



Er bedriftens sikkerhetsfunksjoner for utskrifter og skanning klare for den viktigste endringen i personvernforskriftene på to tiår?

Anthony Buxton, seniorleder ved Legal & Corporate Governance ved Brother International Europe, gir en kommentar om maskinsikkerheten etter hvert som implementeringen av den nye europeiske personvernforordningen (GDPR) nærmer seg.

En undersøkelse som ble foretatt for to år siden, viser at små og mellomstore bedrifter (SMB-er) over hele Europa har vært bevisste på informasjonssikkerhet en stund allerede. 75 %¹ oppga at det var viktig for organisasjonen deres, og 59 % sa at det påvirket avgjørelser de traff angående utskrifter og dokumenthåndtering.

Og en studie av europeiske mellommarkedsbedrifter og større selskaper fra i år viste at hele 96 %² anser utskriftssikkerhet som viktig. Men tross i denne bevisstheten er det en markant mangel på tillit blant foretakene: Bare 22 % av de europeiske selskapene oppga at de er føler seg helt trygge på at maskinene deres er beskyttet mot trusler.

Dataene viste også at større organisasjoner er kommet lengst med GDPR og utskriftssikkerhet. Faktisk er prosentandelen av de store organisasjonene som vil ta med utskriftssikkerhet som en del av GDPR-tiltakene sine, mer enn dobbelt så stor som andelen av organisasjonene i mellommarkedet som vil gjøre det samme – med 53 % mot 24 %.

Hvis vi igjen ser på små og mellomstore bedrifter og på [den europeiske personvernforordningen \(GDPR\)](#) som trer i kraft om bare noen måneder, hvordan kan disse virksomhetene beskytte utskriftene sine mot brudd på datasikkerheten?

Manglende overholdelse av den nye forordningen kan faktisk straffes med bøter på opptil 20 millioner euro eller 4 % av bedriftens samlede omsetningen, avhengig av hvilket beløp som er størst. Og kanskje like viktig som bøkene er det at de enkelte kundene har stadig større forventninger til personvern og personvernrettighetene sine. Små og mellomstore bedrifters omdømme er i dag avhengig av at de har gode rutiner for håndtering av dataene. I forlengelsen



av dette er de nødt til å ta håndteringen av utskrifter og skanning på alvor.

Vær bevisst på truslene

Utskrifts- og skanneoppsettet blir stadig mer fleksibelt og robust satt opp. Større funksjonalitet og flere tilkoblingsmuligheter medfører større sikkerhetsrisiko for nettverkstilkoblede enheter. Truslene kan deles inn i fire viktige områder:

- 1) Utsiktet lekkasje av konfidensielle utskrifter
- 2) Utsiktet lekkasje av konfidensielle skanninger
- 3) Innbrudd i nettverket som følge av utilstrekkelig sikkerhet
- 4) At uautoriserte brukere får fysisk tilgang til ubevoktede enheter

Så hvis noen kan hente dokumenter fra skriveren deres og ta de med seg, er dataene utsatt for risiko, og bedriften deres kan pådra seg et erstatningsansvar.

For en liten eller mellomstor bedrift betyr ikke dette automatisk at man må gjøre store investeringer eller oppgradere til nytt utstyr for å oppfylle kravene i den banebrytende lovgivningen.

Våre skrivere og skannere har en lang rekke innebygde sikkerhetsfunksjoner som kan installeres for å beskytte bedriften mot store bøter som følge av eventuelle brudd på personvernforordningen.

Sikkerhetsløsningene våre er ideelle for bransjer som HR, finans, helse, detaljhandelen, juridisk og utdanning, men kan også være nyttige for andre virksomheter som praktiserer taushetsplikt.

Secure Print

Secure Print er gratis og innebygd i mange av enhetene våre, og er ideell for småbedrifter som av og til skal skrive ut konfidensielle dokumenter. Brukerne kan velge Secure Print-funksjonen når de skal skrive ut et sensitivt dokument, og vil bli bedt om å taste inn en firesifret kode. Koden må tastes inn på maskinen for å

få ut dokumentet, og utskriften venter til brukeren fysisk befinner seg ved enheten. Dette gjør funksjonen ideell for skrivere med flere brukere.

Secure Print+

For små og mellomstore bedrifter med mer omfattende sikkerhetsbehov kan brukerne få et eget ID-kort som de må trekke for å få ut utskriftene sine. Dette fungerer via nærfeltkommunikasjon (NFC) og knyttes til et unikt ansattnummer.

ID-kortet gjør operasjonen brukervennlig for de ansatte, siden de ikke trenger å huske en PIN-kode for å sette i gang utskriftsjobber.

Secure Print og Secure Print+ kan brukes til å kontrollere skanning, kopiering og faksing og gjør det mulig å konfigurere en enhet slik at den automatisk sletter utskriftsjobber som ikke hentes ut.

Secure Function Lock

Denne gratisfunksjonen gir bedriftene større kontroll over enhetene sine ved å begrense tilgangen til maskinens innstillinger via kontrollpanelet.



Secure Function Lock begrenser også adgangen til visse funksjoner, slik at bedriftene kan avgjøre hvilke ansatte som kan gjøre hva med en enhet. For eksempel kan man styre hvem som skal kunne skrive ut, skanne, kopiere og fakse, eller sette opp månedlige bruksgrenser ved hjelp av PIN-koder og NFC-kort.

Etter hvert som implementeringen av GDPR nærmer seg, kan man ved å ta i bruk disse innstillingene i betydelig grad redusere risikoen for at sensitive opplysninger kommer på avveie. Uten denne låsefunksjonen kan for eksempel innstillingen for skanning til e-post endres, slik at en ikke godkjent e-postadresse begynner å motta konfidensiell informasjon.

PrintSmart SecurePro

PrintSmart SecurePro er en mer avansert sikkerhetsløsning rettet mot små og mellomstore bedrifter og større selskaper. Den leverer kompleks skriverbeskyttelse når de forskjellige brukerne har ulike behov for å skrive ut konfidensielle opplysninger. PrintSmart SecurePro er ideell fordi den er en serverbasert løsning som ikke bruker opp enhetens minne.

Den har en «pull printing»-funksjon som frigjør et dokument med en PIN-kode eller et ID-kort på en NFC-leser, slik at sensitive dokumenter beskyttes, mens jobber som eventuelt ikke hentes ut (ikke blir «pulled»), slettes etter en angitt tid. Dette eliminerer risikoen for at en konfidensiell jobb hentes ut av en uautorisert ansatt.

Dermed er det bare brukeren som har sendt jobben, som kan hente den, og konfidensielle opplysninger blir bare tilgjengelige for autoriserte brukere.

Hvis det likevel skulle forekomme lekkasje av data, kan PrintSmart SecurePro opprette en omfattende revisjonslogg, en såkalt «audit trail». Denne rapporten kan opprettes raskt og kan inneholde opplysninger om klokkeslett, dato, IP-adresse, sideantall, A3- eller A4-format og ensfargede eller flerfargede utskrifter.



Siden revisjonsloggen er så detaljert, blir det lettere å undersøke utskriftsaktivitetene, helt i tråd med kravene i GDPR-forordningen.

Innebygd kryptering

Bedriftene bør være klar over at visse typer programvare gjør det mulig å snappe opp dataene mens de sendes til skriveren. For å beskytte dere mot dette har enhetene våre innebygd kryptering i form av Transport Layer Security (TLS) og Secure Socket Layer (SSL). Dette er den samme teknologien som brukes for å beskytte bank- og kredittkortopplysninger i ulike e-handelsløsninger. Dermed kan de mest konfidensielle filene deres krypteres med opptil 256-bits oppløsning når de overføres i nettverket.

Våre løsninger letter utskrifts- og skannesikkerheten for mikrobedrifter og hjemmekontorer som mangler eller bare har en begrenset IT-infrastruktur, og hjelper små, mellomstore og større selskaper med å forberede seg på personvernforordningen som trer i kraft 25. mai 2018.

Bedriftens størrelse er ingen unnskyldning, og klokken tikker.

¹ Brother SMB Research, utført i 2015 av B2B International blant 2502 bedrifter i Storbritannia, Frankrike, Tyskland og USA.

² Quocirca Managed Print Services Landscape, 2017. Resultater fra en europeisk undersøkelse av 180 organisasjoner i mellommarkedet (500–999 ansatte) og store organisasjoner (1000+ ansatte) i Storbritannia, Frankrike og Tyskland som benytter seg av en utskriftsstyringstjeneste.