Teknisk hvidbog

Opfyld lovmæssige krav for netværks- og datasikkerhed

Anbefalinger til at anvende sikkerhedsforanstaltninger i udskrivningsflåden

Indholdsfortegnelse

Klik her for at verificere den nyeste version af dette dokument

En tilsidesættelse af lovmæssige krav kan svække din virksomhed

Udover dyre bøder og sagsanlæg kan et brud på sikkerheden betyde tab af omsætning og et svækket omdømme. Når du udformer din sikkerhedsplan, så husk, at dit netværk kun er så stærkt som det svageste led. Udskrivnings- og scanningsenheder har mange af de samme svagheder som pc'er. Det er essentielt at installere enheder og løsninger, der kan opfylde lovmæssige krav og beskytter dine virksomhedsoplysninger mod sikkerhedstrusler.

Hvad er risikoen?

Hvis regulativer og juridiske krav ikke overholdes, medfører det store omkostninger for globale virksomheder, f.eks. i form af bøder, tabt fortjeneste, dårligt omdømme og gruppesøgsmål.

Ubeskyttede og underbeskyttede slutpunkter skaber flere muligheder for internetkriminalitet. De virksomheder, der deltog i en Ponemon-undersøgelse for nylig, oplevede i gennemsnit to angreb om ugen i 2016, hvilket er en stigning på 23 % i forhold til året før. De mistede gennemsnitligt 9,5 millioner USD om året i kampen mod cyberkriminalitet.[1] Alene sidste år blev 4 milliarder dataposter bragt i fare i hele verden – det svarer til en stigning på 400 % i løbet af de to foregående år.[2]

Selvom mange it-afdelinger omhyggeligt træffer sikkerhedsforanstaltninger på computere og netværket, bliver udskrivnings- og scanningsenheder ofte overset. Men printere kan give adgang til dit netværk, og det er ligeså vigtigt at sikre dem. Af alle signifikante sikkerhedsbrud, der blev rapporteret af it-chefer, involverede 26 % printere.[3]

I kampen mod den voksende trussel er myndigheder overalt i verden ved at indføre nye, strikse sikkerhedsregler, som kræver, at virksomheder og organisationer skal beskytte oplysninger om kunderne bedre. EU's nye persondataforordning er et eksempel på de nye regler. Den træder i kraft i 2018 og skærper kravene til virksomheders databeskyttelse. Derfor er det en god ide at sørge for, at alle enheder på netværket – fra pc'er til printere og mobilenheder – beskyttes effektivt. De nye regler har ikke kun betydning for virksomheder i EU-landene – globale virksomheder skal også overholde reglerne, hvis de indsamler og anvender data fra EU-borgere. Virksomhederne skal overvåge og vurdere hver enkelt enhed samt registrere og rapportere alle brud på sikkerheden inden for 72 timer, efter at de er opdaget. Hvis det ved en kontrol af overholdelse af reglerne viser sig, at der ikke har været overvågning, eller at brud på sikkerheden ikke er blevet rapporteret, kan virksomhederne idømmes bøder på op til 20 millioner USD eller 4 % af den årlige omsætning.

Udnyt fælles sikkerhedsforanstaltninger til at forbedre kravoverholdelse

Det er udfordrende at holde trit med branchekrav og lovmæssige krav, der skal overholdes. Heldigvis har Center for Internet Security (CIS) skabt et sæt fælles sikkerhedsforanstaltninger, der simplificerer internetsikkerhedsanbefalingerne. CIS' kritiske sikkerhedsforanstaltninger er 20 specifikke handlinger, der kan hjælpe dig med at stoppe internetangreb. (Se detaljer på https://www.cisecurity.org/critical-controls.cfm). Foranstaltningerne er tilpasset med mange andre brancheregulativer, såsom PCI-DSS, ISO 27001, US CERT-anbefalinger, HIPAA, FFIEC samt NIST. Foranstaltningerne er ikke et forsøg på at erstatte disse andre rammer, men de bliver ofte brugt af virksomheder til at få disse rammer til at give mening.

CIS' kritiske sikkerhedsforanstaltninger prioriterer et mindre antal handlinger, der giver et stort udbytte. De adresserer de mest almindelige angrebsmønstre fra førende trusselsindberetninger. En alsidig gruppe af brancheeksperter – inklusive nogle af de førende organisationer inden for retsvidenskab og respons på hændelser – har været med til at udvikle dem. Derudover bliver foranstaltningerne kontinuerligt opdateret baseret på de angreb og trusler, der udvikler sig.

Anvend CIS' kritiske sikkerhedsforanstaltninger som hjælp til at organisere din sikkerhedshandlingsplan og overholdelse af lovmæssige krav. Denne hvidbog foreslår handlinger for hver af de 20 foranstaltninger, som sikrer dine udskrivningsenheder, data og dokumenter som en del af din større sikkerhedsplan. Kontrolpunkt 4, 6, 8, 12, 13 og 15 drejer sig specifikt om databeskyttelse og overvågningsaktiviteter relateret til kravene i den nye persondataforordning.

CIS' kritiske sikkerhedsforanstaltninger og anbefalede handlinger

CSC 1: Opgørelse af godkendte og ikke-godkendte enheder

Foranstaltning – Administrer aktivt (lagerfør, spor og korriger) alle hardwareenheder på netværket, så kun godkendte enheder får adgang, og ikke-godkendte og underadministrerede enheder bliver opdaget og forhindret i at få adgang.

Anbefaling – Sørg for, at alle udskrivningsenheder på netværket er registrerede og aktivt administreret for overholdelse af din sikkerhedspolitik. Et effektivt udskrivningssikkerhedsværktøj kan opdage og synliggøre alle netværksenheder og pc-forbundne enheder.

CSC 2: Opgørelse af godkendt og ikke-godkendt software

Foranstaltning – Administrer aktivt (lagerfør, spor og korriger) al software i netværket, så kun godkendt software kan installeres og aktiveres, og ikke-godkendt og underadministreret software bliver opdaget og forhindret i installation og aktivering.

Anbefaling – Sørg for, at al firmware og alle løsninger, der bliver lagt på udskrivnings- og scanningsenheder, er opdaterede, underskrevet og valideret som ægte. Vælg udskrivningsenheder med indbygget beskyttelse for BIOS og firmware, så kun ægte kode bliver indlæst. Proaktive firmwareopdateringer kan skubbes på tværs af flåden med administrationsløsninger til udskrivningsflåder. Software (serverbaseret og klientbaseret) skal være underskrevet og valideret som værende ægte.

CSC 3: Sikre konfigurationer til hardware og software på mobile enheder, bærbare computere, arbejdsstationer og servere.

Foranstaltning – Etabler, implementer og administrer aktivt (spor, indberet på og korriger) sikkerhedskonfigurationen på bærbare computere, servere og arbejdsstationer med en stram konfigurationsadministration, og foretag ændringer i kontrolprocessen for at forhindre hackere i at udnytte sårbare tjenester og indstillinger.

Anbefaling – Ligesom alle andre netværksslutpunkter skal printerne konfigureres forsvarligt. Du bør skabe og udrulle en sikkerhedspolitik på tværs af alle udskrivningsenheder og aktivt afhjælpe afvigelser fra denne politik. Sikkerhedstjeklister (såsom NIST) eller sikkerhedsrådgivningstjenester kan hjælpe dig med at designe og udrulle en omfattende udskrivningssikkerhedspolitik. Et effektivt udskrivningsadministrationsværktøj kan automatisere skabelsen af en politik, udrulning, vurdering og afhjælpning af enhedsindstillinger på tværs af hele udskrivningsflåden. Multifunktionsprintere (MFP'er) på Enterprise-niveau har mere end 250 sikkerhedsindstillinger, så en automatisering af denne proces kan spare meget tid.

CSC 4: Kontinuerlig vurdering og afhjælpning af svagheder

Foranstaltning – Erhverv og vurder nye oplysninger, og grib løbende ind for at identificere svagheder og afhjælpe og minimere hackernes mulighed for at angribe.

Anbefaling – Security information and Event Management-løsninger (SIEM), som f.eks. ArcSight, Splunk eller SIEMonster, kan overvåge aktivitet på dit netværk under drift og give systemadministratorer besked, hvis der sker en hændelse. Det er lige så vigtigt at overvåge udskrivningsenheder som pc'er – sørg for, at dine printere kan sende syslog-beskeder om hændelser til dit SIEM-værktøj.

Vælg udskrivningsenheder med funktioner, der kan opdage angreb under drift og automatisk gendanne, for at maksimere oppetiden og minimere indgriben fra de it-ansatte.

For at reducere antallet af svagheder kan du bruge et flådesikkerhedsadministrationsværktøj, der kan identificere nye printere og automatisk anvende din virksomheds sikkerhedspolitikindstillinger i det øjeblik, enheden bliver forbundet til netværket. Planlæg regelmæssige vurderinger/afhjælpning for at sikre, at hele flåden overholder politikken.

CSC 5: Kontrolleret brug af administratorrettigheder

Foranstaltning – Spor, kontrollér, forebyg og korriger brug, tildeling og konfiguration af administratorrettigheder på computere, netværk og i programmer.

Anbefaling – Vælg udskrivningsenheder og -løsninger med mulighed for at godkende brugere og kontrollere adgangen til funktionalitet baseret på personens rolle, så kun it-ansatte og andet godkendt personale kan opsætte og konfigurere enhedsindstillinger. Brug flådesikkerhedsadministrationssoftware til at installere administratoradgangskoder på tværs af flåden.

CSC 6: Vedligeholdelse, overvågning og analyse af overvågningslogfiler

Foranstaltning – Indsaml, administrer og analysér overvågningslogfiler på hændelser, der kan hjælpe dig med at opdage, forstå og gendanne efter et angreb.

Anbefaling – Udskrivningsenheder skal kunne genere overvågningslogfiler for hændelser, så dit sikkerhedsteam regelmæssigt kan gennemgå filerne og opdage eventuelle uløste problemer. Vælg enheder, der kan sende disse beskeder til flådesikkerhedsadministrationsløsningerne og SIEM-værktøjer under drift og med muligheden for at skabe rapporter til revision eller andre overholdeskrav.

CSC 7: E-mail- og webbrowserbeskyttelse

Foranstaltning – Minimer angrebsfladen og muligheden for, at hackere kan manipulere menneskelig opførsel gennem deres interaktion med webbrowseren og e-mailsystemet.

Anbefaling – MFP'er er ofte forbundet til internettet, så de f.eks. kan sende scanninger via e-mail. Sørg for, at scanninger, der bliver sendt via e-mail, er krypteret for at beskytte følsomme oplysninger. Installer enheder og løsninger, der kan godkende brugere og kontrollere adgang til ressourcer i enheden (som f.eks. webservere ellller e-mailfunktionalitet) baseret på personens rolle. Opret en liste over "Betroede hjemmesider" til dine MFP'er, og administrer dem korrekt for at sikre, at kun betroede hjemmesider kan tilgås fra enheden. Integrer forskellige godkendelsesmetoder (såsom PIN/PIC, LDAP eller Kerberos-godkendelse) med aktive indeks for at få en strømlinet administration og øget sikkerhed. Udskrivningsenheder, der er forbundet til netværket, skal have indbygget malware- og virusbeskyttelse, og printerfirmware skal regelmæssigt opdateres, så den nyeste beskyttelse altid er gældende.

CSC 8: Malwarebeskyttelse

Foranstaltning – Kontrollér installationen, spredningen og aktiveringen af skadelig kode flere steder i koncernen, samtidig med at du optimerer brugen af automatisering for at muliggøre hurtig opdatering af forsvar, dataindsamling og korrigerende handling.

Anbefaling – Vælg udskrivningsenheder, der kun vil indlæse godkendt, underskrevet kode, der har indbyggede anti-malwarefunktioner til aktivt at overvåge enhedens hukommelse i tilfælde af et angreb. Et effektivt udskrivnings-administrationsværktøj kan automatisk vurdere og afhjælpe enhedsindstillinger på tværs af flåden. Du bør også sikre, at alle udskrivningssoftwareløsninger er underskrevet og valideret som ægte.

CSC 9: Begrænsning og kontrol af netværksindgange, protokoller og tjenester

Foranstaltning – Administrer (spor, kontrollér og korriger) løbende den driftsmæssige brug af indgange, protokoller og tjenester på netværksenheder for at minimere angrebsmuligheden for hackere.

Anbefaling – Hvis disse ikke er deaktiveret som standard, så deaktiver indgange, der ikke bliver brugt, samt usikre protokoller (såsom FTP eller Telnet), som hackere kan bruge til at få adgang til enheden. Spar it-afdelingen for tid, og reducer risici ved at installere et udskrivningssikkerhedsværktøj, der automatisk sikrer, at enhedsindstillingerne stemmer overens på tværs af flåden. Brug systemadministratoradgangskoder, godkendelse og rollebaserede kontroller til at begrænse adgangen til enhedens funktionalitet og indstillinger.

CSC 10: Datagendannelsesmulighed

Foranstaltning – Sørg for korrekt sikkerhedskopiering af kritiske oplysninger med en dokumenteret metode for rettidig gendannelse.

Anbefaling – Denne foranstaltning er for nærværende ikke gældende for printere.

CSC 11: Gør konfigurationer for netværksenheder sikre, såsom firewalls, routere og switches

Foranstaltning – Etabler, implementer og administrer aktivt (spor, indberet på og korriger) sikkerhedskonfigurationen på netværksinfrastrukturenheder med en stram konfigurationsadministration, og foretag ændringer i kontrolprocessen for at hindre hackere i at udnytte sårbare tjenester og indstillinger.

Anbefaling – Printere befinder sig på netværket, og ligesom alle andre slutpunkter skal printerne konfigureres forsvarligt. Et effektivt udskrivningsadministrationsværktøj kan automatisere installation, vurdering og afhjælpning af enhedsindstillinger på tværs af flåden, så netværket forbliver sikkert, og it-afdelingen sparer tid.

CSC 12: Afgrænsningsforsvar

Foranstaltning – Opdag, afværg og tilret strømmen i netværk, der overfører information med forskellige tillidsniveauer med fokus på sikkerhedsskadende data.

Anbefaling – Brug kryptering til at beskytte data i transit (udskrivnings- eller scanningsjob, der overføres til eller fra printeren), eller som ligger på enhedens harddisk. Vælg udskrivningsenheder og løsninger med mulighed for at godkende brugere og kontrollere adgangen til funktionaliteter, baseret på personens rolle, så f.eks. kun godkendte brugere kan e-maile scanningsjob eller sende filer til destinationer i skyen. Konfigurer betroede hjemmesider på listen over "Betroede hjemmesider" på enheden for at forhindre adgang til skadelige hjemmesider. Sikre mobile udskrivningsløsninger kan gøre det nemt for brugere at udskrive fra deres mobile enheder, samtidig med at de er med til at beskytte netværket.

CSC 13: Databeskyttelse

Foranstaltning – Forebyg udsivning af data, afbød virkningerne af udsevet data, og sørg for, at følsomme oplysninger forbliver private og bevarer deres integritet.

Anbefaling – Brug kryptering til at beskytte data i transit (udskrivnings- eller scanningsjob, der overføres til eller fra printeren), eller som ligger på enhedens harddisk. Installer pull-udskrivningsløsninger for at undgå, at følsomme dokumenter bliver efterladt i udbakker. Sørg for, at data, som er gemt på enhedsharddiske, bliver sikkert slettet ved returnering af leasede enheder, eller når den udtjente enhed bliver sendt til genbrug.

CSC 14: Kontrolleret adgang baseret på "behov for at vide"

Foranstaltning – Spor, kontrollér, forebyg, korriger og beskyt adgangen til kritiske aktiver (f.eks. oplysninger, ressourcer og systemer) i henhold til formel fastlæggelse af, hvilke personer, computere og programmer der har behov og ret til at tilgå kritiske aktiver baseret på en godkendt klassificering.

Anbefaling – Vælg udskrivningsenheder og -løsninger med mulighed for at godkende brugere, og kontrollér adgangen til funktionalitet baseret på personens rolle. Integrer forskellige godkendelsesmetoder (såsom PIN/PIC-, LDAP- eller Kerberos-godkendelse) med aktive indeks for at få en strømlinet administration og øget sikkerhed. Pull-udskrivningsløsninger kan beskytte følsomme dokumenter mod at ende i de forkerte hænder.

CSC 15: Trådløs adgangskontrol

Foranstaltning – Spor, kontrollér, forebyg og korriger sikkerhedsbrugen af trådløse lokalområdenetværk (LAN-netværk), adgangspunkter og trådløse klientsystemer.

Anbefaling – Et effektivt udskrivningsadministrationsværktøj kan automatisere installation, vurdering og afhjælpning af enhedsindstillinger – inklusive trådløse indstillinger – på tværs af hele flåden. Brug adgangskontrolløsninger til at begrænse adgangen til enhedsfunktionalitet, såsom scanning til e-mail, baseret på brugerens rolle. Sikre mobile udskrivningsløsninger kan gøre det nemt for brugere at udskrive fra deres mobile enheder, samtidig med at de er med til at beskytte netværket. Enheder, der understøtter trådløs peer-to-peer-udskrivning, tillader f.eks. brugere af mobile enheder at udskrive direkte via en printers separate, trådløse signal – uden at tilgå virksomhedens netværk eller trådløse tjeneste.

CSC 16: Kontoovervågning og kontrol

Foranstaltning – Administrer aktivt livscyklussen i systemet og programkonti – deres oprettelse, brug, dvaletilstand, sletning – for at kunne mindske muligheden for, at hackere udnytter dem.

Anbefaling – Vælg udskrivningsenheder og -løsninger med mulighed for at godkende brugere, og kontrollér adgangen til funktionalitet baseret på personens rolle. Integrer godkendelse med aktive indeks for at få centraliseret administration og øget sikkerhed. Gennemgå regelmæssigt brugerkonti, og deaktiver de unødvendige, og brug sporingsløsninger til at overvåge brug af konti. Kryptér kontobrugernavne og godkendelseslegitimationsoplysninger, både i transit og i dvale på enhedens lager. Sikkerhedskonsulenter kan hjælpe dig med at designe en omfattende udskrivningssikkerhedsplan for at minimere risici – og i nogle tilfælde kan de hjælpe dig med at håndtere sikkerhed, inklusive kontoovervågning og kontrol.

CSC 17: Vurdering af sikkerhedsfærdigheder og passende uddannelse til at udfylde hullerne

Foranstaltning – Identificer den specifikke viden, færdighed og evne til at understøtte forsvaret af virksomheden; udvikl og aktivér en integreret plan til at tilgå, identificere og afhjælpe hullerne gennem politik, organisationsplanlægning, uddannelse og programmer, der skaber bevidsthed for alle funktionelle roller i organisationen.

Anbefaling – Udskrivningssikkerhedskonsulenter har specialiseret viden, der hjælper dig med at vurdere dine sikkerhedsricisi, udvikle en omfattende sikkerhedspolitik og -plan samt implementere processer og teknologianbefalinger. Nogle sikkerhedstjenester kan endog administrere udskrivningssikkerhed og overholdelse af krav for dig.

CSC 18: Programsoftwaresikkerhed

Foranstaltning – Administrer sikkerhedslivscyklus på al in-house-udviklet og købt software for at forhindre, opdage og korrigere sikkerhedssvagheder.

Anbefaling – Du skal altid overholde bedste praksis for sikker udvikling af alle udviklede udskrivningsløsninger. Vælg softwareløsninger, der er blevet underskrevet og godkendt som ægte.

CSC 19: Respons på og håndtering af hændelser

Foranstaltning – Beskyt organisationens oplysninger såvel som omdømme ved at udvikle og implementere en struktur for hændelsessvartid (f.eks. planer, definerede roller, uddannelse, kommunikation og administrationstilsyn).

Anbefaling – Bekræft, at dit udskrivningsmiljø er omfattet af din hændelsessvartidsplan.

CSC 20: Indtrængningstest og alarm-øvelser

Foranstaltning – Test den overordnede styrke i hele organisations forsvar (teknologi, processer og personer) ved at simulere de mål og de aktioner, en hacker vil udføre.

Anbefaling – Inkluder dit udskrivningsmiljø, når du kører indtrængningstest. Vurder regelmæssigt dit udskrivningsmiljø for svagheder, og opdater din sikkerhedsplan for at adressere disse svagheder.

Tag det næste skridt

Implementering af anbefalingerne i denne hvidbog hjælper dig med at styrke udskrivningssikkerheden og overholde lovmæssige krav. Brug for hjælp? Udskrivningssikkerhedsadministration og rådgivningstjenester kan hjælpe dig med at udvikle en plan og installere processer og teknologi til at forbedre sikkerheden på dine udskrivningsenheder, data og dokumenter.

Bilag A: HP-udskrivningssikkerhedsfunktioner, -løsninger og -tjenester

De indbyggede sikkerhedsfunktioner på HP-enheder kan sammen med førende softwareløsninger i branchen hjælpe dig til at overholde lovmæssige krav og beskytte dine forretningsoplysninger mod sikkerhedstrusler.

Indbyggede sikkerhedsfunktioner på HP Enterprise-printere og -MFP'er beskytter mod malware og kan automatisk opdage et angreb og gendanne sig selv efter angreb. Kun HP's udskrivningssikkerhed kan under drift opdage, overvåge og validere software, så trusler bliver stoppet i det øjeblik, de starter.[4] (Hjælper med at opfylde i CSC 2, 4, 6 og 8). hp.com/go/PrintersThatProtect

HP Access Control-løsninger leverer en række godkendelsesmetoder og rollebaserede adgangskontroller for at hjælpe med at reducere potentielle brud på sikkerheden samt jobsporing og -regnskab. (Hjælper med at opfylde CSC 5, 7, 10, 12, 13, 14, 15 og 16). hp.com/go/hpac

Kryptering og **HP JetAdvantage Workflow Solutions** beskytter data både, når det bliver lagret på HP Enterprise-enheder og i transit til og fra udskrivningsenheder og til skyen. (Hjælper med at opfylde CSC 12 og 13). hp.com/go/upd, hp.com/go/documentmanagement

HP's pull-udskrivningsløsninger beskytter fortrolige oplysninger ved at lagre udskrivningsjob på en beskyttet server, i skyen eller på din pc. Brugere godkender på det sted, hvor de ønsker at udskrive, og foretager en pull-udskrivning af jobbet. (Hjælper med at opfylde CSC 10, 13 og 14). hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect giver mobile brugere nem adgang til at udskrive fra smartphones og tablet-pc'er, samtidig med at du bevarer den sikkerhed og administrative kontrol, du har behov for. (Hjælper med at opfylde CSC 12 og 15). hp.com/go/JetAdvantageConnect

HP-printerhændelsesdata kan sendes til SIEM-værktøjer, såsom ArcSight, Splunk eller SIEMonster. Dit sikkerhedshold kan nemt se printerslutpunkter som en del af det bredere it-økosystem og kan foretage korrigerende handlinger. (Hjælper med at opfylde CSC 4 og 6).

HP JetAdvantage Security Manager er branchens eneste politikbaserede overholdelsesværktøj til udskrivningssikkerhed.[5] Det hjælper dig med at etablere en sikkerhedspolitik på tværs af flåden, automatisere afhjælpning af enhedsindstillinger samt installere og forny unikke certifikater, samtidig med at du får rapporter, der beviser overholdelse af krav. Løsningens Instant-on-sikkerhedsfunktion konfigurerer automatisk nye enheder, når de bliver sluttet til netværket eller efter en genstart. (Hjælper med at opfylde CSC 1, 2, 3, 4, 5, 6, 8, 9, 11 og 15). hp.com/go/securitymanager

HP Secure Managed Print Services giver den stærkeste og mest omfattende udskrivningssikkerhedsbeskyttelse i branchen.[6] Udskrivningssikkerhed kan være kompliceret. Lad HP administrere din udskrivningssikkerhed med alt fra at styrke enheder til avancerede sikkerhedsløsninger, der adresserer personer, processer og overholdelse af krav. (Hjælper med at opfylde CSC 2, 3, 12, 16, 17, 18 og 19). hp.com/go/SecureMPS

HP Print Security Professional Services leverer sikkerhedseksperter til at gennemgå dit udskrivningsmiljø, proaktivt etablere sikkerhedspolitikker og holde din sikkerhedsplan opdateret. Vi kan endog administrere overholdelse af standarder for udskrivningssikkerhed for dig. (Hjælper med at opfylde CSC 2, 3, 12, 16, 17 og 19). hp.com/go/SecureMPS

Noter

[1] Ponemon-undersøgelse sponsoreret af HPE, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation", 2016.

[2] The 2016 Year End Data Breach QuickView report fra RiskBased Security, januar 2017.

[3] 26,2 % af respondenter i analysen havde oplevet et signifikant brud på sikkerheden, der krævede afhjælpning, og over 26,1 % af disse tilfælde involverede udskrivning. IDC, "Analyse af it- og udskrivningssikkerhed" IDC #US40612015, september 2015.

[4] Gælder for enheder i HP Enterprise-klassen introduceret i begyndelsen af 2015 og baseret på HP's gennemgang af offentliggjorte sikkerhedsfunktioner på konkurrerende printere i klassen. Kun HP tilbyder en kombination af sikkerhedsfunktioner, der kontrollerer integriteten helt ned til BIOS-niveau med selvreparerende funktioner. Aktivering af sikkerhedsfunktioner kræver muligvis opdatering af en FutureSmart-servicepakke. Se en liste over kompatible produkter på hp.com/go/PrintersThatProtect. Få flere oplysninger på hp.com/go/printersecurityclaims.

[5] HP JetAdvantage Security Manager skal købes separat. Du kan få flere oplysninger på: hp.com/go/securitymanager. Udsagn om konkurrencedygtighed baseret på intern HP-analyse af konkurrenternes udbud (Sammenligning af enhedssikkerhed, januar 2015) og løsningsrapport om HP JetAdvantage Security Manager 2.1 fra Buyers Laboratory LLC, februar 2015.

[6] Inkluderer enheds-, data- og dokumentsikkerhed fra førende leverandører af administrerede udskrivningstjenester. Baseret på HP-gennemgang fra 2015-2016 af offentligt tilgængelig information om sikkerhedstjenester, sikkerhed og administration af software og enheder med indbyggede sikkerhedsfunktioner og deres konkurrerende printere i klassen. Du finder flere oplysninger på hp.com/go/MPSsecurityclaims eller hp.com/go/mps.

Modtag opdateringer
hp.com/go/getupdated

Del med kolleger

© Copyright 2016-2017 HP Development Company, L.P. Oplysningerne heri kan ændres uden varsel. De eneste garantier for HP-produkter og -tjenester er angivet i de udtrykkelige garantierklæringer, der følger med sådanne produkter og tjenester. Intet heri må fortolkes som en yderligere garanti. HP er ikke ansvarlig for tekniske eller redaktionelle fejl eller udeladelser heri.

4AA6-8821DAE, Juni 2017, rev. 1