Waarom elk bedrijf een intelligente printservicestrategie nodig heeft

Elk bedrijf heeft een printservicestrategie nodig, zowel met het oog op de veiligheid als de productiviteit. Printbeveiligingsadviseurs Jason O'Keefe en Michael Howard van HP leggen uit waarom.

Meer informatie

"De meeste bedrijven denken dat ze geen beveiliging voor hun printinfrastructuur nodig hebben en daarom heeft printen een lage prioriteit in hun beveiligings-strategie"

Jason O'Keefe, HP Print Security Advisor

Printers die op het netwerk zijn aangesloten zijn minder veilig dan de meeste bedrijven denken. Gezien het groeiende aantal steeds riskantere bedreigingen kunnen grote én kleine bedrijven niet zonder een printservicestrategie om hun bedrijf te beschermen en risico's tot een minimum te beperken. De kern van een krachtige strategie is voor veel bedrijven de samenwerking met een leverancier van Managed Print Services die kwetsbaarheden in de beveiliging kan opsporen en verhelpen en problemen kan oplossen (bv. de apparatuur onderhouden), zodat het printen de productiviteit niet belemmert.

Maatregelen tegen onbeveiligde printers

In een enquête onder meer dan 2000 IT-beveiligers wereldwijd die werd gehouden door Ponemon Institute bekende 60 procent van de ondervraagden dat hun bedrijf vermoedelijk het doelwit was geweest van een dataschending via een op het netwerk aangesloten printer. De meeste respondenten verwachtten zelfs dat er in de komende 12 maanden een dataschending via onveilige netwerkprinters zou plaatsvinden.

Slechts 34 procent van de ondervraagden zei dat hun bedrijf een procedure heeft om toegang tot risicoprinters en de documenten daarop te beperken. Dergelijke grote beveiligingslacunes maken kleine en middelgrote bedrijven kwetsbaar voor aanvallen, die in het beste geval veel geld kosten en op zijn slechtst rampzalig zijn.

Jason O'Keefe, Print Security Advisor bij HP, legt uit dat de meeste bedrijven niet voldoende beseffen hoe kwetsbaar ze via hun printinfrastructuur zijn. "De meeste bedrijven denken dat ze geen beveiliging voor hun printinfrastructuur nodig hebben en daarom heeft printen een lage prioriteit in hun beveiligingsstrategie", zegt hij. "We presenteren ons framework met tot 200 controlemechanismen waarmee we de hele printinfrastructuur controleren op kwetsbare plekken. Plotseling komt het besef en krijgt men een totaal andere kijk op printerbeveiliging. De aanvankelijke scepsis slaat om in ongeloof en schrik, waarna de weg vrij is voor een openhartige, levendige discussie."

Een goede printservicestrategie begint met het evalueren van kwetsbaarheden. Volgens Michael Howard, Chief Security Advisor bij HP, zijn de meeste zwakke plekken in de printbeveiliging te herleiden tot vier factoren: verouderde technologie, ondeskundig geïmplementeerde beveiligingsmaat-regelen, heterogene vendoromgevingen en een niet-beheerde printomgeving.

Wist u dat in een gemiddeld bedrijf ongeveer zes personen een printer delen? Computers en laptops gaan op slot als ze niet worden gebruikt, maar dat geldt niet voor printers. Dit betekent dat er voor elke zes gebruikers een kwetsbare plek is. "Veel beveiligingsteams weten niet hoeveel printers er in hun bedrijf aanwezig zijn. Het kunnen wel 5000 apparaten zijn, die allemaal openstaan", zegt Howard. "Als u bedenkt hoe alomtegenwoordig printers in de meeste bedrijven zijn, is het gebrek aan beveiliging schokkend en beangstigend."

Waarom elk bedrijf een intelligente printservicestrategie nodig heeft

Waarom een printservicestrategie belangrijk is

Bij een intelligente printstrategie worden printers (net zoals computers) vergrendeld, worden beheerrechten ingeperkt, werkt men met gebruikersnamen en wachtwoorden en worden printers bewaakt. Dat is essentieel voor de zichtbaarheid, traceerbaarheid en verantwoording.

Bedrijven kunnen de kwetsbaarheden in hun printomgeving als volgt herstellen:

- Iedere firmware-update uitvoeren
- Het beheer van de printinfrastructuur reduceren
- Printdatabases upgraden van Express- naar Enterprise-edities
- Processen en documentatie implementeren om de beveiliging consistent en meetbaar te houden
- Bewustwording kweken en training geven aan printbeheerders.

"Printbeveiliging is, net zoals bedrijfsbeveiliging, een doorlopend proces"

Jason O'Keefe, HP Print Security Advisor

"Printbeveiliging is, net zoals bedrijfsbeveiliging, een doorlopend proces", zegt Howard. "We moeten voortdurend streven naar verbetering door intensieve evaluatie en deskundig advies." Diepgaande, continue evaluatie is een onderdeel van governance. Voor de printomgeving moet dit bestaan uit beheer van gebruikersaccounts (wie toegang heeft tot de printinfrastructuur), naleving van het bedrijfsbeleid, risicobeheer, veiligheidsdocumentatie en registratie van incidenten.

Wel of niet beheerd – dat is de vraag

Een solide strategie bestaat uit heel diverse componenten. Met name kleine en middelgrote bedrijven hebben geen tijd en mankracht om zelf een dergelijke strategie te ontwikkelen en uit te voeren. Ze willen hun tijd en energie liever besteden aan het runnen van hun bedrijf. Samenwerking met leveranciers van managed printing services, die alle details voor hun rekening nemen en het beveiligingsniveau bieden dat het bedrijf nodig heeft om soepel te draaien, is een uitstekende oplossing.

De eerste stap op weg naar een intelligente printstrategie is: vragen stellen. Welke printers zijn geschikt voor ons bedrijf? Moeten we kiezen voor inkt- of laserprinters? Welke printkenmerken hebben we nodig? Bij het beantwoorden van deze vragen is het zaak om de juiste balans te vinden tussen betrouwbaarheid, kosten en prestaties. Ook moeten bedrijven nadenken over beveiliging, onderhoud en ondersteuning. Moeten we onze printers intern beheren of daarvoor een leverancier inschakelen? Deze vraag roept weer andere vragen op, zoals: Is ons IT-team in staat om printerproblemen te verhelpen? Kost het op de lange termijn meer om printservices in eigen beheer te leveren? Voor kleine bedrijven luidt het antwoord op de laatste vraag vaak Ja.

Bedrijven die een managed printservice kiezen, moeten overwegen of ze naast een leverancier ook een contract willen. Dat roept vragen op zoals: Welke services hebben we nodig? Wat moet er in de servicelevelovereenkomst staan? Wat kost het? Hoe snel verwachten we ons printernetwerk te moeten uitbreiden? Moet onze printstrategie veranderen als we groeien?

De gevaren van niet-beveiligde op het netwerk aangesloten printers zijn duidelijk. Zowel grote als kleine bedrijven moeten printservices opnemen in hun strategie voor beveiliging en productiviteit. Gelukkig zijn er oplossingenleveranciers die u het werk uit handen kunnen nemen.

Meer informatie op:
hp.com

4AA7-1720NLE, november 2017