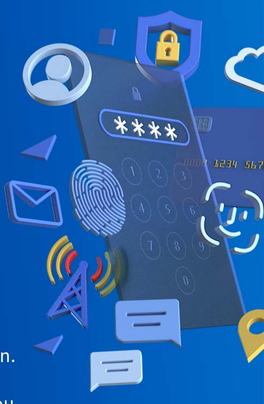
TOSHIBA

Checklist veilig printen

Print speelt nog steeds een belangrijke rol in veel organisaties. Maar wist je dat printerbeveiliging voor veel IT-afdelingen niet bovenaan de prioriteitenlijst staat? Toch is dat niet terecht! Kantoorprinters zijn tegenwoordig net zo krachtig als computers. Ze zijn ook voorzien van een besturingssysteem. Zo is een printer bijvoorbeeld verbonden met het internet en interne netwerk. Via deze weg kunnen cybercriminelen je systemen binnendringen.

Met deze checklist zie je wat je minimaal zou moeten doen om veilig te printen en hackers zoveel mogelijk buiten de deur te houden. Hoeveel punten kun jij al afvinken?



Knowledge On Demand

☐ Veilige pincodes

Pincodes zijn eenvoudig te raden en niet onze eerste keuze als het gaat over de beveiliging van printopdrachten. Indien jouw organisatie echter toch met pincodes wil werken om printopdrachten vrij te geven, werk dan met veilige pincodes.

- Kies een willekeurige reeks en geen herhaaldelijke cijfers, zoals 1111,2222.
- Gebruik 5 cijfers of meer i.p.v. 4 cijfers. Dat ene extra cijfer breidt het aantal mogelijke pincodes uit van ongeveer 10.000 naar ongeveer 100.000. Hierdoor is het moeilijker te raden.

☐ Firmware updates

Firmware updates zorgen ervoor dat hackers veel minder kans krijgen door te dringen in de systemen.

- Vraag altijd aan Toshiba om jouw kantoorprinter(s) aan te melden op het Toshiba cloud platform, zodat updates direct op je printer geïnstalleerd worden zodra deze beschikbaar zijn.

☐ Print altijd beveiligd

Printen waarbij het document direct uit de printer komt is erg onveilig. Je zit vaak nog aan je bureau en moet nog naar de printer lopen. Je collega of bezoeker kan (per ongeluk) met jouw print weglopen voordat jij bij de printer bent.

- Kies altijd voor een beveiligde printoplossing waarbij de print pas uit de printer komt als je er zelf voor staat en de juiste pincode hebt ingevuld, je toegangspas hebt gebruikt of vingerafdrukherkenning om je aan te melden.

☐ Phishing mails

Reageer nooit zomaar op e-mails waarin “door ICT” gevraagd wordt je pincode of toegangscode door te geven door op de handige link te klikken die ‘ICT alvast in de e-mail erbij heeft gezet. Grote kans dat deze email niet van de ICT afdeling komt, maar van een hacker die zo probeert zoveel mogelijk inloggegevens van je buit te maken.

- Toshiba’s printers en printoplossing vragen nooit of je zelf je code wil wijzigen, maar stuurt je direct een nieuwe code toe om te gebruiken. Wel zo veilig en gecontroleerd.

☐ Gebruik een veilige internetverbinding

Voor het versturen van printopdrachten is een beveiligde verbinding noodzakelijk. Je stuurt immers vaak vertrouwelijke gegevens naar de printer toe, zoals een factuur of een orderbevestiging. Gegevens waar een hacker heel wat mee kan doen. Vooral voor de populaire cloudprint-oplossingen is dit van belang. Hierbij kun je immers al printen vanaf huis, onderweg of in een koffiezaak. Gebruik je daar de lokale gratis wifi, dan is een VPN verbinding of versleutelde verbinding zeker noodzakelijk.

Meer weten?

Wil je meer informatie over onze producten, oplossingen of diensten, neem dan contact op en ontdek hoe we jouw organisatie kunnen helpen.

info@toshibatec.nl | www.toshibatec.nl