Derfor har alle virksomheder brug for en intelligent udskrivningsstrategi

Alle virksomheder har brug for en strategi til deres udskriftstjenester for sikkerhedens og produktivitetens skyld. HP's sikkerhedsrådgivere for udskrivning, Jason O'Keefe og Michael Howard, forklarer hvorfor.

Learn more

"De fleste virksomheder tror ikke, at de har brug for sikkerhed til deres printerinfrastruktur, så printerne er meget lavt placeret på deres prioriteringsliste for sikkerhed"

Jason O'Keefe,
HP Print Security Advisor

Printere, som er sluttet til netværk, er mere usikre, end de fleste organisationer er klar over. Med et stigende antal sikkerhedstrusler, som kan være katastrofale, har virksomheder i alle størrelser brug for udskrivningsstrategier for at beskytte deres organisationer og minimere risikoen. Basis for udformningen af en stærk strategi for mange virksomheder er at arbejde sammen med en udbyder af administrerede udskriftstjenester, der kan identificere og afhjælpe sårbarheder i sikkerheden samt løse problemer (ligesom vedligeholdelse af udstyr), så udskrivning aldrig kommer i vejen for produktiviteten.

Håndtering af printersårbarhed

Ifølge en undersøgelse blandt mere end 2000 globale it-sikkerhedseksperter, som blev udført af Ponemon Institute, erkender 60 % af respondenterne, at et brud på datasikkerheden på en printer, som er sluttet til netværket, sandsynligvis har fundet sted, og de fleste respondenter forudser et brud på datasikkerheden på grund af usikre printere, der er sluttet til netværket, inden for de næste 12 måneder.

Kun 34 % af respondenterne siger, at deres organisation har en proces til begrænsning af adgang til højrisikoprintere, inkl. udskrevne, fysiske dokumenter. Disse iøjnefaldende huller i sikkerheden kan medføre, at små og mellemstore virksomheder i særdeleshed er i risikozonen for angreb, der i bedste fald er dyre, men i værste fald kan lamme virksomheden.

Jason O'Keefe, som er HP's sikkerhedsrådgiver for udskrivning, udtaler, at de fleste organisationer undervurderer, hvor sårbare de er på grund af deres printerinfrastruktur. "De fleste virksomheder tror ikke, at de har brug for sikkerhed til deres printerinfrastruktur, så printerne er meget lavt placeret på deres prioriteringsliste for sikkerhed", udtaler han. "Vi præsenterer vores struktur, der har op til 200 kontrolfunktioner, som vi gennemgår for sårbarheder på tværs af printerinfrastrukturen. Pludselig får de øjnene op, og piben får en anden lyd. Den oprindelige skepticisme bliver til vantro og chok, som så åbner op for en meget ærlig og livlig diskussion."

En god udskrivningsstrategi bør starte med en evaluering af sårbarheder. Ifølge Michael Howard, som er HP's øverste sikkerhedsrådgiver, kan de fleste printerbaserede sikkerhedsproblemer koges ned til fire faktorer: forældet teknologi, manglende korrekt implementering af sikkerhedskontrol, heterogene leverandørmiljøer og printermiljøer, der ikke administreres.

Vidste du, at den gennemsnitlige organisation har omkring seks brugere pr. printer? Mens stationære og bærbare computere kan låses, når de ikke er i brug, følger printere ikke de samme protokoller, hvilket giver en sårbarhed for hver sjette bruger. "Mange sikkerhedsmedarbejdere ville ikke kunne fortælle dig, hvor mange printerenheder der findes i deres miljø. Der kunne være 5.000 enheder – alle sammen åbne", udtaler Howard. "Når man tænker på, hvor

Derfor har alle virksomheder brug for en intelligent udskrivningsstrategi

vigtig udskrivning er i de fleste organisationer, er manglen på proaktiv sikkerhed chokerende og skræmmende."

Derfor spiller udskrivningsstrategier en vigtig rolle

En smart udskrivningsstrategi låser printere (ligesom med computere), begrænser de administrative rettigheder, implementerer retningslinjer for brugernavn og adgangskode og tilbyder overvågning. Dette er nøglen til at skabe gennemsigtighed, sporbarhed og ansvarlighed.

"Gennemsigtighed er afgørende", udtaler O'Keefe. "Jeg vil også fremhæve samarbejde som en nøgle til effektiv printersikkerhed. For at samle den omfattende viden, der kræves for at opnå robust sikkerhed, skal virksomheder nedbryde barriererne mellem udskriftsadministratorer, sikkerhedsmedarbejdere og internt revisionspersonale. Disse grupper skal være villige til at arbejde sammen for at sikre en vigtig del af netværket, som er blevet overset i årevis."

Endvidere kan organisationer afhjælpe deres printerbaserede sårbarheder ved:

- Konsekvent at opdatere deres firmware
- At reducere administrationen på tværs af printerinfrastrukturen
- At opgradere deres udskriftsdatabaser fra Express- til Enterprise-udgaver
- At implementere processer og dokumentation for at holde sikkerheden ensartet og målbar
- At tilbyde udskriftsadministratorer kurser i sikkerhedsbevidsthed.

"Printersikkerhed er ligesom virksomhedssikkerhed en løbende proces", udtaler Howard. "Derfor er det afgørende at sørge for en konstant forbedring gennem mere dybdegående vurderinger og ekspertrådgivning."

"Printersikkerhed er ligesom virksomhedssikkerhed en løbende proces", Michael Howard, HP Chief Security Advisor

Mere dybdegående, løbende vurderinger hænger sammen med vigtigheden af styring. I forbindelse med udskrivning bør styring omfatte administration af brugerkonti (hvem har adgang til printerinfrastrukturen), overholdelse af virksomhedspolitikker, risikostyring, sikkerhedsdokumentation og hændelseslogføring.

Styret eller ikke styret – det er spørgsmålet

En solid strategi kræver en lang række forskellige komponenter. For de fleste virksomheder, især små og mellemstore virksomheder, er det ikke en prioritet at lave og udføre denne type strategi selv. De vil hellere bruge deres tid og energi på at drive virksomheden. Et samarbejde med udbydere af printertjenester, der kan håndtere alle de små detaljer og levere det sikkerhedsniveau, som virksomhederne har brug for, er en kvalitetsløsning.

Det første trin til at skabe en intelligent udskrivningsstrategi er at stille spørgsmål. Hvilke printere er de rette for vores organisation? Skal vi købe blæk- eller laserprintere? Hvilke printerfunktioner har vi brug for? Det er nødvendigt at balancere pålidelighed, omkostninger og ydeevne for at kunne besvare disse spørgsmål

Dernæst skal virksomhederne tænke på sikkerhed, vedligeholdelse og support. Skal vi styre vores printere internt eller arbejde sammen med en udbyder? Dette spørgsmål fører til flere, som f.eks.: Er vores IT-team i stand til at håndtere printerproblemer? Vil det koste mere at håndtere printertjenester selv på længere sigt? For mindre virksomheder er svaret ofte ja.

Virksomheder, der vælger en administreret printertjeneste, bør tænke over, hvornår man skal overveje en udbyder, og hvilken udbyder de i så fald vil arbejde med. Dette kræver, at de stiller spørgsmål som: Hvilke tjenester har vi brug for? Hvad indgår i serviceniveauaftalen? Hvor meget vil det koste? Hvor hurtigt forventer vi at udvide vores printernetværk? Når vi vokser, hvordan skal udskrivningsstrategien så ændres?

Farerne ved usikre printere, der er sluttet til netværket, er tydelige, og virksomheder af alle størrelser skal gøre printertjenester til en del af deres overordnede tilgang til sikkerhed og produktivitet. Heldigvis findes der udbydere af løsninger, som kan klare det beskidte arbejde.

Learn more
hp.com

4AA7-1720DAE, November 2017