Technische whitepaper

Voldoen aan nalevingsvereisten voor beveiliging van netwerken en gegevens

Aanbevelingen voor het toepassen van beveiligingsmaatregelen op het printerpark

Inhoud

Klik hier om de meest recente versie van dit document te controleren.

Niet-naleving kan nadelige gevolgen hebben voor uw bedrijf

Behalve hoge boetes en rechtszaken kan een inbreuk op de beveiliging verlies van inkomsten en reputatieschade veroorzaken. Wanneer u uw beveiligingsplan opstelt, denk er dan aan dat uw netwerk net zo sterk is als de zwakste schakel ervan. Printers en imagingapparaten kennen veel van dezelfde beveiligingsproblemen als pc's. Het is van cruciaal belang dat u apparaten en oplossingen implementeert die voldoen aan nalevingsvereisten en uw bedrijfsgegevens beschermt tegen beveiligingsrisico's.

Wat is het risico?

Niet-naleving van regelgeving en wetten resulteert voor internationaal opererende bedrijven in hoge kosten, zoals boetes, misgelopen opdrachten, reputatieschade en collectieve juridische procedures.

Niet-beveiligde of onvoldoende beveiligde endpoints geven cybercriminelen nog meer gelegenheid om toe te slaan. Organisaties die onlangs door Ponemon zijn onderzocht hadden in 2016 gemiddeld twee keer per week met een aanval te maken. Dat is een toename van 23% per jaar, waarbij naar schatting per jaar gemiddeld $ 9,5 miljoen verloren gaat in het gevecht tegen cybercriminaliteit.[1] Alleen al in het afgelopen jaar zijn er wereldwijd meer dan 4 miljard gegevensbestanden gecompromitteerd. Dat is een toename van 400% ten opzichte van de twee voorafgaande jaren.[2]

Hoewel de meeste IT-afdelingen strenge beveiligingsmaatregelen hebben getroffen voor computers en het netwerk, worden printers en imagingapparaten vaak over het hoofd gezien. Maar printers kunnen wel degelijk een ingang tot uw netwerk vormen, en de beveiliging ervan is net zo belangrijk. Van alle belangrijke door IT-beheerders gerapporteerde gegevensschendingen, had 26% te maken met printers.[3]

Om de groeiende bedreigingen het hoofd te bieden, implementeren overheidsorganen overal ter wereld nieuwe, strenge beveiligingsmaatregelen die voorschrijven dat organisaties klantgegevens beter moeten beschermen. De nieuwe Algemene Verordening Gegevensbescherming van de EU bijvoorbeeld (afgekort tot GDPR in het Engels, General Data Protection Regulation) is een belangrijk mandaat dat in 2018 van kracht wordt. De Algemene Verordening Gegevensbescherming stelt hogere eisen aan bedrijven om gegevens te beschermen. Daarom wordt geadviseerd om ervoor te zorgen dat elk apparaat in uw netwerk, van pc's tot printers tot mobiele apparaten, beschermd is. Het nieuwe mandaat heeft niet alleen gevolgen voor landen in de EU. Wereldwijd moeten bedrijven aan deze vereisten voldoen als zij gegevens van inwoners van de EU verzamelen. Organisaties zullen elk apparaat moeten controleren om inbreuken op de beveiliging te detecteren en deze te rapporteren binnen 72 uur nadat zij zich hiervan bewust zijn geworden. Als nalevingsaudits inbreuken aan het licht brengen die niet zijn opgemerkt en niet zijn gerapporteerd, kunnen er boetes worden opgelegd tot € 20 miljoen of 4% van de jaarlijkse omzet van een bedrijf.

Hanteer gangbare beveiligingsmaatregelen om de naleving te verbeteren

Het is een hele uitdaging om naleving en regelgeving in de sector bij te houden. Gelukkig heeft het Center for Internet Security (CIS) een reeks algemene beveiligingsmaatregelen opgesteld om aanbevelingen op het gebied van cyberveiligheid te vereenvoudigen. De kritieke beveiligingsmaatregelen van het CIS bestaan uit 20 specifieke acties die cyberaanvallen een halt kunnen toeroepen. (Raadpleeg https://www.cisecurity.org/critical-controls.cfm voor meer informatie.) De maatregelen sluiten aan op andere regelgeving in de sector, waaronder die van PCI-DSS, ISO 27001, US CERT-aanbevelingen, HIPAA, FFIEC en NIST. De maatregelen zijn geen poging om deze andere kaders te vervangen, maar worden vaak gebruikt door ondernemingen om andere kaders beter te begrijpen.

De kritieke beveiligingsmaatregelen van het CIS zijn een opsomming van acties in volgorde van belangrijkheid die veel resultaat opleveren. De maatregelen hebben betrekking op de meest algemene aanvalspatronen uit toonaangevende bedreigingsrapporten. Een brede groep deskundigen in de sector, waaronder enkele vooraanstaande organisaties op het gebied van forensisch onderzoek en incidentrespons, heeft bijgedragen aan de opstelling ervan. Bovendien worden de maatregelen steeds bijgewerkt op basis van bedreigingen en aanvallen die zich steeds verder ontwikkelen.

Hanteer de kritieke beveiligingsmaatregelen van het CIS om uw beveiligingsactieplan op te stellen en aan nalevingsregels te voldoen. In deze whitepaper vindt u voorgestelde acties voor elk van de 20 maatregelen om uw printers en imagingapparaten, gegevens en documenten te beveiligen als onderdeel van uw grotere beveiligingsplan. Met name maatregel 4, 6, 8, 12, 13 en 15 gaan in op gegevensbeveiliging en controleactiviteiten die betrekking hebben op de vereisten van de nieuwe Algemene Verordening Gegevensbescherming.

Kritieke beveiligingsmaatregelen van het CIS en aanbevolen acties

Kritieke beveiligingsmaatregel 1: Inventariseer geautoriseerde en niet-geautoriseerde apparaten

Maatregel. Beheer (inventariseer, volg en corrigeer) actief alle hardwareapparaten in het netwerk, zodat alleen geautoriseerde apparaten toegang wordt verleend en ongeautoriseerde en niet-beheerde apparaten worden gevonden en wordt verhinderd dat deze toegang krijgen.

Aanbeveling. Zorg ervoor dat alle printers in het netwerk bekend zijn en actief worden beheerd, en dat hierop de beveiligingsregels en uw beveiligingsbeleid wordt nageleefd. Een effectieve beheertool voor printbeveiliging kan alle apparaten in het netwerk en alle verbonden pc's detecteren en hierin inzicht geven.

Kritieke beveiligingsmaatregel 2: Inventariseer geautoriseerde en niet-geautoriseerde software

Maatregel. Beheer (inventariseer, volg en corrigeer) actief alle software in het netwerk, zodat er alleen geautoriseerde software wordt geïnstalleerd en kan worden uitgevoerd, en ongeautoriseerde en niet-beheerde software wordt gevonden en wordt verhinderd dat deze wordt geïnstalleerd en uitgevoerd.

Aanbeveling. Zorg ervoor dat alle firmware en oplossingen die op printers en imagingapparaten zijn gezet up-to-date zijn, zijn ondertekend en dat gevalideerd is dat deze authentiek zijn. Kies printers met ingebouwde beveiliging voor BIOS en firmware om ervoor te zorgen dat er alleen authentieke code wordt geladen. Proactieve firmware-updates kunnen met parkbeheeroplossingen naar het gehele park worden gepusht. Software (serversoftware of clientsoftware) moet zijn ondertekend en er moet zijn gevalideerd dat deze authentiek is.

Kritieke beveiligingsmaatregel 3: Beveilig hardware- en softwareconfiguraties op mobiele apparaten, laptops, werkstations en servers

Maatregel. Stel een beveiligingsconfiguratie op, implementeer deze en beheer (volg, rapporteer en corrigeer) deze actief op laptops, servers en werkstations aan de hand van een streng configuratiebeheer- en wijzigingsbeheerproces om te verhinderen dat aanvallers services en instellingen met een beveiligingsprobleem misbruiken.

Aanbeveling. Net als bij andere endpoints in het netwerk moeten printerconfiguraties veilig zijn. U dient beveiligingsbeleid op te stellen en te implementeren voor al uw printers en elke afwijking van dat beleid actief op te lossen. Checklists voor de beveiliging (zoals NIST) of beveiligingsadviesdiensten kunnen u helpen bij het opstellen en implementeren van een allesomvattend beveiligingsbeleid voor uw printers. Met een effectieve beheertool voor printbeveiliging kan het maken, implementeren, beoordelen en oplossen van beleidsproblemen voor het gehele printerpark worden geautomatiseerd. Multifunctionele printers (MFP's) in een onderneming kunnen meer dan 250 beveiligingsinstellingen hebben. Het automatiseren van dit proces kan u heel wat tijd besparen.

Kritieke beveiligingsmaatregel 4: Controleer doorlopend op beveiligingsproblemen en los deze op

Maatregel. Win voortdurend nieuwe informatie in, beoordeel deze en onderneem actie om beveiligingsproblemen te identificeren, op te lossen en de kansen van aanvallers te minimaliseren.

Aanbeveling. SIEM-oplossingen (Security Information and Event Management) zoals ArcSight, Splunk en SIEMonster kunnen activiteiten in uw netwerk in realtime bewaken en beheerders op de hoogte brengen van incidenten die zich voordoen. Het controleren van printers is net zo belangrijk als het controleren van pc's. Zorg ervoor dat uw printers syslogberichten van gebeurtenissen kunnen verzenden naar uw SIEM-tool.

Kies printers met functies die aanvallen in realtime kunnen detecteren en hiervan automatisch kunnen herstellen om de uptime te maximaliseren en IT-interventies te minimaliseren.

Om beveiligingsproblemen te verkleinen, kunt u het beste een beveiligingsbeheertool voor uw printerpark gebruiken die nieuwe printers kan identificeren en automatisch de instellingen van bedrijfsbeveiligingsbeleid kan toepassen zodra apparaten verbinding met het netwerk maken. Plan periodieke beoordelingen en pas dan oplossingen toe zodat uw gehele printerpark het beleid blijft naleven.

Kritieke beveiligingsmaatregel 5: Zorg voor gecontroleerd gebruik van beheerdersmachtigingen

Maatregel. Volg, controleer, verhinder en corrigeer gebruik, toewijzing en configuratie van beheerdersmachtigingen op computers, in netwerken en applicaties.

Aanbeveling. Kies printers en printoplossingen die de mogelijkheid hebben om gebruikers te authenticeren en toegang tot functionaliteit te controleren op basis van iemands rol, zodat alleen IT-medewerkers of ander geautoriseerd personeel apparaatinstellingen kunnen instellen en configureren. Gebruik beheersoftware voor de beveiliging van uw printerpark om beheerderswachtwoorden in het gehele park te implementeren.

Kritieke beveiligingsmaatregel 6: Onderhoud, controleer en analyseer auditlogboeken

Maatregel. Verzamel, beheer en analyseer auditlogboeken van gebeurtenissen zodat u een aanval kunt detecteren, begrijpen en ervan kunt herstellen.

Aanbeveling. Printers moeten de mogelijkheid hebben om systeemlogberichten over incidenten te genereren zodat uw beveiligingsteam regelmatig auditlogboeken kan bekijken om problemen te detecteren en op te lossen. Kies apparaten die deze berichten naar beveiligingsoplossingen voor het beheren van printerparken en SIEM-tools kunnen verzenden, zodat controle in realtime mogelijk is en er rapporten kunnen worden gegenereerd ten behoeve van audits of andere nalevingsvereisten.

Kritieke beveiligingsmaatregel 7: Beveilig e-mail en webbrowsers

Maatregel. Minimaliseer het aanvalsoppervlak en de gelegenheden die aanvallers hebben om menselijk gedrag te manipuleren tijdens het gebruik van webbrowsers en e-mailsystemen.

Aanbeveling. Multifunctionele printers zijn vaak met internet verbonden. Deze apparaten kunnen bijvoorbeeld scans per e-mail verzenden. Zorg ervoor dat gemailde scans zijn versleuteld, zodat gevoelige gegevens beveiligd zijn. Implementeer apparaten en oplossingen die gebruikers kunnen authenticeren en die de toegang tot bronnen in het apparaat (zoals webservers of e-mailfunctionaliteit) kunnen controleren op basis van iemands rol. Maak een lijst met vertrouwde sites voor uw multifunctionele printers en beheer deze lijst om ervoor te zorgen dat alleen vertrouwde websites vanaf het apparaat worden benaderd. Integreer diverse authenticatiemethoden (zoals PIN/PIC, LDAP en Kerberos-authenticatie) in Active Directory voor een gestroomlijnd beheer en een betere beveiliging. Printers die zijn verbonden met het netwerk moeten ingebouwde malware- en virusbeveiliging hebben, en printerfirmware moet regelmatig worden bijgewerkt zodat de nieuwste bescherming van kracht is.

Kritieke beveiligingsmaatregel 8: Verdedig u tegen malware

Maatregel. Beheer de installatie, verspreiding en uitvoering van schadelijke code op meerdere punten in de onderneming, terwijl u het gebruik van automatisering optimaliseert om uw verdediging, het verzamelen van gegevens en het uitvoeren van correctieve acties snel bij te werken.

Aanbeveling. Kies printers waarop alleen geverifieerde, ondertekende code wordt geladen en die zijn uitgerust met ingebouwde antimalwarefuncties om het apparaatgeheugen actief te controleren en printers opnieuw op te starten in het geval van een aanval. Een beheertool voor printbeveiliging kan apparaatinstellingen in het gehele printerpark automatisch beoordelen en herstellen. U moet er ook voor zorgen dat alle printsoftwareoplossingen ondertekend zijn en zijn gevalideerd als authentiek.

Kritieke beveiligingsmaatregel 9: Beperk en beheer netwerkpoorten, protocollen en services

Maatregel. Beheer (volg, controleer en corrigeer) het alledaagse operationele gebruik van poorten, protocollen en services op netwerkapparaten om de kans op misbruik van beveiligingsproblemen door aanvallers te minimaliseren.

Aanbeveling. Schakel ongebruikte poorten en onbeveiligde protocollen uit (zoals FTP of Telnet) die aanvallers kunnen gebruiken om toegang tot het apparaat te krijgen, indien deze nog niet standaard zijn ingeschakeld. Bespaar IT-tijd en verlaag het risico door een beheertool voor printbeveiliging te implementeren om instellingen in het gehele printerpark automatisch aan het nalevingsbeleid te laten voldoen. Gebruik beheerderswachtwoorden, authenticatie en rollen als toegangsbeheermethoden om de toegang tot apparaatfunctionaliteit en instellingen te beperken.-

Kritieke beveiligingsmaatregel 10: Zorg dat gegevensherstel mogelijk is

Maatregel. Maak back-ups van cruciale informatie met een bewezen methodologie zodat u gegevens snel kunt herstellen.

Aanbeveling. Deze beheermaatregel is momenteel niet van toepassing op printers.

Kritieke beveiligingsmaatregel 11: Beveilig de configuratie van netwerkapparaten zoals firewalls, routers en switches

Maatregel. Stel een beveiligingsconfiguratie op, implementeer deze en beheer (volg, rapporteer en corrigeer) deze actief op netwerkinfrastructuurapparaten aan de hand van een streng configuratiebeheer- en wijzigingsbeheerproces om te verhinderen dat aanvallers services en instellingen met een beveiligingsprobleem misbruiken.

Aanbeveling. Printers bevinden zich in het netwerk en net als andere endpoints moeten deze een veilige configuratie hebben. Met een effectieve beheertool voor printbeveiliging kan de implementatie, beoordeling en het herstel van apparaatinstellingen in het printerpark worden geautomatiseerd om het netwerk veilig te houden en de IT-afdeling tegelijk tijd te besparen.

Kritieke beveiligingsmaatregel 12: Verdedig de buitengrenzen

Maatregel. Detecteer, voorkom en corrigeer de informatiestroom van en naar netwerken met verschillende vertrouwensniveaus en let daarbij in het bijzonder op gegevens die de beveiliging schade toebrengen.

Aanbeveling. Maak gebruik van versleuteling om gegevens te beveiligen die worden verzonden (print- of scantaken die van of naar de printer worden verzonden) en op de harde schijf van het apparaat zijn opgeslagen. Kies printers en printoplossingen met de mogelijkheid gebruikers te authenticeren en toegang tot functionaliteit te beheren op basis van iemands rol, zodat alleen geautoriseerde gebruikers scantaken kunnen e-mailen of bestanden kunnen verzenden naar een bestemming in de cloud. Neem vertrouwde websites op in de lijst met vertrouwde websites op het apparaat om toegang tot schadelijke websites te voorkomen. Met veilige oplossingen voor mobiel afdrukken kunnen gebruikers gemakkelijk vanaf hun mobiele apparaat afdrukken en tegelijk het netwerk beschermen.

Kritieke beveiligingsmaatregel 13: Bescherm uw gegevens

Maatregel. Voorkom het uitfilteren van gegevens, verklein de gevolgen van uitgefilterde gegevens en garandeer de privacy en integriteit van gevoelige informatie.

Aanbeveling. Maak gebruik van versleuteling om gegevens te beveiligen die worden verzonden (print- of scantaken die van of naar de printer worden verzonden) en op de harde schijf van het apparaat zijn opgeslagen. Implementeer pullprintoplossingen om te voorkomen dat gevoelige documenten in de uitvoerbak blijven liggen. Zorg ervoor dat gegevens die op de harde schrijven van apparaten zijn opgeslagen, veilig worden gewist voordat leaseapparaten worden teruggegeven en zorg voor een veilige recycling aan het einde van de nuttige levensduur van apparaten.

Kritieke beveiligingsmaatregel 14: Beheer toegang op basis van noodzaak

Maatregel. Volg, beheer, voorkom, corrigeer en beveilig toegang tot cruciale activa (bijvoorbeeld informatie, bronnen en systemen) op basis van een formele bepaling van welke personen, computers en applicaties recht op toegang tot deze cruciale activa moeten hebben.

Aanbeveling. Kies printers en printoplossingen die de mogelijkheid bieden om gebruikers te authenticeren en de toegang tot functionaliteit te controleren op basis van iemands rol. Integreer diverse authenticatiemethoden (zoals PIN/PIC, LDAP en Kerberos-authenticatie) in Active Directory voor een gestroomlijnd beheer en een betere beveiliging. Pullprintoplossingen kunnen voorkomen dat gevoelige documenten in verkeerde handen vallen.

Kritieke beveiligingsmaatregel 15: Beheer toegang tot draadloze netwerken

Maatregel. Volg, controleer, voorkom en corrigeer het veilige gebruik van draadloze netwerken (LAN's), accesspoints en draadloze clientsystemen.

Aanbeveling. Met een effectieve beheertool voor printbeveiliging kan het maken, implementeren, beoordelen en oplossen van onjuiste apparaatinstellingen, waaronder instellingen voor draadloze netwerken, voor het gehele printerpark worden geautomatiseerd. Maak gebruik van toegangsbeheeroplossingen om de toegang tot apparaatfunctionaliteit, zoals scannen naar een e-mailadres, op basis van iemands rol te beperken. Met veilige oplossingen voor mobiel afdrukken kunnen gebruikers gemakkelijk vanaf hun mobiele apparaat afdrukken en tegelijk het netwerk beschermen. Een voorbeeld: apparaten die ondersteuning bieden voor draadloos peer-to-peer afdrukken staan toe dat gebruikers van mobiele apparaten rechtstreeks afdrukken via een discreet draadloos signaal van een printer, zonder dat daarbij gebruik wordt gemaakt van het bedrijfsnetwerk of een draadloze service.

Kritieke beveiligingsmaatregel 16: Controleer en beheer accounts

Maatregel. Beheer actief de levenscyclus van systeem- en applicatieaccounts - maken, gebruiken, sluimerbestaan en verwijderen - om aanvallers minder kans te geven hiervan misbruik te maken.

Aanbeveling. Kies printers en printoplossingen die de mogelijkheid bieden om gebruikers te authenticeren en de toegang tot functionaliteit te controleren op basis van iemands rol. Integreer authenticatie in Active Directory ten behoeve van gecentraliseerd beheer en een betere beveiliging. Neem gebruikersaccounts regelmatig onder de loep, schakel onnodige accounts uit en gebruik volgoplossingen om het accountgebruik te controleren. Versleutel gebruikersnamen en authenticatiegegevens van accounts, zowel tijdens verzending ervan als wanneer deze op apparaten zijn opgeslagen. Beveiligingsadviseurs kunnen u helpen bij het opstellen van een uitgebreid printbeveiligingsplan om risico's te minimaliseren. In bepaalde gevallen kunnen zij u helpen bij het beheren van uw beveiliging, onder ander met accountcontrole en -beheer.

Kritieke beveiligingsmaatregel 17: Inventariseer beveiligingsvaardigheden en de behoefte aan aanvullende training

Maatregel. Breng de specifieke kennis en vaardigheden in kaart die nodig zijn voor de verdediging van de onderneming; ontwikkel een geïntegreerd plan en voer dit uit om hiaten in kaart te brengen en te verhelpen door middel van beleid, organisatorische planning, training en bewustwordingsprogramma's voor alle functierollen in de organisatie.

Aanbeveling. Beveiligingsadviseurs op het gebied van printing beschikken over gespecialiseerde kennis om u te helpen bij het beoordelen van uw beveiligingsrisico's, het ontwikkelen van een uitgebreid beveiligingsbeleid en -plan, en het implementeren van proces- en technologieaanbevelingen. Bepaalde beveiligingsdiensten kunnen zelfs de beveiliging en naleving van printbeveiliging voor u beheren.

Kritieke beveiligingsmaatregel 18: Beveilig applicatiesoftware

Maatregel. Beheer de beveiligingslevenscyclus van alle in-house ontwikkelde en aangeschafte software om (potentiële) beveiligingsproblemen te voorkomen, detecteren en verhelpen.

Aanbeveling. Houd u aan best practices op het gebied van het veilig ontwikkelen van software voor alle ontwikkelde printoplossingen. Kies softwareoplossingen die zijn ondertekend en zijn gevalideerd als authentiek.

Kritieke beveiligingsmaatregel 19: Incidentrespons en -beheer

Maatregel. Bescherm de informatie van uw organisatie, evenals de reputatie ervan, door een incidentresponsinfrastructuur (bijvoorbeeld plannen, gedefinieerde rollen, training, communicatie en beheertoezicht) op te stellen en te implementeren.

Aanbeveling. Controleer of uw printomgeving in uw incidentresponsplan is opgenomen.

Kritieke beveiligingsmaatregel 20: Voer penetratietests uit en oefen met het rode team

Maatregel. Test de algehele sterkte van de verdediging van een organisatie (technologie, processen en mensen) door de doelstellingen en acties van een aanvaller te simuleren.

Aanbeveling. Zorg dat uw printomgeving deel uitmaakt van de penetratietests. Beoordeel uw printomgeving regelmatig op (potentiële) beveiligingsproblemen en werk uw beveiligingsplan bij zodat deze beveiligingsproblemen daarin zijn opgenomen.

Zet de volgende stap

Het implementeren van de aanbevelingen in deze whitepaper kan ertoe bijdragen dat uw printbeveiliging wordt versterkt en regelgeving naleeft. Hulp nodig? Printbeveiligingbeheer en adviesdiensten kunnen u helpen bij het opstellen van een plan, en processen en technologie implementeren om de beveiliging van uw printers, gegevens en documenten te verbeteren.

Bijlage A: HP printbeveiligingsfuncties, oplossingen en services

De beveiligingsfuncties die zijn ingebouwd in HP apparaten kunnen er samen met toonaangevende softwareoplossingen en services in de sector voor zorgen dat u voldoet aan de vereisten voor naleving van regelgeving en wetgeving, en dat uw bedrijfsinformatie is beschermd tegen beveiligingsdreigingen.-leading software solutions and services, can help you meet regulatory and legal compliance requirements and protect your business information

Ingebouwde beveiligingsfuncties in HP Enterprise-printers en multifunctionele printers zorgen voor verdediging tegen malware, en kunnen aanvallen automatisch herkennen en hiervan herstellen. Alleen HP printbeveiliging biedt realtimedetectie, geautomatiseerde controle en ingebouwde softwarevalidatie om bedreigingen een halt toe te roepen zodra deze opduiken.[4] (Draagt bij aan naleving van kritieke beveiligingsmaatregel 2, 4, 6 en 8.) hp.com/go/PrintersThatProtect

HP Access Control-oplossingen bieden uiteenlopende authenticatie- en op rollen gebaseerde toegangsbeheerfuncties waarmee u het risico van potentiële schendingen van de beveiliging kunt verlagen, taken kunt volgen en er verantwoording over kunt afleggen. (Draagt bij aan naleving van kritieke beveiligingsmaatregel CSC 5, 7, 10, 12, 13, 14, 15 en 16.) hp.com/go/hpac

Encryption en **HP JetAdvantage Workflow Solutions** beschermen gegevens zowel wanneer deze zijn opgeslagen op HP Enterprise-apparaten als wanneer gegevens worden verzonden van en naar printers of de cloud. (Draagt bij aan naleving van kritieke beveiligingsmaatregel 12 en 13.) hp.com/go/upd, hp.com/go/documentmanagement

HP pullprintoplossingen beschermen vertrouwelijke documenten door afdruktaken op te slaan op een beschermde server, in de cloud of op uw pc. Gebruikers authenticeren zich bij de printlocatie van hun keuze om hun documenten vrij te geven en af te drukken. (Draagt bij aan naleving van kritieke beveiligingsmaatregel CSC 10, 13 en 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

Dankzij **HP JetAdvantage Connect** kunnen mobiele gebruikers gemakkelijk afdrukken vanaf smartphones en tablets terwijl de beveiliging en administratieve controle die u nodig hebt behouden blijven. (Draagt bij aan naleving van kritieke beveiligingsmaatregel 12 en 15.) hp.com/go/JetAdvantageConnect

Gegevens over HP printergebeurtenissen kunnen worden verzonden naar SIEM-tools, zoals ArcSight, Splunk en SIEMonster. Uw IT-beveiligingsteam ziet de printerendpoints als onderdeel van het totale IT-ecosysteem en kan indien nodig eenvoudig actie ondernemen. (Draagt bij aan naleving van kritieke beveiligingsmaatregel 4 en 6.)

HP JetAdvantage Security Manager is de enige op beleid gebaseerde tool op de markt voor de naleving van printbeveiliging.[5] Definieer beveiligingsbeleid voor al uw printers, automatiseer apparaatherstel, installeer en vernieuw unieke certificaten en ontvang de rapporten die nodig zijn als bewijs van naleving. De functie Instant-On van deze oplossing configureert automatisch nieuwe apparaten wanneer die aan het netwerk worden toegevoegd of opnieuw worden opgestart. (Draagt bij aan naleving van kritieke beveiligingsmaatregel 1, 2, 4, 5, 6, 8, 9 en 15.) hp.com/go/securitymanager

HP Secure Managed Print Services biedt de krachtigste, meest uitgebreide printbeveiliging in de sector.[6] Printbeveiliging kan uiterst gecompliceerd zijn. Laat HP uw printbeveiliging beheren, van het versterken van de beveiliging van apparaten tot geavanceerde beveiligingsoplossingen die voorzien in de behoeften van mensen, processen en nalevingvereisten. (Draagt bij aan naleving van kritieke beveiligingsmaatregel 2, 3, 12, 16, 17, 18 en 19.) hp.com/go/SecureMPS

HP Print Security Professional Services levert beveiligingsdeskundigen die u helpen bij het evalueren van uw printomgeving, proactief beveiligingsbeleid opstellen en uw beveiligingsplan up-to-date houden. Wij kunnen zelfs de naleving van printbeveiliging voor u beheren. (Draagt bij aan naleving van kritieke beveiligingsmaatregel 2, 3, 12, 16, 17 en 19.) hp.com/go/SecureMPS

Opmerkingen

[1] Onderzoek van Ponemon, gesponsord door HPE, naar de kosten van cybercriminaliteit en de risico's van bedrijfsinnovatie in 2016, oktober 2016.

[2] Het Year End Data Breach QuickView-rapport 2016 van RiskBased Security, januari 2017.

[3] 26,2% van de respondenten in een onderzoek was het slachtoffer van een forse schending van de IT-beveiliging en ruim 26,1% van die incidenten betrof de printomgeving. IDC, 'IT and Print Security Survey 2015' IDC #US40612015, september, 2015.

[4] Geldt voor HP Enterprise-klasseapparaten die zijn geïntroduceerd sinds 2015 en is gebaseerd op een evaluatie door HP van in 2016 gepubliceerde beveiligingskenmerken van concurrerende printers in dezelfde klasse. Alleen HP biedt een dergelijke combinatie van beveiligingsfuncties, van integriteitscontrole tot zelfherstellend BIOS. Om beveiligingsfuncties te activeren, is mogelijk een FutureSmart-servicepackupdate nodig. Kijk voor een overzicht van compatibele producten op hp.com/go/PrintersThatProtect. Kijk voor meer informatie op hp.com/go/printersecurityclaims.

[5] HP JetAdvantage Security Manager moet apart worden aangeschaft. Kijk voor meer informatie op hp.com/go/securitymanager. Claim over concurrenten is gebaseerd op intern onderzoek van HP naar concurrenten (Device Security Comparison, januari 2015) en een Solutions Report over HP JetAdvantage Security Manager 2.1 van Buyers Laboratory LLC, februari 2015.

[6] Omvat apparaat-, gegevens- en documentbeveiligingsfunctionaliteit van toonaangevende leveranciers van managed printservices. Gebaseerd op een evaluatie door HP van in 2015-2016 openbaar beschikbare informatie over beveiligingsservices, beveiligings- en beheersoftware en ingebouwde beveiligingskenmerken in concurrerende printers in dezelfde klasse. Kijk voor meer informatie op hp.com/go/MPSsecurityclaims of hp.com/go/mps.

4AA6-8821NLE, juni 2017, Rev. 1