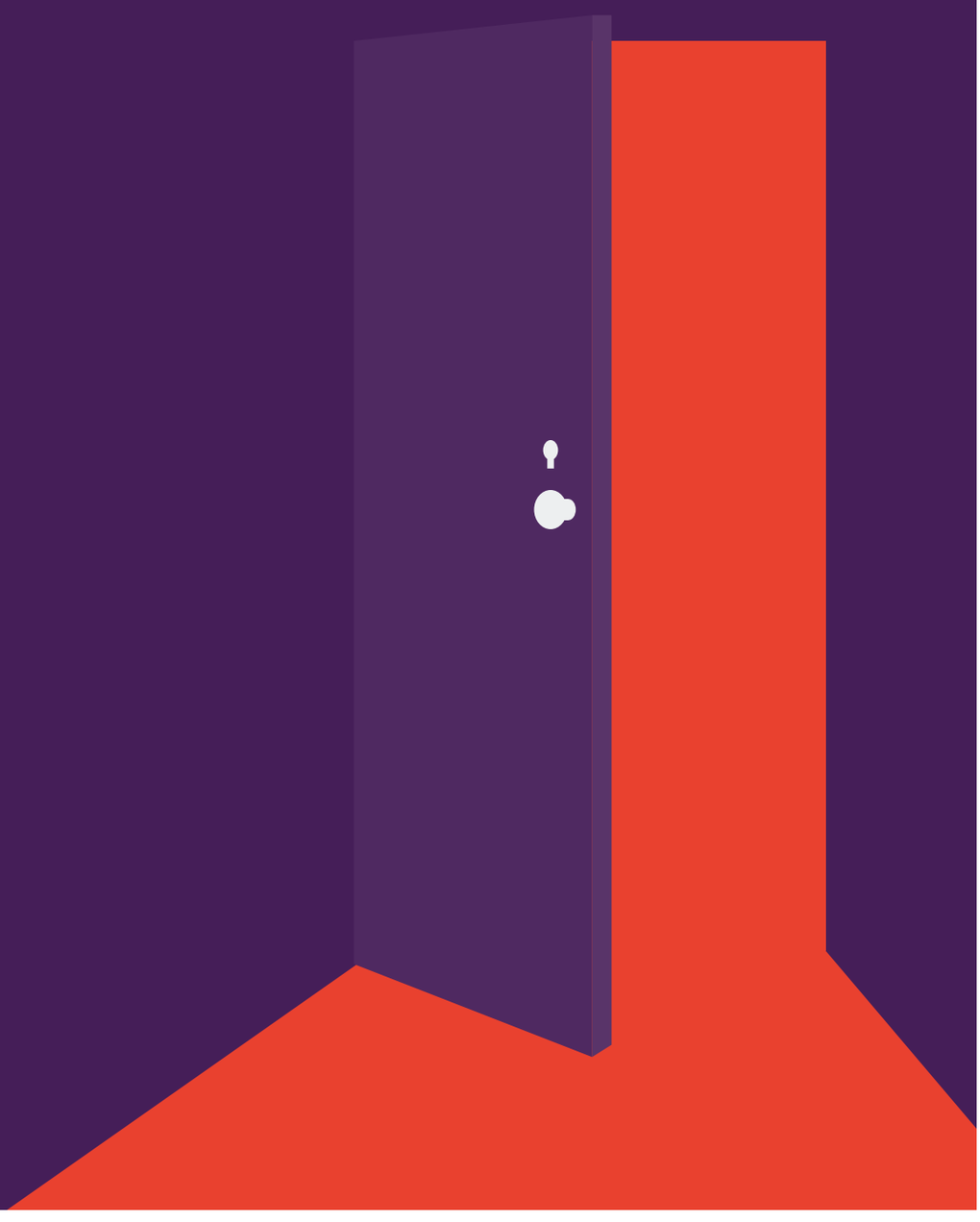
WHITEPAPER

UNCLOSED DOORS

UIT ONDERZOEK BLIJKT DAT PRINTERS KWETSBAAR ZIJN VOOR CYBERAANVALLEN

IT-teams richten zich vooral op andere endpoints en zien de beveiliging van bedrijfsprinters over het hoofd



Printers zijn een gemakkelijk doelwit: te veel netwerkprinters zijn onbeperkt toegankelijk en onvoldoende beveiligd.

Maar de dreiging is reëel en mag niet worden genegeerd. Bedrijfsprinters hebben zich ontwikkeld tot krachtige netwerkapparaten met dezelfde kwetsbaarheden als andere endpoints in uw netwerk. De kans op cyberaanvallen op deze meestal niet beveiligde ingangen is reëel; ze bieden daarmee ook toegang tot de financiële bedrijfsgegevens en persoonlijke informatie, wat ernstige gevolgen kan hebben voor uw onderneming.

Toch bleek uit een recent onderzoek van Spiceworks onder meer dan 300 IT-beslissers in grote ondernemingen dat slechts 16% van de respondenten printers als een risicofactor voor bedreigingen/inbreuken op de beveiliging beschouwt. Dat is aanzienlijk minder dan bij desktop pc's/laptops en mobiele devices.[1] Dit beeld beïnvloedt de manier waarop IT-medewerkers netwerkbeveiliging aanpakken. Bijna drie op de vijf ondernemingen hebben beveiligingsmaatregelen getroffen voor printers, maar dit is een veel lager percentage dan voor andere endpoints. Zo blijven printers kwetsbaar, terwijl er eenvoudige oplossingen zijn om dit specifieke toegangspunt te beveiligen.

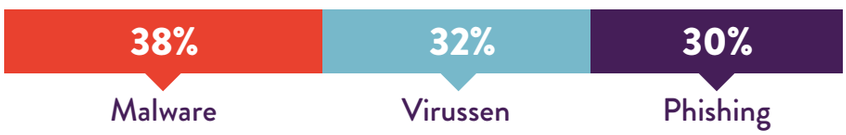
In dit whitepaper worden uitkomsten over printerbeveiliging gepresenteerd uit een onderzoek van Spiceworks naar de gevolgen van beveiligingsinbreuken en informatie over enkele moderne ingebouwde printerbeveiligingskenmerken die beschermen tegen cyberaanvallen.

SLECHTS 16% VAN DE RESPONDENTEN MEENT DAT PRINTERS EEN HOOG RISICO VORMEN VOOR EEN INBREUK OP DE BEVEILIGING.[1]

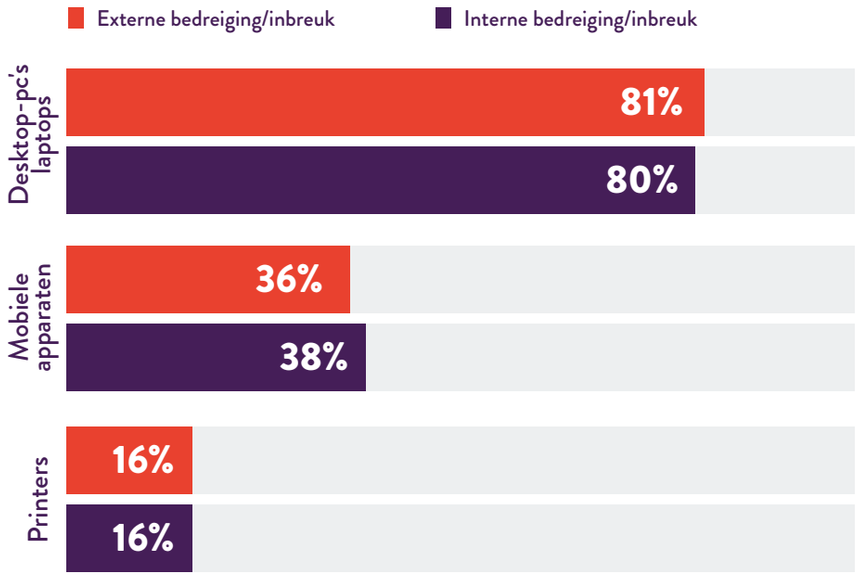
DE DEUR STAAT OPEN VOOR AANVALLEN

In het onderzoek van Spiceworks zei 74% van de respondenten (netto) dat er het afgelopen jaar in hun onderneming minimaal één vorm van externe bedreiging of schending van de IT-beveiliging had plaatsgevonden. 70% (netto) had een interne bedreiging of inbreuk op de IT-beveiliging meegemaakt, meestal door een gebruikersfout, het gebruik van privéapparaten op het werk of doordat werknemers een openbaar of thuisnetwerk voor het werk gebruikten.[1]

BELANGRIJKSTE EXTERNE BEDREIGINGEN/INBREUKEN OP DE IT-BEVEILIGING



De voornaamste bedreigingen komen binnen via desktop-pc's en laptops, maar ook via mobiele apparaten en printers.[1] (De 16% die binnenkomt via printers is aanzienlijk hoger dan de 4% die in 2014 in een vergelijkbaar onderzoek van Spiceworks werd gemeld.) Het is mogelijk dat het aantal aanvallen via printers te laag wordt ingeschat, omdat printers niet zo intensief worden bewaakt als pc's en mobiele apparaten.



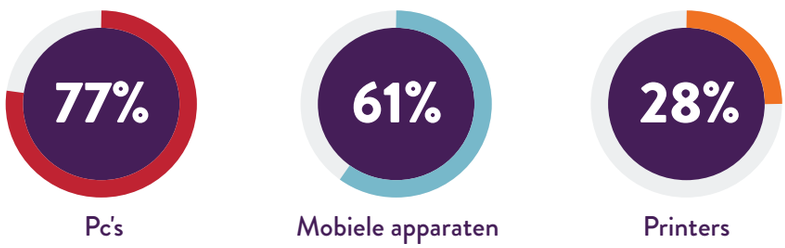
WIJ ZIEN ONZE PRINTERS OVER HET HOOFD

In elk geval maakt het onderzoek van Spiceworks duidelijk dat printerbeveiliging vaak een sluitpost is.

Ondernemingen zijn zich zeer bewust van het belang van netwerk-, endpoint- en databeveiliging. Meer dan driekwart van de respondenten maakt gebruik van netwerkbeveiliging, toegangscontrole, data-bescherming, endpointbeveiliging of een combinatie daarvan.[1]

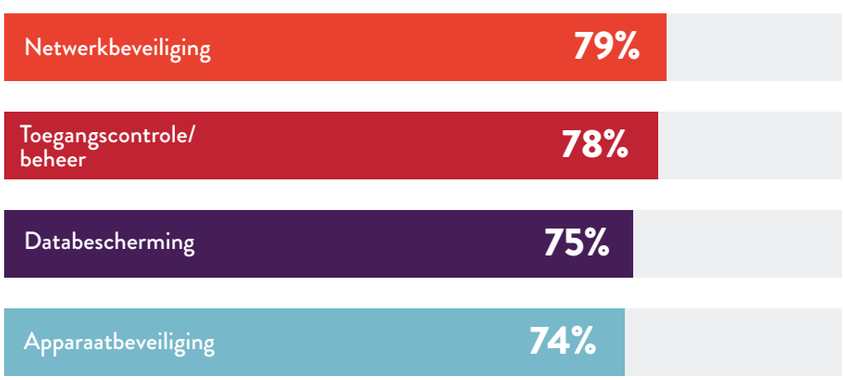
Dergelijke oplossingen worden veel minder vaak op printers geïmplementeerd. 83% van de respondenten gebruikt netwerk-beveiliging op desktop-pc's en laptops en 55% op mobiele apparaten, maar slechts 41% doet dat ook op printers.[1]

Voor endpointbeveiliging is het verschil nog groter:



Minder dan een derde (28%) van de respondenten gebruikt beveiligingscertificaten voor printers, terwijl 79% dat doet voor pc's en 54% voor mobiele apparaten.[1]

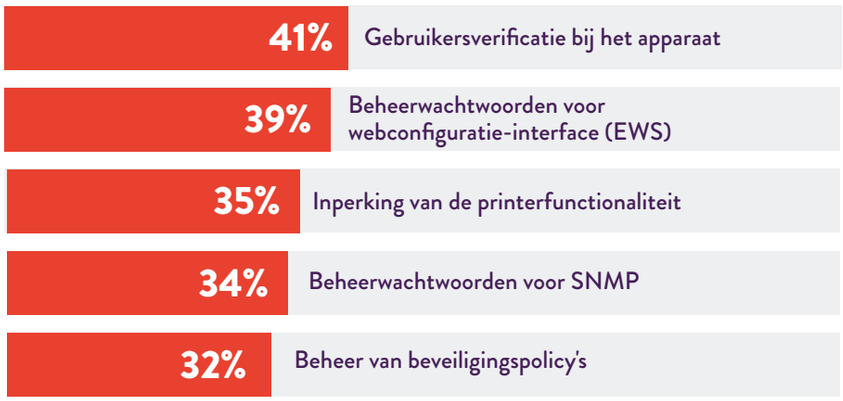
BESTE ENDPOINT BEVEILIGINGSPRAKTIJKEN



Van de beschikbare beschermingsmaatregelen voor endpoint-apparaten worden documentbeveiliging, netwerkbeveiliging en toegangscontrole het meest op printers toegepast. In het onderzoek antwoordde echter nog niet de helft van de respondenten dat hun onderneming deze op printers toepast.[1]

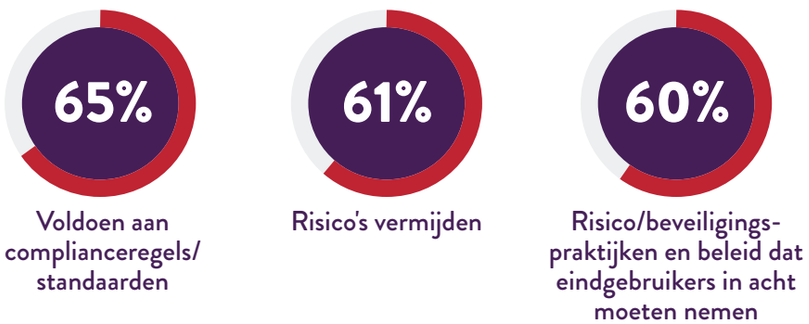
Sommige bedrijven werken met specifieke printerbeveiliging, maar ook daar zijn de onderlinge verschillen groot. Iets meer dan 40% van de ondernemingen werkte met gebruikersverificatie en minder dan 40% had beheerwachtwoorden ingesteld voor de webconfiguratie-interface.[1] Voor een goede bescherming zou elke onderneming een combinatie van deze oplossingen moeten gebruiken, en meer.

BESTE BEVEILIGINGSPRAKTIJKEN VOOR PRINTERS



Als het gaat om endpointcompliance en audits, loopt de controle op printerbeveiliging ver achter op die van vrijwel alle andere endpoints. Bijna 90% van de ondernemingen heeft een policy voor informatie-beveiliging, maar die geldt niet standaard ook voor printers. Terwijl bijvoorbeeld 57% van de respondenten meldde dat ze beveiliging tegen malware op hun pc's hebben geïnstalleerd, had slechts 17% dat ook op printers gedaan.[1]

BIJNA 9 OP DE 10 IT-PROFESSIONALS ZEGT DAT HUN ONDERNEMING EEN INFORMATIEBEVEILIGINGSPOLICY HEEFT, OM DE VOLGENDE REDENEN:



Ondernemingen nemen printerbeveiliging duidelijk niet serieus, maar dat zou wel moeten.

"Veel printers hebben nog een standaardwachtwoord of helemaal geen wachtwoord en soms wordt hetzelfde wachtwoord door tien mensen gebruikt", vertelde Michael Howard, chief security advisor voor HP in juni aan Computerworld. "Een printer zonder wachtwoord-bescherming is een goudmijn voor hackers. Een veelvoorkomend soort inbreuk is de man-in-the-middle aanval, waarbij hackers de printer overnemen en inkomende documenten naar een laptop sturen voordat deze worden geprint. Ze zien alles wat de CEO naar de printer stuurt."[2]

DE POTENTIËLE GEVOLGEN VAN PRINTERINBREUKEN

Volgens senior analist e-bedreigingen bij Bitdefender, Bogdan Botezatu, vormen printers een forse potentiële lacune in de beveiliging. "Wij zien veel telemetrie in de labs waar we de kwetsbaarheid beoordelen. De router is niet langer het gevaarlijkste apparaat op internet. Dat is nu de printer."[3]

Deze kwetsbaarheid kan ernstige gevolgen hebben voor een bedrijf. Eén niet-beveiligde printer kan uw hele netwerk met aangesloten apparaten blootstellen aan een aanval. Dan kunnen hackers mee-kijken op de apparaten in uw netwerk en de beveiliging van het hele netwerk in gevaar brengen.

Wij kennen allemaal de gevolgen van inbreuken op de beveiliging. In het onderzoek van Spiceworks noemden de respondenten de vijf belangrijkste gevolgen:[1]

1. Meer helpdesktelefoontjes en ondersteuningstijd

2. Minder productiviteit/ efficiëntie

3. Meer systeemdowntime

4. Meer tijd kwijt aan ondersteunings-gesprekken

5. Betere handhaving van eindgebruikersbeleid

Een inbreuk op een printer heeft extra catastrofale gevolgen als het om een multifunctionele printer gaat waarop geprinte data elektronisch worden opgeslagen. Printtaken die in het printercache

zijn opgeslagen geven hackers toegang tot gevoelige persoonlijke en bedrijfsgegevens.

Erger nog, hackers kunnen zich via een niet-beveiligde printer toegang verschaffen tot het bedrijfsnetwerk en bijvoorbeeld burgerservicenummers, financiële informatie of interne memo's en documenten stelen. Deze gestolen informatie kan niet alleen individuele werknemers schaden, maar bijvoorbeeld door concurrenten worden gebruikt of reputatieschade veroorzaken voor het bedrijf.

EENVOUDIGE OPLOSSING: INGEBOUWDE BEVEILIGINGSKENMERKEN

Bedrijven moeten ook hun printers beveiligen. Sommige moderne bedrijfsprinters bevatten gebruiksvriendelijke ingebouwde beveiliging die helpt bedreigingen af te weren. Onder andere:

- Automatische detectie, bescherming en herstel na aanvallen
- Controle op het gebruik om ongeautoriseerd gebruik te voorkomen
- Eenvoudige aanmeldingsopties zoals pincodes of smartcards
- Proximity-kaartlezer waarmee gebruikers zich snel met hun bestaande id-badge bij een printer kunnen authenticeren om veilig te printen
- Veilig versleuteld printen voor vertrouwelijke documenten

Als u een nieuwe printer aanschaft, ongeacht of het een desktopprinter of een multifunctionele printer is, kijk dan naar de ingebouwde beveiliging en activeer deze ook. Als u dergelijke eenvoudige printerspecifieke kenmerken gebruikt, bent u minder kwetsbaar via uw printers; met Internet of Things zijn er immers al voldoende toegangspunten om u zorgen over te maken. **Daar hoeven uw printers niet bij te horen.**

ZOEKT U BETER BEVEILIGDE PRINTERS?

MEER INFORMATIE ›

Bronnen:

[1] Enquête van Spiceworks onder 309 IT-professionals in Noord-Amerika, EMEA, Azië en Oceanië, die uitgevoerd werd namens HP, november 2016.

[2] "Printer Security: Is your company's data really safe?" Computerworld, 1 juni 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet", The Register, 8 september 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/