IDC
Analyze the Future

I D C M A R K T S P O T L I G H T

Beveiliging van de printinfrastructuur is essentieel voor digitale transformatie

December 2016

Door Robert Palmer, IDC Research Director, Imaging-, printing- en documentoplossingen

Gesponsord door HP Inc.

Het IT-beveiligingsplan van een onderneming is een eerste prioriteit voor goede bescherming en de juiste afweer tegen potentiële bedreigingen en schendingen. Printbeveiliging moet deel uitmaken van dit plan, met name in het tijdperk van het 3e computerplatform (mobiliteit, cloud, big data en social media). In ieder beveiligingsplan voor de zakelijke printomgeving moeten oplossingen en diensten worden opgenomen voor apparatuur- en databeveiliging. In dit artikel wordt het belang uiteengezet van het beveiligen van de print- en documentinfrastructuur en wordt beschreven welke rol managed printservices daarbij kunnen spelen.

Inleiding

De uitdagingen van IT-beveiliging en dataprivacy staan al meer dan 10 jaar bovenaan de prioriteitenlijst van CIO's en IT-managers. Uit eigen onderzoek van IDC blijkt dat beveiliging een zeer hoge prioriteit heeft voor de meeste bedrijven en slechts iets lager op de lijst staat dan een ander belangrijk bedrijfsinitiatief: digitale transformatie. Beide worden beschouwd als onderscheidende factoren, dus het is belangrijk om te begrijpen hoezeer digitale transformatie en beveiliging met elkaar verbonden zijn.

Ondernemingen die hun IT-infrastructuur beveiligen, worden met een scala aan bedreigingen geconfronteerd. De meeste technologisch onderlegde bedrijven beschouwen beveiliging als topprioriteit. Ze richten zich op de bescherming van het netwerk tegen aanvallen van buitenaf, de beveiliging van netwerkapparaten, toegangsbeheer voor verbonden devices en het voorkomen van het uitlekken van vertrouwelijke informatie.

Op het eerste gezicht is duidelijk dat al deze zaken draaien om de bescherming van het belangrijkste bezit van een onderneming: bedrijfsinformatie en klantgegevens. Bedrijven geven miljarden dollars uit aan software voor documentbeheer en Enterprise Content Management (ECM) en investeren fors in systemen waarmee ze controle krijgen over bedrijfskritische content. De problemen worden nog vergroot door de aanhoudende verschuiving naar mobiliteit en cloud computing. Kenniswerkers rekenen tegenwoordig op 24x7 toegang tot informatie en daartoe moet content binnen en buiten de firewall van het bedrijf vrij kunnen bewegen.

Opmerkelijk genoeg bevindt de print- en documentinfrastructuur van een bedrijf zich precies op het snijvlak van digitale transformatie en IT-beveiliging. Toch zijn de meeste bedrijven zich niet bewust van de kwetsbaarheden in de beveiliging van hun bestaande print- en documentomgeving. De kern van het probleem is de rol die slimme MFP's spelen. Deze hebben zich ontwikkeld tot intelligente verwerkingshubs die fungeren als in- en uitgang voor bedrijfsgegevens, ongeacht of deze in een apparaat, in het bedrijfsnetwerk, op papier of in de cloud zijn opgeslagen.

Een onzichtbare bedreiging die niet wordt beheerd

Als verbonden maar niet-beheerd apparaat vormt de MFP een potentieel beveiligingsrisico. De MFP kan echter ook worden gebruikt als eerstelijnsapparaat om de netwerktoegang te beveiligen, data-beveiliging te beheren en de toegang tot informatie te beschermen.

Volgens onderzoek van IDC uit 2015 naar *'User Perspectives on Print Security'* , hanteert meer dan 30% van de bedrijven geen beveiligingsbeleid voor toegangsbeheer en controle van de gebruikers-rechten voor op het netwerk aangesloten printers en MFP's. Tegelijkertijd gaf meer dan de helft van de ondervraagden aan zich veel zorgen te maken over ongeautoriseerd gebruik van kopieer-apparaten of MFP's.

Wanneer bedrijven hun eigen actuele IT-beveiligingspraktijk beoordelen, zijn vergelijkbare inconsistenties waarneembaar. Volgens het IDC-onderzoek *MaturityScape Benchmark: Print Security in the United States* uit 2016 zei meer dan 70% van de ondervraagden dat printbeveiliging veel invloed heeft op de printers en MFP's die zij kopen of leasen. Verrassend genoeg was het percentage dat aangaf printbeveiliging "heel belangrijk" te vinden slechts 26%. Dat is minder dan degenen zich zorgen maakten over algehele IT-beveiliging.

Veel beveiligings- en IT-managers gaan ervan uit dat de systemen die zij hebben geïnstalleerd om het netwerk te beveiligen ook andere aangesloten randapparaten zullen beschermen. Maar beveiliging aan de rand van het netwerk brokkelt af en ieder apparaat dat met het netwerk verbonden is vormt nu een endpointbeveiligingsrisico. Dat geldt ook voor printers en MFP's.

De dreiging is reëel: potentiële inbreuken zijn het gevolg van kwaadaardige aanvallen die een netwerkprinter of -MFP als ingang gebruiken of van onzorgvuldig gebruik van apparatuur door werknemers. De printomgeving is uniek, omdat deze gebruikt wordt voor het beheren van data, documenten en informatie in digitaal formaat én op papier. Bedrijfskritische informatie wordt daardoor op verschillende manieren kwetsbaar voor uitlekken. Wanneer de printomgeving niet wordt beveiligd als onderdeel van een totale IT-strategie, is een onderneming net zo kwetsbaar als wanneer de IT-omgeving helemaal niet beveiligd zou zijn.

Het resultaat van een inbreuk op de beveiliging van de print- en documentinfrastructuur is hetzelfde als dat van elke andere schending: hoge kosten voor downtime om de inbreuk op te sporen en te verhelpen, boetes in verband met corporate governance en compliance met wet- en regelgeving, verlies van klanten of reputatieschade.

Veilige printservices

De problemen van print- en documentbeveiliging zijn duidelijk, maar het blijkt voor veel bedrijven lastig om een veilige printstrategie te ontwikkelen. Strijdige belangen in een onderneming vormen daarbij een hinderpaal. Apparatuurbeveiliging valt meestal onder verantwoordelijkheid van IT, met inbreng van de IT-afdeling, de beveiligingsmanager, de helpdesk, endpointbeveiliging en netwerk-beveiliging. Ook faciliteitenbeheer is vaak betrokken bij de discussie over beveiliging van printers en MFP's.

Contentbeveiliging wordt echter vaak geassocieerd met problemen rond regelgeving, met belanghebbenden in corporate risk en governance. Vertegenwoordigers van ERP-applicaties, databaseclusters, contentmanagement en andere line of business (LOB)-managers kunnen ook een belang hebben. Te vaak wordt de beveiliging van content en printers apart aangepakt, met een gebrek aan integratie en meer lacunes in de beveiliging tot gevolg. Tegelijkertijd zijn bedrijven niet op de hoogte van de vele veilige printoplossingen en professionele diensten die op de markt beschikbaar zijn.

MPS (managed print services) kan bijvoorbeeld een belangrijke rol spelen in de verbetering van print- en documentbeveiliging. Veel bedrijven hebben wel een contract met een MPS-leverancier om hun printinfrastructuur te optimaliseren en efficiënter te maken en de printkosten te reduceren, maar print- en contentbeveiliging wordt in deze printservicecontracten vaak over het hoofd gezien. Tegenwoordig hebben sommige MPS-leveranciers de mogelijkheid, de tools en de resources om bedrijven te helpen actuele beveiligingsrisico's te identificeren en te prioriteren. Bij dergelijke processen moet eerst een beveiligingsevaluatie worden gemaakt om lacunes in de huidige apparaat- en content-infrastructuur op te sporen. Daarna kan het bedrijf samen met de serviceleverancier veilige managed printservices ontwikkelen en implementeren om de bestaande kwetsbaarheden te verhelpen, de documentinfrastructuur te versterken en toekomstige veiligheidsrisico's te beperken.

De MPS-leverancier is ook als enige in staat om de verschillende belanghebbenden op een lijn te brengen en printservices op contractbasis te leveren aan alle afdelingen en divisies, wat essentieel is voor het hanteren van een holistische aanpak van apparaat- en contentbeveiliging. Deze benadering biedt ook voordelen bij het ontwikkelen van een beveiligingsplan dat de digitale transformatiestrategie van het bedrijf ondersteunt. Veilige printservices kunnen variëren van basisbeveiliging ter bescherming van apparatuur en data tot meer geavanceerde maatregelen, die minder eenvoudig te implementeren zijn maar een betere apparaat- en contentbescherming bieden.

Conclusie: Van reactief naar proactief

De conclusie is dat de print- en documentinfrastructuur onvoldoende aandacht krijgt in vergelijking met andere bedreigingen van de netwerk- en cyberbeveiliging. Inbreuken leiden tot angst en onzekerheid en hebben een grote impact op de operationele kosten, de bedrijfsactiviteiten en de reputatie van een onderneming.

Ondernemingen moeten proactief maatregelen nemen om beveiligingsproblemen in de print- en documentinfrastructuur op te lossen, met de MPS-leverancier als belangrijke partner. Wanneer u een printservicesleverancier zoekt, kies dan voor degene die essentiële kennis bezit en ervaring heeft in het evalueren en verhelpen van risico's.

Kies bovendien voor een partner met hardware en oplossingen die gebouwd zijn rond een beveiligingsecosysteem dat de volgende kwetsbaarheden in de documentinfrastructuur kan aanpakken:

- Gebruikersverificatie en -autorisatie
- Apparaatbeheer
- Bescherming van apparatuur tegen malware
- Firmware-updates en wachtwoordbeheer
- Contentbeveiliging, privacy en datamigratie
- Mogelijkheden om menselijke fouten bij installatie, configuratie en gebruik van apparatuur te voorkomen

MPS-oplossingen moeten ontworpen worden voor integratie met documentmanagement- en ECM-systemen van derde partijen voor extra bescherming en hulp bij governance- en compliance-vereisten.

Door een holistische aanpak kunnen bedrijven lacunes in de beveiliging dichten en de bescherming van de print- en documentomgeving, waarschijnlijk de zwakste schakel in de beveiliging van het bedrijf, versterken.

O V E R D E Z E P U B L I C A T I E

Deze publicatie is geproduceerd door IDC Custom Solutions. De hierin gepresenteerde mening, analyse en onderzoeksresultaten zijn gedestilleerd uit meer gedetailleerd onderzoek en analyses die onafhankelijk door IDC zijn uitgevoerd en gepubliceerd, tenzij de naam van een specifieke sponsor wordt vermeld. IDC Custom Solutions maakt informatie van IDC beschikbaar in diverse formaten, voor distributie door verschillende bedrijven. Een licentie voor het distribueren van IDC-content houdt geen aanbeveling van, of mening over, de licentiehouder in.

Bezoek www.idc.com voor meer informatie over IDC. Kijk voor meer informatie over IDC Custom Solutions op http://www.idc.com/prodserv/custom_solutions/index.jsp.

Wereldwijd hoofdkantoor: 5 Speen Street, Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com