance-Zwecken zu ermöglichen.

CSC 7: E-Mail- und Webbrowserschutz

Maßnahme – Verringern der Angriffsfläche und der Möglichkeiten für Angreifer, Benutzerverhalten durch ihre Interaktionen mit Internetbrowsern und E-Mail-Systemen zu manipulieren

Empfehlung – MFPs sind häufig mit dem Internet verbunden, um beispielsweise das Scannen an E-Mail zu ermöglichen. Stellen Sie sicher, dass per E-Mail gesendete Scans verschlüsselt werden, um vertrauliche Daten zu schützen. Stellen Sie Geräte und Lösungen bereit, die Benutzer authentifizieren und rollenbasiert den Zugriff auf die über das Gerät verfügbaren Ressourcen steuern können (beispielsweise Webserver oder E-Mail-Funktionen). Erstellen Sie eine Liste mit vertrauenswürdigen Sites für Ihre MFPs und verwalten Sie diese entsprechend, um sicherzustellen, dass über die Geräte nur auf vertrauenswürdige Websites zugegriffen wird. Binden Sie unterschiedliche Authentifizierungsmethoden in Active Directory ein (beispielsweise das Anmelden per PIN/PIC, LDAP oder Kerberos-Authentifizierung), um die Verwaltung zu optimieren und die Sicherheit zu erhöhen. Mit dem Netzwerk verbundene Druckgeräte sollten über einen integrierten Malware- und Virenschutz verfügen und die Drucker-Firmware sollte regelmäßig aktualisiert werden, sodass die neuesten Schutzmechanismen greifen können.

CSC 8: Schutz vor Malware

Maßnahme – Überwachen der Installation, Verbreitung und Ausführung von Malware an verschiedenen Stellen im Unternehmen, während gleichzeitig die Automatisierung verstärkt wird, um eine schnelle Aktualisierung der Schutzmechanismen, Datenerfassung und Korrekturmaßnahmen zu ermöglichen

Empfehlung – Wählen Sie Druckgeräte, die ausschließlich verifizierten und signierten Code laden und über integrierte Funktionen zum Schutz vor Malware verfügen, die den Gerätespeicher aktiv überwachen und im Falle eines Angriffs automatisch einen Neustart auslösen. Ein effektives Verwaltungstool für die Drucksicherheit kann die Geräteeinstellungen für die gesamte Druckerflotte automatisch bewerten und korrigieren. Sie sollten sicherstellen, dass alle Softwarelösungen für den Druck signiert und als authentisch validiert wurden.

CSC 9: Einschränkung und Überwachung der Netzwerk-Ports, Protokolle und Netzwerkdienste

Maßnahme – Verwalten (Nachverfolgen, Kontrollieren und Korrigieren) der fortlaufenden Nutzung von Ports, Protokollen und Diensten von Netzwerkgeräten, um Schwachstellen zu minieren und auf diese Weise so wenig Angriffsfläche wie möglich zu bieten

Empfehlung – Deaktivieren Sie, falls diese nicht standardmäßig deaktiviert sind, nicht genutzte Anschlüsse und unsichere Protokolle (wie FTP oder Telnet), um den Zugriff von Angreifern auf die Geräte zu unterbinden. Verringern Sie den Zeitaufwand der IT und mindern Sie Risiken, indem Sie ein Verwaltungstool für die Drucksicherheit bereitstellen, um automatisch für flottenübergreifend richtlinienkonforme Geräteeinstellungen zu sorgen. Nutzen Sie Administrator-Kennwörter, Authentifizierung und eine rollenbasierte Zugriffssteuerung, um den Zugriff auf Gerätefunktionen und -einstellungen zu beschränken.

CSC 10: Funktion für die Datenwiederherstellung

Maßnahme – Ordnungsgemäßes Sichern kritischer Informationen mithilfe bewährter Methoden für eine zeitnahe Wiederherstellung

Empfehlung – Diese Maßnahme ist derzeit nicht für Drucker anwendbar.

CSC 11: Sichere Konfigurationen für alle Netzwerkkomponenten wie Firewalls, Router und Switches

Maßnahme – Festlegen, Implementieren und aktives Verwalten (Nachverfolgen, Erfassen in Berichten und Korrigieren) der Sicherheitskonfiguration von Netzwerkinfrastrukturgeräten durch konsequentes Konfigurationsmanagement und ein strenges Änderungsüberwachungsverfahren, um zu verhindern, dass Angreifer Dienste und Einstellungen manipulieren

Empfehlung – Drucker sind in das Netzwerk eingebunden und sollten, wie andere Netzwerkendpunkte auch, eine sichere Konfiguration aufweisen. Ein effektives Verwaltungstool für die Drucksicherheit kann die Richtlinienerstellung, -implementierung und -bewertung sowie die Korrektur von Geräteeinstellungen für die gesamte Druckerflotte automatisieren, um das Netzwerk zu schützen und der IT Zeiteinsparungen zu ermöglichen.

CSC 12: Absicherung des Netzwerkperimeters

Maßnahme – Erkennen, Verhindern und Korrigieren der Übertragung von Informationen über Netzwerke mit unterschiedlichen Vertrauensstufen, wobei der Schwerpunkt auf sicherheitsgefährdenden Daten liegt

Empfehlung – Verschlüsseln Sie die Daten, um sie bei der Übertragung (Druck- oder Scanaufträge, die an oder vom Drucker übertragen werden) und nach der Speicherung auf der Festplatte des Geräts zu schützen. Wählen Sie Druckgeräte und -lösungen, die die Authentifizierung von Benutzern und die rollenbasierte Steuerung des Zugriffs auf Funktionen ermöglichen, sodass beispielsweise nur autorisierte Benutzer Scanaufträge per E-Mail versenden oder Dateien an Cloud-Ziele senden können. Konfigurieren Sie vertrauenswürdige Websites in der Liste mit vertrauenswürdigen Sites für das Gerät, um den Zugriff auf bösartige Websites zu unterbinden. Mit Lösungen für sicheres mobiles Drucken können Benutzer ohne großen Aufwand über ihre mobilen Geräte drucken, während gleichzeitig das Netzwerk geschützt wird.

CSC 13: Datenschutz

Maßnahme – Verhindern der Ausschleusung von Daten, Mindern der Auswirkungen ausgeschleuster Daten und Gewährleisten des Schutzes und der Vertraulichkeit sensibler Daten

Empfehlung – Verschlüsseln Sie die Daten, um sie bei der Übertragung (Druck- oder Scanaufträge, die an oder vom Drucker übertragen werden) und nach der Speicherung auf der Festplatte des Geräts zu schützen. Stellen Sie Pull-Printing-Lösungen bereit, um zu vermeiden, dass vertrauliche Dokumente im Ausgabefach der Druckgeräte vergessen werden. Stellen Sie sicher, dass auf den Gerätefestplatten gespeicherte Daten vor der Rückgabe geleaster Geräte oder dem Recycling ausgemusterter Geräte gelöscht werden.

CSC 14: Ausschließliche Vergabe von erforderlichen Zugriffsrechten

Maßnahme – Nachverfolgen, Steuern, Verhindern, Korrigieren und Schützen des Zugriffs auf kritische Assets (beispielsweise Informationen, Ressourcen und Systeme) gemäß der formalen Festlegung, welche Benutzer, Computer und Anwendungen auf Grundlage einer genehmigten Klassifizierung auf diese kritischen Assets zugreifen müssen und dürfen

Empfehlung – Wählen Sie Druckgeräte und -lösungen, die die Authentifizierung von Benutzern und die rollenbasierte Steuerung des Zugriffs auf Funktionen ermöglichen. Binden Sie unterschiedliche Authentifizierungsmethoden in Active Directory ein (beispielsweise das Anmelden per PIN/PIC, LDAP oder Kerberos-Authentifizierung), um die Verwaltung zu optimieren und die Sicherheit zu erhöhen. Pull-Printing-Lösungen können verhindern, dass vertrauliche Dokumente in falsche Hände geraten.

CSC 15: Zugriffssteuerung für Wireless-Netzwerke

Maßnahme – Nachverfolgen, Kontrollieren, Verhindern und Korrigieren der sicheren Nutzung von Wireless Local Area Networks (WLANs), Zugangspunkten und Wireless-Clientsystemen

Empfehlung – Ein effektives Verwaltungstool für die Drucksicherheit kann die Richtlinienerstellung, -implementierung und -bewertung sowie die Korrektur von Geräteeinstellungen – einschließlich Einstellungen für drahtlose Verbindungen – für die gesamte Druckerflotte automatisieren. Verwenden Sie Lösungen zur Zugriffssteuerung, um den Zugriff auf Gerätefunktionen wie das Scannen an E-Mail rollenbasiert zu beschränken. Mit Lösungen für sicheres mobiles Drucken können Benutzer ohne großen Aufwand über ihre mobilen Geräte drucken, während gleichzeitig das Netzwerk geschützt wird. Beispielsweise ermöglichen Geräte, die Peer-to-Peer Wireless-Druck unterstützen, direktes mobiles Drucken mithilfe des eigenständigen Wireless-Signals des Druckers – ohne hierfür auf das Unternehmensnetzwerk oder Wireless-Services zugreifen zu müssen.

CSC 16: Überwachung und Kontrolle von Benutzerkonten

Maßnahme – Aktives Verwalten des Lebenszyklus von System- und Anwendungskonten – ihre Erstellung, Nutzung, Inaktivität, Löschung –, um die Möglichkeiten potenzieller Angreifer zu minimieren, diese Konten für ihre Zwecke zu nutzen

Empfehlung – Wählen Sie Druckgeräte und -lösungen, die die Authentifizierung von Benutzern und die rollenbasierte Steuerung des Zugriffs auf Funktionen ermöglichen. Binden Sie Authentifizierungsmethoden in Active Directory ein, um die Verwaltung zu zentralisieren und die Sicherheit zu erhöhen. Überprüfen Sie regelmäßig die Benutzerkonten und deaktivieren Sie nicht benötigte Konten. Verwenden Sie außerdem Lösungen zur Nachverfolgung, um die Kontennutzung zu überwachen. Verschlüsseln Sie bei der Übertragung und nach dem Speichern Kontobenutzernamen und Anmeldeinformationen für die Authentifizierung. Sicherheitsberater können Sie bei der Entwicklung eines umfassenden Plans für die Drucksicherheit zur Minimierung von Risiken unterstützen und Ihnen ggf. helfen, die Sicherheitsmaßnahmen wie Benutzerkontenüberwachung und -steuerung zu verwalten.

CSC 17: Bewertung der Sicherheitskenntnisse und Durchführung von Schulungsmaßnahmen

Maßnahme – Identifizieren spezieller Kenntnisse, Fertigkeiten und Fähigkeiten, die zur Unterstützung der Schutzmaßnahmen des Unternehmens erforderlich sind; Entwickeln und Ausführen eines integrierten Plans zum Bewerten, Identifizieren und Beseitigen von Wissenslücken mithilfe von Richtlinien, strategischer Planung, Schulungen und Programmen zur Sensibilisierung für alle Benutzer mit funktionalen Aufgaben im Unternehmen

Empfehlung – Berater für Drucksicherheit verfügen über spezielle Kenntnisse, mit denen sie Sie dabei unterstützen können, Ihre Sicherheitsrisiken zu bewerten, eine umfassende Sicherheitsrichtlinie und einen Plan zu entwickeln sowie Verfahrens- und Technologieempfehlungen umzusetzen. Einige Sicherheitsservices können sogar die Drucksicherheit und Compliance für Sie verwalten.

CSC 18: Schutz der Softwareanwendungen

Maßnahme – Verwalten des Sicherheitslebenszyklus aller intern entwickelten und erworbenen Anwendungen, um Schwachstellen hinsichtlich der Sicherheit zu vermeiden, zu erkennen und zu beseitigen

Empfehlung – Halten Sie Best Practices für eine sichere Entwicklung für alle intern entwickelten Drucklösungen ein. Wählen Sie Softwarelösungen, die signiert und als authentisch validiert wurden.

CSC 19: Reaktion auf sicherheitsrelevante Ereignisse und Störungsmanagement

Maßnahme – Schützen der Daten und des Rufs des Unternehmens durch den Aufbau einer Infrastruktur für die Vorfallsreaktion (beispielsweise Pläne, definierte Rollen, Schulungen, Kommunikation und Managementaufsicht)

Empfehlung – Stellen Sie sicher, dass Ihre Druckumgebung in Ihrem Vorfallsreaktionsplan berücksichtigt ist.

CSC 20: Penetrationstests und Red Team-Analysen

Maßnahme – Testen der allgemeinen Stärke der Schutzmechanismen eines Unternehmens (Technologie, Verfahren und Mitarbeiter) durch Simulation der Ziele und Aktionen eines Angreifers

Empfehlung – Binden Sie Ihre Druckumgebung bei der Ausführung von Penetrationstests ein. Bewerten Sie Ihre Druckumgebung regelmäßig, um Schwachstellen zu erkennen, und aktualisieren Sie Ihren Sicherheitsplan, um diese Sicherheitslücken zu schließen.

Machen Sie den nächsten Schritt

Durch die Umsetzung der in diesem Whitepaper aufgeführten Empfehlungen können Sie die Drucksicherheit in Ihrem Unternehmen stärken und Compliance-Anforderungen besser erfüllen. Benötigen Sie Unterstützung? Drucksicherheits-management- und Beratungsservices können Ihnen bei der Entwicklung eines Plans sowie der Umsetzung von Verfahren und Bereitstellung von Technologien helfen, um die Sicherheit für Ihre Druckgeräte, Daten und Dokumente zu verbessern.

Anhang A: HP Funktionen, Lösungen und Services für die Drucksicherheit

Die in HP Geräte integrierten Sicherheitsfunktionen sowie branchenführende Softwarelösungen und -services können Ihnen helfen, regulatorische Anforderungen und Compliance-Vorgaben zu erfüllen und Ihre Geschäftsinformationen vor Sicherheitsbedrohungen zu schützen.

Integrierte Sicherheitsfunktionen in HP Enterprise-Druckern und -MFPs schützen vor Malware und ermöglichen die automatische Angriffserkennung und Wiederherstellung. Nur HP Lösungen für sicheres Drucken bieten Optionen zur Erkennung von Bedrohungen in Echtzeit, eine automatisierte Überwachung und eine integrierte Funktion zur Überprüfung von Software, um Bedrohungen abzuwehren, sobald sie auftreten.[4] (Bieten Unterstützung bei der Umsetzung der Maßnahmen CSC 2, 4, 6 und 8.) hp.com/go/PrintersThatProtect

HP Access Control-Lösungen bieten eine Vielzahl von Methoden zur Authentifizierung und rollenbasierten Zugriffssteuerung, um mögliche Sicherheitsverstöße zu vermeiden, sowie Funktionen zur Nachverfolgung und Abrechnung von Aufträgen. (Bieten Unterstützung bei der Umsetzung der Maßnahmen CSC 5, 7, 10, 12, 13, 14, 15 und 16.) hp.com/go/hpac

Verschlüsselung und **HP JetAdvantage Workflow-Lösungen** schützen Daten sowohl während der Speicherung auf HP Enterprise-Geräten als auch bei der Übertragung an bzw. von Geräten oder Cloud-Speichern. (Bieten Unterstützung bei der Umsetzung der Maßnahmen CSC 12 und 13.) hp.com/go/upd, hp.com/go/documentmanagement

HP Pull-Printing-Lösungen schützen vertrauliche Dokumente, indem die Druckaufträge auf einem geschützten Server, in der Cloud oder auf Ihrem PC gespeichert werden. Die Benutzer authentifizieren sich am Drucker ihrer Wahl, um ihre Druckaufträge abzurufen und die Dokumente zu drucken. (Bieten Unterstützung bei der Umsetzung der Maßnahmen CSC 10, 13 und 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect ermöglicht mobilen Benutzern das einfache Drucken über Smartphones und Tablets, ohne Sicherheitsrisiken einzugehen oder die Kontrolle aus der Hand zu geben. (Bietet Unterstützung bei der Umsetzung der Maßnahmen CSC 12 und 15.) hp.com/go/JetAdvantageConnect

Ereignisdaten von HP Druckern können in SIEM-Tools wie ArcSight, Splunk oder SIEMonster eingespeist werden. Geräte können als Teil des weiteren IT-Systems problemlos von Ihrem Sicherheitsteam überwacht werden, sodass dieses Maßnahmen zur Fehlerbehebung einleiten kann. (Bieten Unterstützung bei der Umsetzung der Maßnahmen CSC 4 und 6.)

HP JetAdvantage Security Manager ist das branchenweit einzige Compliance-Tool für die richtlinienbasierte Drucksicherheit.[5] Es hilft Ihnen, eine flottenübergreifende Sicherheitsrichtlinie zu implementieren, die Korrektur der Sicherheitseinstellungen von Geräten zu automatisieren und eindeutige Zertifikate zu installieren und zu erneuern, während Sie gleichzeitig die erforderlichen Berichte abrufen, um die Compliance nachzuweisen. Mit der inbegriffenen Instant-on-Funktion der Lösung lassen sich neue Geräte problemlos schützen, sobald diese dem Netzwerk hinzugefügt oder neu gestartet werden. (Bietet Unterstützung bei der Umsetzung der Maßnahmen CSC 1, 2, 3, 4, 5, 6, 8, 9, 11 und 15.) hp.com/go/securitymanager

HP Secure Managed Print Services bieten die branchenweit effektivsten und umfassendsten Mechanismen für Drucksicherheit.[6] Drucksicherheit zu gewährleisten ist keine einfache Aufgabe. Überlassen Sie HP die Verwaltung Ihrer Drucksicherheit – von der Stärkung der Gerätesicherheit bis hin zur Bereitstellung von erweiterten Sicherheitslösungen für Mitarbeiter, Verfahren und Compliance. (Bieten Unterstützung bei der Umsetzung der Maßnahmen CSC 2, 3, 12, 16, 17, 18 und 19.) hp.com/go/SecureMPS

HP Print Security Professional Services stellen Ihnen Sicherheitsexperten zur Seite, die Ihnen dabei helfen, Ihre Druckumgebung zu bewerten, proaktiv Sicherheitsrichtlinien einzuführen und Ihren Sicherheitsplan auf dem neuesten Stand zu halten. Wir können sogar die Einhaltung der Drucksicherheit für Sie verwalten. (Bieten Unterstützung bei der Umsetzung der Maßnahmen CSC 2, 3, 12, 16, 17 und 19.) hp.com/go/SecureMPS

Hinweise

[1] Ponemon-Studie im Auftrag von HPE, „2016 Cost of Cyber Crime Study & the Risk of Business Innovation“, 2016.

[2] 2016 Year End Data Breach QuickView Report von RiskBased Security, Januar 2017.

[3] 26,2 % der Umfrageteilnehmer haben einen gravierenden Verstoß gegen die IT-Sicherheit erlebt, der Maßnahmen zur Problemkorrektur erforderte, und mehr als 26,1 % dieser Fälle standen im Zusammenhang mit der Drucktechnologie. IDC, „IT and Print Security Survey 2015“, IDC #US40612015, September 2015.

[4] Gilt für Anfang 2015 eingeführte HP Geräte der Enterprise-Klasse und basiert auf Untersuchungen von HP zu im Jahr 2016 veröffentlichten integrierten Sicherheitsfunktionen vergleichbarer Drucker anderer Hersteller. Nur HP bietet eine Kombination aus Sicherheitsfunktionen für Integritätsprüfungen, die selbst das BIOS einschließen und Technologien zur automatischen Fehlerbehebung umfassen. Möglicherweise ist ein FutureSmart Service-Pack-Update erforderlich, um die Sicherheitsfunktionen zu aktivieren. Eine Liste kompatibler Produkte finden Sie unter hp.com/go/PrintersThatProtect. Weitere Informationen finden Sie unter hp.com/go/printersecurityclaims.

[5] HP JetAdvantage Security Manager muss separat erworben werden. Weitere Informationen hierzu finden Sie unter hp.com/go/securitymanager. Angaben basieren auf internen HP Untersuchungen zu Angeboten anderer Anbieter (Vergleich zur Gerätesicherheit, Januar 2015) und einem Lösungsbericht zu HP JetAdvantage Security Manager 2.1 von Buyers Laboratory LLC, Februar 2015.

[6] Beinhaltet Sicherheitsfunktionen führender Managed Print Services-Anbieter zum Schutz von Geräten, Daten und Dokumenten. Basierend auf internen HP Analysen von öffentlich verfügbaren Informationen von 2015-2016 zu Sicherheitsservices, Sicherheits- und Verwaltungssoftware und integrierten Sicherheitsfunktionen vergleichbarer Drucker anderer Hersteller. Weitere Informationen finden Sie unter hp.com/go/MPSsecurityclaims oder hp.com/go/mps.

Für Updates registrieren unter
hp.com/go/getupdated

An Kollegen weiterleiten

4AA6-8821DEE, Juni 2017, Rev. 1