IDC
Analyze the Future

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

Sikring af udskrivningsinfrastrukturen er kritisk for digital transformation

December 2016

Af Robert Palmer, IDC Research Director, Imaging, Printing and Document Solutions

Sponsoreret af HP Inc.

En organisations it-sikkerhedsplan har åbenlyst høj prioritet i forbindelse med at sikre passende beskyttelse og reaktion på potentielle trusler og sikkerhedsbrud. Printersikkerhed skal være en del af denne plan, især i denne æra med nye computerplatforme (mobilitet, cloud, big data og sociale medier). En del af enhver overordnet plan, der varetager sikkerheden i organisationens printermiljø, bør således omfatte løsninger og tjenester til varetagelse af både enheds- og datasikkerhed. I dette dokument undersøges vigtigheden af at sikre udskrivnings- og dokumentinfrastrukturen og den rolle, som administrerede printertjenester kan spille for at nå dette mål.

Indledning

Spørgsmål relateret til sikkerhed og datasikkerhed har været placeret fast øverst på listen for CIO'er og it-chefer i over et årti. IDC's egen forskning viser, at sikkerhed nu har fået høj prioritet for et flertal af virksomheder, dog en anelse lavere end et andet nøglevirksomhedsinitiativ: Digital transformation. Selvom begge betragtes som nøgledifferentiatorer i virksomheder, er det vigtigt at forstå, hvordan digital transformation og sikkerhed er tæt forbundet.

Organisationer står over for en bred vifte af trusler med hensyn til at sikre deres it-infrastruktur. De fleste teknologiske organisationer har givet sikkerheden høj prioritet ved at fokusere på problemer som beskyttelse af netværket mod eksterne angreb, sikring af netværksenheder, styring af adgang til tilsluttede enheder og forebyggelse af offentliggørelse af fortrolige data.

På overfladen er det let at se, hvordan alle disse problemer drejer sig om behovet for at beskytte organisationens mest værdsatte aktiver: Forretningsoplysninger og kundedata. Virksomheder bruger millioner af dollar på dokumenthåndtering og ECM-software (Enterprise Content Management-software) og foretager betydelige investeringer i systemer for at få kontrol over forretningskritisk indhold. Udfordringen vanskeliggøres af den stadige bevægelse hen mod mobilitet og cloud computing. Nutidens vidensarbejdere kræver adgang til information døgnet rundt alle ugens dage, hvilket betyder, at indholdet skal bevæge sig frit både inden og uden for virksomhedens firewall.

Interessant nok er en organisations udskrivnings- og dokumentinfrastruktur placeret, hvor den digitale transformation og it-sikkerheden mødes. Ikke desto mindre lykkes det ikke de fleste virksomheder at genkende de sikkerhedsrisici, som er forbundet med deres eksisterende udskrivnings- og dokumentmiljø. Kernen i problemet er den smarte MFP, der er blevet et intelligent center for håndtering af virksomhedsdata og fungerer som en til- og frakørselsrampe for forretningsoplysninger, uanset om de er gemt i enheden, på virksomhedens netværk, på papir eller i skyen.

En uset trussel, der ikke tages hånd om

Den netværksforbundne MFP er en potentiel sikkerhedsrisiko ligesom andre ikke-administrerede tilsluttede enheder. MFP'en kan imidlertid også udnyttes som et frontlinjeaktiv til sikring af netværksadgang, styring af datasikkerhed og beskyttelse af adgang til information.

Ifølge undersøgelser fra IDC's *User Perspectives on Print Security, 2015*, har mere end 30 % af alle organisationer ingen sikkerhedspolitikker for styring af adgang til og kontrol af brugsrettigheder for printere og MFP'er, der er placeret på netværket. Samtidig angiver over halvdelen af de undersøgte respondenter et højt niveau af bekymring vedrørende uautoriseret brug af kopimaskiner eller MFP'er.

Der er lignende uoverensstemmelser, når man kigger på, hvordan virksomheder ser deres nuværende it-sikkerhedspraksis. Ifølge IDC's *MaturityScape Benchmark: Print Security in the United States, 2016,* siger over 70 % af de undersøgte respondenter, at udskrivningssikkerhed har stor indflydelse på, hvilke printere og MFP'er de køber eller lejer. Overraskende nok var antallet af respondenter, der indikerede, at printersikkerhed var "meget vigtig", mindst 26 % mindre end antallet af dem, der var bekymrede for den overordnede it-sikkerhed.

Mange sikkerheds- og it-chefer har antaget, at systemer, som er etableret for at beskytte netværket, ville blive udvidet til andre tilsluttede eksterne enheder. Men sikkerheden omkring netværkets perimeter falder fra hinanden, og alle enheder, der er tilsluttet netværket, udgør nu en sikkerhedsrisiko – også printere og MFP'er.

Truslen er reel med potentielle sikkerhedsbrud enten på grund af ondsindede angreb ved hjælp af en netværksprinter eller MFP som indgangspunkt eller medarbejdernes utilsigtede, men uforsigtige brug af enheder. Printermiljøet er unikt, fordi det udnyttes specifikt til at håndtere data, dokumenter og informationer i både digitalt format og papirformat, så forretningskritisk indhold er udsat og sårbart på en række måder. Hvis man undlader at sikre printermiljøet som en del af en overordnet it-strategi, vil en organisation være lige så sårbar, som den ville være uden nogen it-sikkerhed overhovedet.

Slutresultatet af et sikkerhedsbrud på udskrivnings- og dokumentinfrastrukturen er det samme som for enhver anden sikkerhedsmangel: Omfattende omkostninger i forbindelse med nedetid for at identificere og afhjælpe et sikkerhedsbrud, bøder i forbindelse med virksomhedsledelse og overholdelse af lovgivningen, mistede kunder eller andre skader på virksomhedens omdømme.

Sikre udskrivningstjenester

Udfordringerne i forbindelse med udskrivnings- og dokumentsikkerhed er lette at identificere, men udviklingen af en sikker udskrivningsstrategi har vist sig svær for mange virksomheder. Et problem vedrører de forskellige interessenter i organisationen. Enhedssikkerhed har tendens til at være inkluderet i it-funktionen og omfatter typisk it-afdelingen, sikkerhedsadministratoren, helpdesk, endepunktssikkerhed og netværkssikkerhed. Derudover involverer enhver diskussion vedrørende printersikkerhed og MFP-sikkerhed ofte facilitetsstyring.

Indholdssikkerhed ses derimod ofte i forbindelse med problemer vedrørende lovoverholdelse, og interessenterne er som regel en del af virksomhedernes ledelse. Medarbejdere, der beskæftiger sig med ERP-applikationer, databaseklynger og indholdsstyring samt andre LOB-chefer kan også inddrages. Ofte håndteres sikkerhed for indhold og printere separat, hvilket medfører manglende integration og større huller i sikkerheden. Samtidig er virksomhederne ofte uvidende om de forskellige sikre printerløsninger og professionelle tjenester, der er tilgængelige på markedet.

Dette er et område, hvor administrerede udskrivningstjenester (MPS) kan spille en vigtig rolle for at fremme udskrivnings- og dokumentsikkerheden. Selvom mange virksomheder har indgået kontrakt med en MPS-udbyder for at optimere deres udskrivningsinfrastruktur med henblik på at fremme effektiviteten og reducere produktionsomkostningerne, er udskrivnings- og indholdssikkerhed i vid

udstrækning blevet overset i de fleste kontraktlige udskrivningstjenester. I dag har nogle MPS-udbydere kapacitet, værktøjer og ressourcer til at hjælpe virksomheder med at identificere og prioritere de nuværende sikkerhedstrusler. En del af denne proces kan være en forudgående sikkerhedsvurdering, hvilket er afgørende for at identificere huller i den nuværende enheds- og indholdsinfrastruktur. Virksomheder kan derefter arbejde sammen med tjenesteudbyderen om at udvikle og implementere sikre administrerede udskrivningstjenester for at afhjælpe aktuelle sårbarheder, styrke dokumentinfrastrukturen og mindske fremtidige sikkerhedsrisici.

MPS-udbyderen er også yderst dygtig til at samle forskellige interessenter og levere kontraktlige udskrivningstjenester på tværs af afdelinger og forretningsområder, hvilket er afgørende for at implementere en holistisk tilgang til enheds- og indholdssikkerhed. Denne tilgang er også gavnlig for at udvikle en sikkerhedsplan, der udvider sig med organisationens egen digitale transformationsstrategi. Sikre udskrivningstjenester kan variere fra basissikkerhed til beskyttelse af udstyr og data til mere avancerede foranstaltninger, der er betydeligt mere komplekse i deres implementering og giver et højere niveau af enhedssikkerhed og indholdsbeskyttelse.

Konklusion: Fra reaktiv til proaktiv

Når alt kommer til alt, har udskrivnings- og dokumentinfrastrukturen ikke fået samme opmærksomhed som andre trusler inden for netværks- og cybersikkerhed. Sikkerhedsbrud skaber frygt og usikkerhed, og konsekvenserne for driftsomkostninger, jobpræstationer og virksomhedernes omdømme kan være alvorlige.

Organisationer skal tage proaktive skridt for at løse sikkerhedsproblemer i udskrivnings- og dokumentinfrastrukturen, og MPS-udbyderen bør ses som en vigtig partner i denne indsats. Når du søger efter udskrivningstjenester, skal du overveje dem, der udviser kernekompetencer i vurdering af trusselsniveau og afhjælpning.

Derudover skal du vælge partnere med hardware og løsninger, der er bygget op omkring et sikkerhedsøkosystem og kan løse følgende sårbarheder i dokumentinfrastrukturen:

- Brugerbekræftelse og -godkendelse
- Enhedsstyring
- Beskyttelse af enheder mod malware
- Firmwareopdateringer og adgangskodehåndtering
- Indholdssikkerhed, beskyttelse af personlige oplysninger og dataintegritet
- Udfordringer ved den menneskelige faktor i forbindelse med installation, konfiguration og brug af udstyr

MPS-løsninger bør også udformes, så de kan integreres med tredjepartssystemer til dokumenthåndtering og ECM-systemer for at yde yderligere beskyttelse og hjælpe med styring og overholdelse af lovkrav.

Gennem en holistisk tilgang kan virksomheder begynde at lukke hullerne i sikkerheden og styrke beskyttelsen af udskrivnings- og dokumentmiljøet, hvilket sandsynligvis er din organisations svageste sikkerhedsled.

OM DENNE PUBLIKATION

Denne publikation blev produceret af IDC Custom Solutions. Holdningen, analysen og forskningsresultaterne, der præsenteres her, er hentet fra mere detaljeret forskning og analyse, der er udført uafhængigt af og offentliggjort af IDC, medmindre der er anført specifik sponsorering. IDC Custom Solutions gør IDC-indhold tilgængeligt i en bred vifte af formater til distribution via forskellige virksomheder. En licens til at distribuere IDC-indhold er ikke udtryk for nogen form for godkendelse af eller holdning til licenshaveren.

OPHAVSRET OG BEGRÆNSNINGER

Gå til www.idc.com for at få yderligere oplysninger om IDC. Gå til http://www.idc.com/prodserv/custom_solutions/index.jsp. for at få yderligere oplysninger om IDC Custom Solutions.

Det globale hovedkontor: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com