Checklista för att säkra skrivare enligt säkerhetskraven.

EU:s allmänna dataförordning kräver att företag implementerar tekniska och organisatoriska åtgärder för att säkra personlig information och eventuellt meddela personer och myndigheter som har påverkats om ett dataintrång inbegriper personlig information.

Det är en utmaning för företag att hitta tid och resurser för att uppfylla efterlevnadsreglerna.

Men om de inte kan uppvisa mer än en enkel brandvägg som skydd, kan de utsättas för attacker och få böter på flera miljoner. Det är troligt att alla företag någon gång kommer att drabbas av ett intrång, så det är av största vikt att upptäcka intrånget och åtgärda det så fort som möjligt med hjälp av rätt produkter, processer och verktyg.

Den här checklistan är en praktisk resurs för företag som vill förbättra sin IT-säkerhet och undvika de kostsamma påföljderna av ett intrång. Börja med det grundläggande och gå igenom listan nivå för nivå för att maximera säkerhetsnivåerna, så kan ni säkerställa att era skrivare är säkrade och uppfyller GDPR-reglerna.

En praktisk lista för att säkra skrivarna i ert nätverk.

Grundläggande säkerhetsnivå

- Köp endast enheter med inbyggt skydd mot skadlig programvara och med krypterade hårddiskar
- Uppdatera den inbyggda programvaran, särskilt om den nya versionen innehåller kritiska säkerhetsuppdateringar, på samma sätt som man uppdaterar apparna i sin mobiltelefon
- Konfigurera enheternas gränssnitt och inaktivera protokoll som FTP och telnet som inte krävs av programmen
- Gå igenom nya enheter och stäng av portar eller protokoll som inte används just nu och som kan ge inkräktare åtkomst
- Använd unika administratörslösenord för varje enhet
- Inaktivera frontpanelen för att hindra åtkomst till administratörsfunktioner
- Kryptera den information som flödar till och från enheten
- Ställ in procedurer för att radera gammal information från hårddiskarna, särskilt på skrivare

Fortsätt med nästa säkerhetsnivå när detta är gjort.

Mellanliggande säkerhetsnivå

- Integrera data från skrivarnas systemloggar i SIEM-verktyget för att övervaka nätverket mot hot på ett mer heltäckande sätt. Visibilitet är kärnan i att uppfylla de nya efterlevnadsreglernas rapporteringskrav
- Implementera användarverifiering vid skrivaren för att spåra vem som kopierar, skannar och faxar från enheten. Denna information är användbar vid kriminaltekniska utredningar efter ett intrång
- Tillämpa pull printing för att undvika att känslig information glöms bort. Detta hjälper även till att uppfylla miljökrav genom att minska onödiga utskrifter

Fortsätt med sista säkerhetsnivån när detta är gjort.

Avancerad säkerhetsnivå

- Använd jobbspårning och redovisningsrapporter
- Överväg att ange och automatiskt verkställa regler för vem som kan komma åt och använda vilka skrivare och varför med rollbaserade behörigheter
- Använd unika digitala certifikat för varje skrivare på samma sätt som för andra internetanslutna enheter i nätverket
- Använd en administrationstjänst för mobila utskrifter för datakryptering, enhetsåtkomst i nätverket, användarverifiering och spårning

4AA7-1093SVE