

Oprethold et sikkert print-økosystem

En del af Brother Digital
Transformation-serien



Forskningsbaseret
thought leadership-rapport

brother.dk

Forhindringer for at investere i printersikkerhed

Med den voksende trussel mod dokumentetsikkerheden og risikoen for hacking er de fleste små og mellemstore virksomheder (SMV'er) meget opmærksomme på at beskytte deres it-systemer.

Håndtering af IT-aktivernes sikkerhed er en udfordring, der skal tackles over hele linjen. Printere, scannere og kopimaskiner skal være lige så sikre som andet udstyr. Hvis man glemmer det, risikerer disse enheder at åbne en bagdør til organisationen for hackere. SMV'er bliver i stigende grad opmærksomme på vigtigheden af dette emne, og **72 %** af virksomhederne finder det afgørende, at deres printere, scannere og kopimaskiner er sikre. Dette er endnu mere aktuelt blandt de organisationer, der håndterer følsomme data såsom liberale erhverv (**82 %**) og sundhedsvæsenet (**81 %**).

Det efterlader dog stadig tæt ved en tredjedel af organisationer, der ikke erkender vigtigheden. Samtidigt er det næsten halvdelen, der ikke oplever, at deres organisation har investeret tilstrækkeligt i printersikkerhed.

Hvis virksomhederne forstår behovet for at investere i printersikkerhed, hvorfor gør de det så ikke i øjeblikket?

Vores undersøgelse peger på to klare årsager:



Uklar ansvarsplacering, når det gælder printersikkerhed



Manglende forståelse af og viden om sikkerhedstrusler og -standarder

Denne rapport er udarbejdet med det formål at hjælpe SMV-beslutningstagere med at forstå, hvor vigtig printersikkerhed er, og hvordan sikre printløsninger indføres. Den er en del af en serie, der forsøger at informere beslutningstagere om, hvordan de bedst kan udnytte digitale teknologier i SMV'er. Rapporterne er baseret på undersøgelser gennemført blandt SMV-beslutningstagere i EMEA-regionen (Europa, Mellemøsten og Afrika). Serien er opdelt i fire rapporter, der hver især behandler følgende emner:

- Digitale workflows
- Implementering af den rigtige løsning til din virksomhed
- Sikkerhed
- Bæredygtighed



Hvem er ansvarlig for printersikkerheden?

Alt for ofte er det uklart hvem, der har ansvaret, når det kommer til printersikkerhed. Næsten halvdelen af SMV'erne i Vesteuropa (**44 %**) fortæller, at det er uklart, hvem der er ansvarlig for printersikkerheden i deres organisation. Hvis ansvarsområderne er uklare, går det sandsynligvis ud over beslutninger omkring og implementering af printersikkerhed, så virksomheden efterlades sårbar.

Når ansvaret for printersikkerhed ikke er placeret, skyldes det ofte, at print-setuppet traditionelt ikke er blevet betragtet som et svagt punkt på samme måde som andre enheder såsom laptops. Selvom vores undersøgelse viser, at beslutningstagere begynder at blive opmærksomme på printsikkerhedens betydning, ser SMV-stillingerne ikke ud til at afspejle dette endnu.

SMV'er er særligt sårbare, da ansvaret for virksomhedens maskiner og software ofte ligger hos nogle få medarbejdere. Hvis medarbejderne ikke er opmærksomme på risiciene ved printsikkerhed, kan det let blive prioriteret lavt.

Men alle medarbejdere i en organisation har en eller anden grad af ansvar for at følsomme oplysninger holdes sikre.



Mens IT- og teknologi-specialister er ansvarlige for maskinernes sikkerhed, har medarbejderne et ansvar for at sørge for, at data holdes sikre. Datasikkerhed er måske det største risikoområde, når det handler om følsomme forretningsoplysninger.

Datasikkerhed omfatter en bred vifte af trusler, herunder:



uautoriseret adgang til print



at glemme at logge ud efter at have udskrevet fortrolige dokumenter



manglende sporing af, hvem der har haft adgang til hvilke dokumenter ved printeren

Næsten 9 ud af 10 virksomheder har oplevet en printerrelateret sikkerhedshændelse ...



... og syv ud af ti (**72%**) mener, at datasikkerhed er en større trussel end maskinsikkerhed. Men i øjeblikket er det mindre end en tredjedel af virksomhederne, der siger, at de føler sig forvisset om, at deres printinfrastruktur rummer tilstrækkelige sikkerhedsforanstaltninger. Derimod er det **53%** af virksomhederne, der føler, at de har den rette maskin-sikkerhed på plads.

De fleste SMV'er (**64%**) siger også, at det er en topprioritet at sørge for, at deres data er sikre. Dette betragtes som en afgørende udfordring og kan være en reel hindring for effektive præstationer.

I dag er det næsten halvdelen af SMV'erne (**48%**), der siger, at de kun har få eller ingen procedurer, som gør det muligt at redegøre for, hvem der printer eller henter printjobs. Det er ikke overraskende, at næsten ni ud af ti virksomheder (**86%**) fortæller, at de har haft en printerrelateret sikkerhedshændelse.

Disse sikkerhedshændelser er typisk relateret til fortrolige papirer, som ligger uden opsyn ved printeren, uafhængte print eller medarbejdere, som tager fortrolige dokumenter, der ikke er deres.

Som en konsekvens heraf begynder de fleste SMV'er (**64%**) at indføre foranstaltninger til at håndtere printerrelaterede sikkerhedsudfordringer i form af begrænset adgang til visse printere eller indførelse af ID-kort/PIN-koder, så printjobs kun frigives for de rette personer.

Det er et skridt i den rigtige retning. I de kommende år vil det blive vigtigt for alle virksomheder at indføre mere sikre procedurer, og for dem, der allerede er i gang, at fastholde og forbedre deres indsats omkring ansvar og opsyn.

Reel informationssikkerhed har tre hovedmål:

Disse mål dækker både maskin- og datasikkerhed:

Fortrolighed

Beskyttelse af fortrolige forretningsdata for at sikre, at de kun deles med de rette modtagere. Til det skal man bruge autentificering og autorisation, som kræver, at brugerne bekræfter deres identitet, og at de har rettigheder til at gøre det, de forsøger at gøre, inden et print frigives.

Integritet

At sørge for, at maskinernes firmware er sikker og robust i forhold til hacking og andre eksterne trusler.

Tilgængelighed

At sørge for, at maskinerne fungerer og er tilgængelige for autoriserede brugere, så de kan udføre deres arbejdsopgaver.

Manglende viden medfører dårlig håndtering af sikkerhed

Mindre end en tredjedel (**32 %**) af de centrale IT-beslutningstagere, der arbejder i SMV'er, siger, at de har avanceret viden om teknologisk sikkerhed og potentielle trusler. Hvis IT-beslutningstagere ikke har tilstrækkelig viden, vil virksomhederne fortsat have problemer med at iværksætte passende foranstaltninger for at beskytte sig selv. I SMV'er har IT-beslutningstageren typisk en rolle, der omfatter vidt forskellige teknologier. Det er forståeligt, at de ikke er eksperter i printerspecifik sikkerhed.

Ofte er det fagsproget, der er problemet. Mere end halvdelen (**51 %**) af SMV'erne siger, at der bruges for meget fagsprog i forbindelse med printersikkerhed, og det er særligt udtalt i Frankrig og Italien.

Næsten 60 % af SMV'erne siger, at de har en god forståelse for relevante sikkerhedsstandarder.

I den forbindelse har beslutningstagere typisk ikke en solid viden om de udbydere inden for printteknologi, der kunne være mest relevante for deres sikkerhedsbehov. Det er således ikke overraskende, at virksomheder kigger efter mærker, som de "ved" leverer sikre printere, uden helt at forstå, hvilke sikkerhedsforanstaltninger de i øjeblikket har eller ikke har på plads

Printerpartnere er nødt til at gøre mere for at hjælpe jer med at afkode de relevante sikkerhedsstandarder og sikre, at I vælger den bedste løsning til jeres virksomhed.



Brother Insights

På baggrund af kompleksiteten i printsikkerhed har Brother syv afgørende indsigter og anbefalinger, der kan hjælpe SMV'erne i deres indsats for at beskytte sig mod de omfattende økonomiske, juridiske og image-mæssige konsekvenser af datatab.



Inddrag ledelsen

Omfanget af de ødelæggelser, som cyberangreb og brud på datasikkerheden medfører, samt kravene i persondataforordningen (GDPR) betyder at printsikkerhed er nødt til at omfatte andet end IT-afdelingen. Sikkerhed må indgå på strategisk niveau, og virksomhedens Chief Information Officer (CIO) og Chief Information Security Officer (CISO) må involveres.



Gennemfør en grundig undersøgelse

Det er vigtigt, at virksomhederne afdækker eventuelle sårbarheder i printsikkerheden ved at sikre, at deres printmiljø inddrages i en regelmæssig gennemgang af sikkerheden. Dette er særligt vigtigt, hvis virksomheden har en blanding af nye og gamle enheder. I forbindelse med MPS-løsninger (Managed Print Services) tilbyder de fleste udbydere ikke alene komplette vurderinger; en evaluering vil også strukturere den løbende overvågning af printerne, når flåden er optimeret og sikret.



Skift forudindstillede administrator-passwords

Standard og forudindstillede passwords udgør et svagt punkt for printere – men den gode nyhed er, at det er let at fikse. Når printeren er installeret, skal du blot ændre passwordet til et stærkt og sikkert password.



Opdatér jeres firmware og patch

Potentielle sikkerhedsbrister for printere kan reduceres betydeligt ved at opdatere firmwaren og indstille enheden til automatiske opdateringer. Hvis du har spørgsmål hertil, kan du kontakte producenten af din printer og få rådgivning.



Beskyt printjobbene

Det er ikke kun printere, der har brug for beskyttelse, men også de dokumenter, du sender til udskrivning. En ende-til-ende-kryptering af netværkstrafikken gør overførslen af printjob til printerne sikker. Eftersom de fleste printere gemmer printjobbene midlertidigt, skal du sørge for, at dataene er krypteret.



Overvåg printerne

Hvis du kender printerens aktuelle status, får du et holistisk overblik over hele jeres printermiljø. Virksomheder bør overveje at anvende softwareværktøjer til at overvåge printerne og gøre det muligt straks at løse problemerne. Printere genererer en masse data, og disse kan ofte anvendes til at identificere mulige sikkerhedsproblemer og iværksætte hurtige foranstaltninger mod angreb. MPS-brugere kan også få regelmæssige rapporter, der inkluderer overvågning og rapportering af brud på datasikkerheden.



Uddan medarbejderne

Mange datatab sker utilsigtet, og det er derfor afgørende, at virksomhederne uddanner medarbejderne i vigtigheden af at beskytte følsomme informationer og øge opmærksomheden om trusler. Ofte vil MPS-udbydere kunne hjælpe med uddannelsesbehovene.



Afsluttende tanker

Printsystemer har muligvis været et overset aspekt inden for virksomheds-sikkerhed indtil nu, men SMV'erne indser i stigende grad vigtigheden af det. Der findes dog stadig betydelige udfordringer, når det kommer til at implementere printsikkerhed.

SMV'er er nødt til klart at definere ansvarsområder i forbindelse med printersikkerheden for at sikre, at deres maskiner er tilstrækkeligt beskyttet og holder trit med truslerne. Udover beskyttelsen af maskinerne er data-sikkerheden også vigtig at tage i betragtning, og virksomhedens medarbejdere skal samarbejde for at minimere risiciene.

Selv hvis ansvarsområderne er klart defineret i virksomheden, er det stadig en stor udfordring at have tilstrækkelig viden for effektivt at kunne håndtere printsikkerheden. Printteknologi bliver mere og mere kompleks, og det er en verden fuld af fagsprog. Virksomheder bør gå efter betroede leverandører, så de kan træffe fornuftige beslutninger.

Et effektivt print-setup skal være andet og mere end bare sikkert. De andre rapporter i Digital Transformation-serien fortæller mere om implementeringen af digitale workflows, maksimering af produktiviteten og arbejdet med at sikre, at dit setup er holdbart.

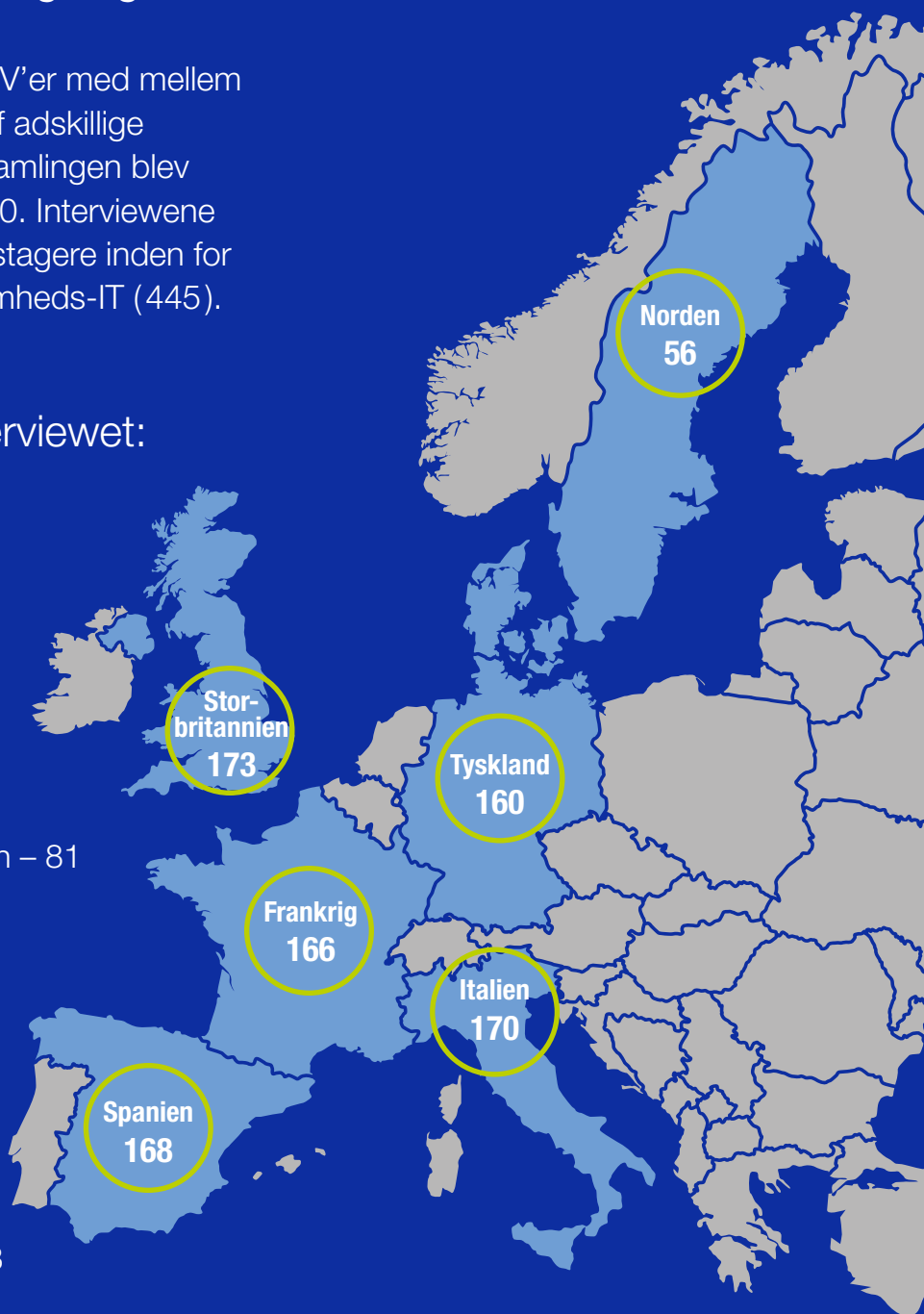
Vores undersøgelsesmetode

Denne rapport er baseret på 893 besvarelser af en online-undersøgelse blandt beslutningstagere.

Beslutningstagere, der arbejder i SMV'er med mellem 10 og 499 medarbejdere på tværs af adskillige vesteuropæiske markeder. Dataindsamlingen blev udført i 2019 og begyndelsen af 2020. Interviewene blev jævnt fordelt mellem beslutningstagere inden for strategisk forretning (448) og virksomheds-IT (445).

Nøgleindustrier, der blev interviewet:

-  Sundhed – 152
-  Detailhandel – 117
-  Logistik – 113
-  Hotel og restaurationsbranchen – 81
-  Transport og lager – 62
-  Liberale erhverv – 65
-  Produktion – 54
-  Finansielle tjenesteydelser – 53
-  Uddannelse – 51
-  Byggeri – 39



Yderligere interviews blev afholdt blandt andre brancher, herunder energi, medicinal, landbrug, forsvar, ejendomme og ejendomsmæglervirksomhed, sport og underholdning.

Få den nyeste viden

Vores næste rapporter i Brother Digital Transformation-serien, kommer snart.



brother

at your side

brother.dk

Brother Nordic A/S

Baldershøj 22

2635 Ishøj

Tlf. 43 31 31 31

salg@brother.dk

Alle specifikationer er korrekte på tidspunktet for udgivelsen og med forbehold for ændringer. Brother er et registreret varemærke tilhørende Brother Industries Ltd. Produktnavne er registrerede varemærker eller varemærker tilhørende de respektive virksomheder.