5 pijnlijke printervragen die je nu moet stellen

- De vijf pijnlijke printervragen die je moet stellen om een printerhack te voorkomen
- 6 verontrustende cijfers over printerbeveiliging
- 14 praktische tips voor printerbeveiliging

Slim zakendoen
over winnen met IT

Slim zakendoen
over winnen met IT

Printerhack checklist – Voorkom veelvoorkomende printerhacks: 5 vragen, 6 cijfers, 14 tips

Beveilig je printers en voorkom een printerhack en erger. In deze printerhack checklist vind je:

- De vijf pijnlijke printervragen die je moet stellen om een printerhack te voorkomen
- 6 verontrustende cijfers over printerbeveiliging
- 14 praktische tips voor printerbeveiliging

Met deze printerhack checklist weet je binnen vijf minuten waar jouw organisatie staat in printerbeveiliging. Je brengt de belangrijkste vraagstukken en risico's in kaart en krijgt handzame tips om direct je printers te beveiligen. Zo zet je printerbeveiliging goed op de agenda.

Voor directie en IT

Printerbeveiliging lijkt een IT-kwestie, maar de mogelijke gevolgen van een slechte printerbeveiliging raken iedereen in het bedrijf. Een printerhack kan het begin zijn van een datalek. Dat kan resulteren in reputatieschade, bedrijfsschade en per 25 vanaf mei 2018 mogelijk ook een fikse boete onder de GDPR. Die kan oplopen tot € 20 miljoen of 4 procent van de omzet. Toch zijn printers vanuit beveiligingsoogpunt vaak het ondergeschoven kindje. Daarom is het van groot belang dat de directie op de hoogte is van de risico's en mee kan praten over printerbeveiliging.

- 60% van de organisaties heeft onbeveiligde printers binnen haar netwerk (IDG, 2017).
- 23% van de organisaties past databescherming toe op haar printerpark (Spiceworks, 2016).
- 64% van de IT-managers vermoedt dat hun bedrijfsprinters besmet zijn met malware (Ponemon Institute, 2015).
- 60% van de bedrijven heeft te maken gehad met een dataschending waarbij printers waren betrokken (Ponemon Institute, 2015).
- 73% van de beveiligingsmanagers verwacht binnen een jaar doelwit te worden van een beveiligingsschending (Help Net Security, 2015).
- $ 3,6 miljoen bedraagt de gemiddelde schade na één dataschending. (Ponemon Institute, 2017).

De vijf pijnlijke printervragen die je nu moet stellen

Bij elke printervraag krijg je een toelichting op het risico en drie deelvragen met praktische printertips. Vakjargon leggen we uit. De tips omvatten beleid, instellingen en features om te overwegen bij de aanschaf van een printer. Met deze checklist start je de discussie over printerbeveiliging.

1. Zijn onze printers veilig aangesloten op het internet?

Printers zijn vandaag de dag slimme devices met internettoegang. Toch zijn printers vaak niet of slecht beveiligd. En daarmee loop je een groot risico. Zonder goede printerbeveiliging zijn printers die zijn aangesloten op het netwerk gemakkelijk te hacken. Hackers kunnen dan printopdrachten onderscheppen en verdere aanvallen op het netwerk voorbereiden. Multifunctionele printers (MFP's) hebben bovendien een harde schijf waarop bestanden worden opgeslagen. Zo kunnen hackers ook bij scans of kopieën.

1. **Zijn al onze poorten beveiligd?**
   Een printer heeft allerlei poorten om te communiceren met andere devices in het netwerk. Voor het functioneren van de printer hoeven deze niet allemaal open te staan. Beveilig de poorten die je wel gebruikt. Veel printers luisteren naar poort 9100 en printen alles wat daar binnenkomt zonder authenticatie.

2. **Zijn de verstuurde gegevens beveiligd?**
   Met een printopdracht verstuur je informatie via het netwerk naar de printer. Het netwerk hoort beveiligd te zijn met een firewall, virusscanner, malwaredetectie en 802.1x- of IPsec-netwerkbeveiliging. Gebruik daarnaast ook encryptie om de printopdrachten te beveiligen. Daarmee voorkom je dat onderschepte printopdrachten gelezen kunnen worden.

3. **Zijn de printerinstellingen beveiligd en wordt dit gecontroleerd?**
   De apparaatgegevens waarmee je de printer beheert moeten worden beveiligd. Dat kan met de Embedded Web Server die standaard op een netwerkprinter zit. HP's JetAdvantage Security Manager biedt bovendien een automatische controle op de beveiligingsinstellingen en herstelt deze indien nodig.

2. Hoe regelmatig worden de printers geüpdatet?

Schrikbarend veel bedrijven onderhouden de printerbeveiliging niet of nauwelijks. De firmware waarop de printer draait, wordt nooit geüpdatet. Patches worden genegeerd en de fabriekswachtwoorden blijven ongewijzigd. Dat maakt het hackers wel heel gemakkelijk om jouw printers te hacken, want alle wachtwoorden en hackmogelijkheden zijn gewoon online te vinden.

4. **Zijn onze printers beveiligd met een eigen wachtwoord?**
   Met een wachtwoord beveilig je de printers. Verander direct het standaard wachtwoord. Wijzig het wachtwoord regelmatig.

5. **Is onze firmware up-to-date?**
   Wanneer printerhacks bekend worden, leveren hardwarefabrikanten updates van de firmware. Update hiermee direct je printers, want oude of besmette firmware maken je netwerk kwetsbaar voor cyberaanvallen.

6. **Hebben onze printers een white listing-functie?**
   Hackers kunnen proberen hun eigen applicaties op jouw printers te plaatsen. Met white listing kunnen alleen goedgekeurde en geautoriseerde applicaties draaien. Bij een afwijking start het apparaat op in een veilige modus en wordt de IT-afdeling geïnformeerd.

3. Wie kan er bij ons printen?

Alle werknemers binnen het bedrijf moeten kunnen printen. En verder niemand. Het is belangrijk om gebruikers te verifiëren voordat ze toegang krijgen tot de netwerkprinters. Steeds meer bedrijven laten hun werknemers mobiel en via de cloud werken. Dat vraagt extra aandacht voor printerbeveiliging.

7. **Worden gebruikers geverifieerd voordat ze kunnen printen?**
   Zorg ervoor dat alleen geverifieerde gebruikers toegang krijgen. Gebruik hiervoor verificatieoplossingen zoals LDAP-authenticatie, proximitykaarten, smartcards of biometrische toegangsoplossingen. Regel per gebruiker de toegang tot specifieke instellingen en functies.

8. **Kan er veilig mobiel worden geprint?**
   Geef werknemers mobiele printmogelijkheden zoals HP Wireless Direct Printing of NFC touch-to-print. Hiermee kunnen werknemers veilig printen zonder het bedrijfsnetwerk op te gaan. Per mail krijgen ze een veiligheidscode waarmee de printopdracht wordt bevestigd.

9. **Kan er veilig vanuit de cloud worden geprint?**
   Via onbeveiligde clouddiensten kunnen hackers zichzelf toegang verlenen tot de netwerkprinters. Kies daarom voor een beveiligingsoplossing die gebruikersauthenticatie ondersteunt, ongeacht de locatie van de data.

4. Hoe veilig zijn mijn printopdrachten?

Veel bedrijven maken geen onderscheid in de documenten die worden geprint. Iedereen kan dan vertrouwelijke informatie van de printer inzien en meenemen. Daarnaast worden printopdrachten vaak opgeslagen op de netwerkprinter. Zorg ervoor dat prints pas na verificatie bij de printer worden vrijgegeven en beveilig of wis de printbestanden op de printer.

10. **Kan iemand anders mijn prints meenemen?**
    Voorkom dat prints blijven liggen of door een ander worden meegenomen. Met pull-printing worden printtaken eerst opgeslagen. Pas na fysieke identificatie bij de printer met een pincode of badge wordt er daadwerkelijk geprint. Daarmee voorkom je ook dat prints niet worden opgehaald. Dit kun je combineren met een fysiek slot op de uitvoerlade.

11. **Wat gebeurt er met het printbestand?**
    Data op de interne drive of vaste schijf van de printer zijn kwetsbaar. Kies voor printers die deze data automatisch encrypten of direct verwijderen. Dat is ook van belang wanneer de printers worden afgedankt of geretourneerd na leasen.

12. **Is de USB-poort op de printer wel nodig?**
    Via de USB-poort van de printer kun je vaak gemakkelijk data van de harde schijf halen. Op MFP's staan bovendien ook scans en kopieeropdrachten. Schakel daarom de USB-poorten op alle printers standaard uit, tenzij je 100% zeker bent van de beveiliging en USB-sticks veel worden gebruikt.

5. Hoe ontdekken wij een eventuele printerhack?

Voorkomen is natuurlijk beter dan genezen. Maar ondanks alle maatregelen hierboven kan het toch gebeuren dat je printer wordt gehackt. Het tijdig ontdekken en bestrijden van een printerhack is cruciaal om ernstige schade te voorkomen.

13. Worden de printers actief gemonitord op aanvallen?

Afwijkingen in de firmware of het geheugen van de printer wil je direct opsporen. HP's run-time inbraakdetectie bewaakt continu en herkent aanvallen. Bij een aanval wordt de printer automatisch opnieuw opgestart.

14. Starten de printers veilig op?

Een printer start op met het BIOS: een lijst met instructies om de hardwarecomponenten te laden voor gebruik. Met HP's Sure Start wordt het BIOS eerst gecontroleerd. Is er geknoeid of klopt er iets niet, dan wordt het BIOS automatisch overschreven met een gegarandeerd correcte versie.

Direct ondersteuning nodig?

Heb je na het lezen van dit document behoefte aan ondersteuning, aarzel dan niet om contact op te nemen. Stuur dan een e-mail naar service@slim-zakendoen.nl. Wil je deze informatie delen met anderen? Stuur dit document dan gerust door.

www.slim-zakendoen.nl

Slim zakendoen
over winnen met IT