TJEKLISTE FOR PRINTERSIKKERHED

Denne tjekliste er nyttig for virksomheden, der vil forbedre sin it-sikkerhed, beskytte sit omdømme, undgå de kostbare følger af et indbrud og opfylde de nye, strengere GDPR-regler. Begynd med det grundlæggende trin og gå igennem listen punkt for punkt.

1

Grundlæggende sikkerhedsniveau

- [ ] Køb kun enheder med integreret beskyttelse mod skadelig software og med krypterede harddiske.
- [ ] Opdatér printerens software, specielt hvis den nye version indeholder vigtige sikkerhedsopdateringer – ligesom når du opdaterer apps på din mobiltelefon.
- [ ] Konfigurér enhedernes interface og deaktivér protokoller som FTP og telnet, som programmerne ikke bruger.
- [ ] Gennemgå nye enheder og luk for porte eller protokoller, der ikke anvendes nu, og som kan give it-kriminelle adgang.
- [ ] Brug en unik administratoradgangskode til hver enhed.
- [ ] Deaktivér muligheden for at konfigurere administratorindstillinger direkte på printeren.
- [ ] Kryptér de oplysninger, som brugerne udveksler med enheden.
- [ ] Iværksæt procedurer for at slette gamle oplysninger fra printerens hukommelse.

+ Fortsæt til næste sikkerhedsniveau, når du er færdig.

2

Mellemliggende sikkerhedsniveau

- [ ] Integrér data fra printernes systemlogs i SIEM-værktøjet for at overvåge netværket mere overordnet i forhold til trusler. Synlighed er kernen i at opfylde de nye regulativers rapporteringskrav.
- [ ] Implementér brugergodkendelse på printeren for at spore, hvem der kopierer, scanner og faxer fra enheden. Disse oplysninger kan bruges i den kriminaltekniske udredning efter en eventuel indtrængen.
- [ ] Indfør pull-print for at undgå, at følsomme oplysninger eksponeres. Det hjælper også med til at opfylde miljøkrav ved at reducere unødvendige udskrifter.

+ Fortsæt til det sidste sikkerhedsniveau, når du er færdig

3

Avanceret sikkerhedsniveau

- [ ] Brug jobsporing og revisionsrapporter
- [ ] Overvej at indføre – og automatisk håndhæve – regler for, hvem der må bruge hvilke printere med rollebaserede tilladelser.
- [ ] Brug unikke digitale certifikater til hver printer på samme måde som på andre internetforbundne enheder i netværket.
- [ ] Brug en administrationstjeneste til mobiludskrivning med datakryptering, enhedsadgang på netværket, brugergodkendelse og sporing.