

Sørge for et sikkert økosystem for utskrift

En del av Brother sin serie
om digital transformasjon



Hindringer for investering i utskriftssikkerhet

Brudd på personvernet og hacking utgjør en stadig større trussel, og de fleste små og mellomstore bedrifter (SMB-er) er fullt klar over behovet for å beskytte IT-systemene sine.

Å håndtere sikkerheten til IT-ressursene er en utfordring som krever et helhetlig perspektiv. Skrivere, skannere og kopimaskiner må være like sikre som annet IT-utstyr. Hvis vi overser dem, kan de gi hackere en enkel vei inn i organisasjonen. SMB-er blir stadig mer klar over hvor viktig dette er: **72 %** av bedriftene sier det er avgjørende at skriverne, skannerne og kopimaskinene deres er sikre. Dette er ekstra viktig i organisasjoner som behandler sensitiv informasjon, for eksempel i tjenestebedrifter (**82 %**) og i helsesektoren (**81 %**).

Likevel ser vi at nesten en tredjedel av organisasjonene ikke erkjenner hvor viktig det er. Samtidig føler nesten halvparten at organisasjonene deres ikke har investert nok i skriftersikkerhet.

Men hvis bedriftene forstår behovet for å investere i skriftersikkerhet, hvorfor gjør de det ikke?

Forskningen vår tyder på at det er to klare grunner:



Uklare ansvarsområder knyttet til skriftersikkerhet



Manglende forståelse av og kunnskap om sikkerhetstrusler og -standarder

Hensikten med denne rapporten er å hjelpe beslutningstakere i SMB-er med å forstå hvor viktig utskriftssikkerhet er, samt hvordan de kan implementere sikre utskriftsløsninger. Den inngår i en serie der formålet er å informere beslutningstakere om hvordan de best kan utnytte digital teknologi i SMB-er. Rapportene er basert på omfattende forskning som er gjennomført blant beslutningstakere i SMB-er i EMEA-regionen*. Serien består av fire rapporter, én for hvert av følgende temaer:

- digitale arbeidsflyter
- implementering av riktig løsning for din bedrift
- sikkerhet
- bærekraft

*Europa, Midtøsten og Afrika



Hvem er ansvarlig for skriver-sikkerheten?

Altfor ofte er det uklart hvem som har ansvaret for skriverversikkerhet. Nesten halvparten av SMB-ene i Vest-Europa **(44 %)** oppgir at det er uklart hvem som har ansvaret for skriverversikkerheten i organisasjonen de tilhører. Hvis ansvarsområdene er uklare, er det sannsynlig at beslutningstaking og implementering knyttet til skriverversikkerhet blir skadelidende, noe som gjør bedriftene sårbare.

At ofte ingen har ansvaret for skriverversikkerhet, kan skyldes at utskriftsløsningen ikke har vært ansett som et «svakt punkt» på samme måte som andre enheter, for eksempel bærbare datamaskiner. Selv om forskningen vår viser at beslutningstakere er i ferd med å innse at utskriftssikkerhet er viktig, gjenspeiler ikke jobbrollene i SMB-ene dette ennå.

SMB-er er spesielt sårbare, siden ansvaret for all maskinvare og programvare i hele organisasjonen ofte ligger hos noen få medarbeidere. Hvis IT-medarbeiderne ikke er klar over risikoen forbundet med utskriftssikkerhet, kan den bli lavt prioritert.

Alle medarbeiderne i organisasjonen har imidlertid en del av ansvaret for å ivareta sikkerheten til sensitiv informasjon.



Selv om IT- og teknologispesialister har ansvaret for sikkerheten til selve enhetene, er medarbeiderne ansvarlige for at informasjonen er sikker. Informasjonssikkerhet er kanskje det største risikoområdet for forretningssensitiv informasjon.

Informasjonssikkerhet omfatter en rekke ulike trusler, blant annet:



uautorisert tilgang til utskrifter



manglende utlogging etter utskrift av fortrolige dokumenter



manglete sporing av hvem som har hatt tilgang til hvilke dokumenter på skriveren

Nesten 9 av 10 bedrifter har opplevd en skriverrelatert sikkerhetshendelse ...



... og sju av ti (**72 %**) mener at informasjonssikkerhet er en større trussel enn enhetssikkerhet. Per i dag sier imidlertid færre enn én av tre bedrifter at de har stor tillit til at infrastrukturen deres for utskrift omfatter tilstrekkelige sikkerhetstiltak. Til sammenligning mener **53 %** av bedriftene at de har tilstrekkelig maskinvaresikkerhet på plass.

Flertallet av SMB-ene (**64 %**) sier også at de prioriterer informasjonssikkerhet høyt. Dette anses som en sentral utfordring og kan være en reell hindring for effektiv ytelse.

Per i dag sier nesten halvparten av SMB-ene (**48 %**) at de har få eller ingen prosesser som gjør at de kan finne ut hvem som skriver ut eller henter utskriftsjobber. Det kommer ikke som noen overraskelse at nesten ni av ti bedrifter (**86 %**) oppgir at de har hatt en utskriftsrelatert sikkerhetshendelse.

Disse sikkerhetshendelsene skyldes som oftest at fortrolige dokumenter blir liggende uten tilsyn på skriveren, at utskrifter ikke blir hentet, eller at medarbeidere får tak i fortrolige dokumenter som tilhører andre.

Som et resultat av dette har de fleste SMB-ene (**64 %**) begynt å iverksette tiltak for å håndtere utskriftsrelaterte sikkerhetsproblemer ved å begrense tilgangen til visse skrivere eller innføre ID-kort/PIN-koder for å levere utskriftsjobber til riktige personer.

Dette er et steg i riktig retning. De neste årene vil det være viktig at alle bedrifter innfører sikrere prosesser, og at de som allerede er i gang, ivaretar og forbedrer ansvarsfordeling og revisjonsspor.

Reell informasjonssikkerhet har tre hovedmål.

De omfatter både enhets- og informasjonssikkerhet:

Fortrolighet

Beskytte fortrolig forretningsinformasjon for å sikre at den bare deles med den planlagte mottakeren. Til det trenger man autentiserings- og autoriseringstiltak som krever at brukerne bekrefter identiteten sin, og at de har rettigheter til å gjøre det de prøver å gjøre, før de får tak i utskriften.

Integritet

Sørge for at enhetens maskinvare er sikker og motstandsdyktig mot hacking og andre eksterne trusler.

Tilgjengelighet

Sørge for at enheten fungerer, og at den er tilgjengelig for autoriserte brukere som skal utføre viktige arbeidsoppgaver.

Mangel på kunnskap bidrar til dårlig sikkerhetspraksis

Færre enn en tredjedel (**32 %**) av sentrale IT-beslutningstakere i SMB-er sier at de har avansert kunnskap om teknologisikkerhet og potensielle trusler. Hvis IT-beslutningstakere ikke har tilstrekkelige kunnskaper om trusler, vil bedriftene oppleve stadige problemer med å iverksette egnede tiltak for å beskytte seg selv. I SMB-er har IT-beslutningstakeren vanligvis en rolle som omfatter mange ulike typer teknologi. Det er forståelig at de ikke er eksperter på skrifterspesifikk sikkerhet.

Ofte er det sjargongen som har skylden. Over halvparten (**51 %**) av SMB-ene sier at det brukes for mye sjargong i forbindelse med skriftersikkerhet, og dette er spesielt tilfellet i Frankrike og Italia.

Og nesten 60 % av SMB-ene sier at de har god forståelse av relevante sikkerhetsstandarder.

På bakgrunn av dette er det også usannsynlig at beslutningstakere har pålitelig kunnskap om hvilke leverandører av utskriftsteknologi som kan være mest relevante for sikkerhetsbehovene deres. Derfor er det ikke overraskende at bedrifter satser på merker de «vet» lager sikre skrivere, uten egentlig å forstå hvilke sikkerhetstiltak de allerede har eller ikke har iverksatt.

Skriverpartnere må gjøre mer for å hjelpe deg med å forstå de relevante sikkerhetsstandardene og for å sikre at du velger den beste løsningen for din bedrift.



Innsikt fra Brother

Utskriftssikkerhet er et komplekst område, og Brother har sammenfattet sin innsikt i sju viktige anbefalinger for å hjelpe SMB-er med å beskytte seg mot de omfattende økonomiske, juridiske og omdømmemessige konsekvensene av datatap.



Få styret med i styringen

Omfanget av ødeleggelsene cyberangrep og datainnbrudd forårsaker, i kombinasjon med kravene i personvernforordningen (GDPR), tilsier at utskriftssikkerhet må være et felt som strekker seg utover IT-avdelingens domene. Dette må vurderes strategisk på styrenivå, og CIO (Chief Information Officer) og CISO (Chief Information Security Officer) må involveres.



Gjennomfør en grundig revisjon

Det er helt avgjørende at bedrifter avdekker eventuelle sårbarheter knyttet til utskriftssikkerhet, ved å sørge for at utskriftsmiljøet omfattes av regelmessige sikkerhetsrevisjoner. Dette er spesielt viktig hvis bedriften har en blanding av nye og gamle enheter. Når det gjelder Managed Print Services (MPS), tilbyr de fleste leverandører ikke bare fullstendige vurderinger, men også en evaluering som strukturerer den pågående overvåkingen av enheter så snart utstyret er optimalisert og sikret.



Endre forhåndsinnstilte admin-passord

Standardpassord eller forhåndsinnstilte admin-passord er et svakt punkt for utskriftsenheter – den gode nyheten er at det er enkelt å gjøre noe med det. Endre ganske enkelt passordene så snart enheten er installert, og velg sterke og sikre passord.



Oppdater fastvaren og patchen

Potensielle sikkerhetssårbarheter for utskriftsenheter kan reduseres betydelig ved at fastvaren oppdateres og enheten konfigureres for automatiske oppdateringer. Hvis du har spørsmål angående dette, ber vi deg om å kontakte produsenten av utskriftsenheten for å få råd.



Beskytt utskriftsjobber

Det er ikke bare utskriftsenheter som trenger beskyttelse. Det gjør også dokumentene dere sender til utskrift. Ende-til-ende-kryptering av nettverkstrafikk sørger for sikker overføring av utskriftsjobber til skrivere. Fordi de fleste skrivere lagrer utskriftsjobber midlertidig, må dere sikre at dataene krypteres.



Overvåk enheter

Når du er kjent med gjeldende status for bedriftens utskriftsenheter, får du et helhetlig perspektiv på hele utskriftsmiljøet. Bedrifter bør vurdere å bruke programvareverktøy for å overvåke enheter, slik at feil rettes opp så snart de oppstår. Enheter genererer en mengde data, og disse kan ofte brukes til å identifisere potensielle sikkerhetshendelser og muliggjøre raske svar på angrep. MPS-brukere kan også få regelmessige samsvarsrapporter, som bør innbefatte overvåking og rapportering av datainnbrudd.



Lær opp medarbeiderne

Fordi datatap ofte skjer utilsiktet, er det avgjørende at bedrifter lærer opp medarbeiderne i viktigheten av å beskytte sensitiv informasjon, og skaper større bevissthet om ondsinnede trusler. MPS-leverandører tilbyr ofte å hjelpe til med opplæring.



Noen tanker til slutt

Utskriftssystemer kan tidligere ha blitt oversett i forbindelse med organisasjonssikkerhet, men SMB-er erkjenner i økende grad hvor viktige de er. Likevel er det betydelige utfordringer forbundet med å implementere utskriftssikkerhet.

SMB-er må definere klare ansvarsområder knyttet til skriftersikkerhet for å sikre at enhetene har tilstrekkelig beskyttelse og holder tritt med trusselutviklingen. I tillegg til enhetssikkerhet er informasjonssikkerhet viktig, og samarbeid mellom interne medarbeidere vil være nødvendig for å minimere risikoen for datainnbrudd.

Selv om ansvarsområdene i en SMB er klart definerte, er det fortsatt en stor utfordring å ha nok kunnskap til å kunne håndtere utskriftssikkerhet på en effektiv måte. Utskriftsteknologi er et stadig mer komplekst område, og det brukes mye sjargong. Bedrifter bør rådføre seg med leverandører de stoler på, for å ta fornuftige beslutninger.

Det kreves mer av en effektiv utskriftsløsning enn at den er sikker. De andre rapportene i serien om digital transformasjon inneholder mer informasjon om å implementere digitale arbeidsflyter, maksimere produktiviteten og sørge for at løsningen er bærekraftig.

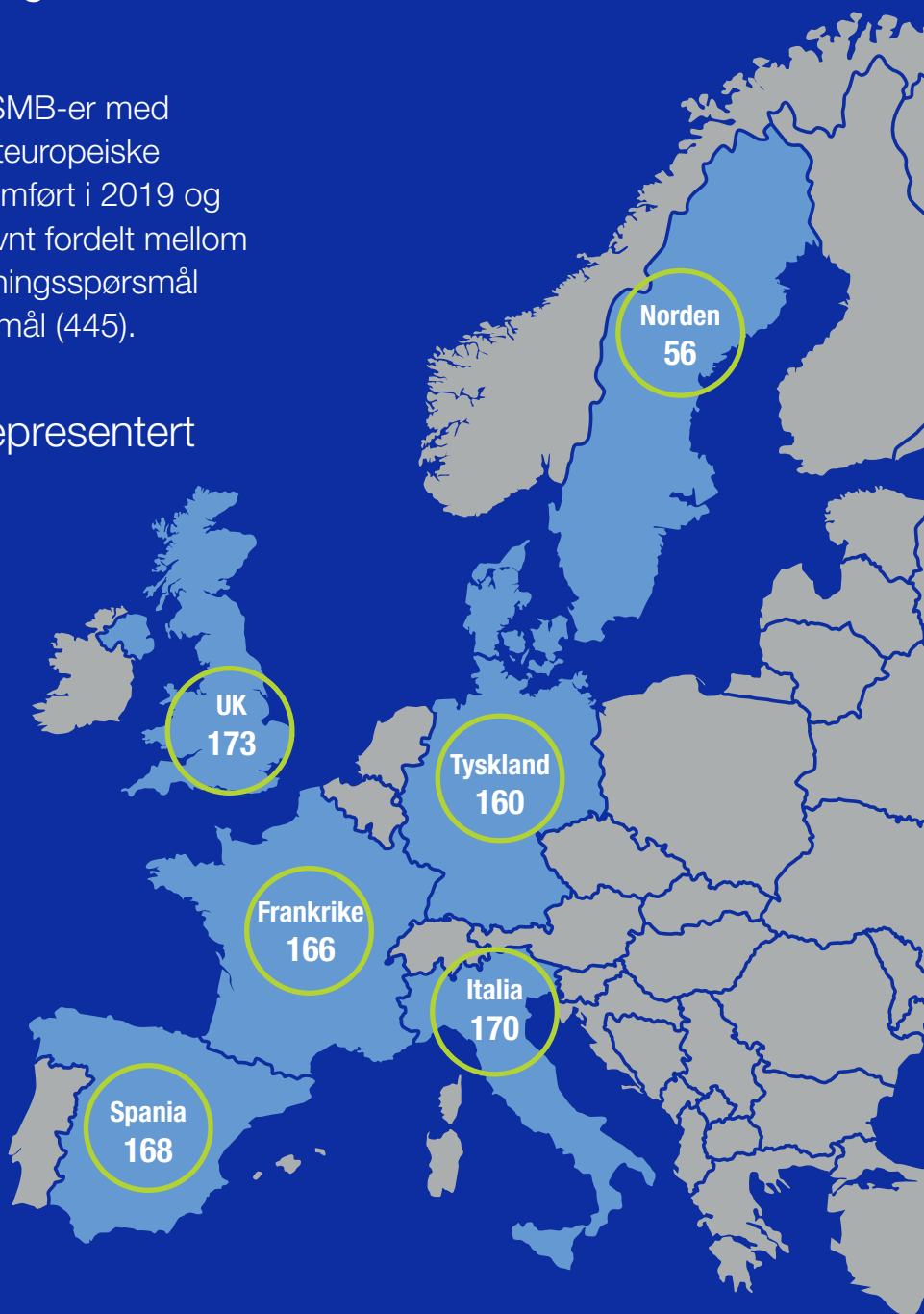
Vår metode

Denne rapporten er basert på 893 nettbaserte spørreundersøkelser blant beslutningstakere i IT- og forretningsspørsmål.

Disse beslutningstakerne arbeider i SMB-er med mellom 10 og 499 ansatte i flere vesteuropeiske markeder. Undersøkelsen ble gjennomført i 2019 og første del av 2020. Intervjuene var jevnt fordelt mellom beslutningstakere i strategiske forretningsspørsmål (448) og beslutningstakere i IT-spørsmål (445).

Bransjene som primært er representert i undersøkelsen:

-  Helse – 152
-  Detaljhandel – 117
-  Logistikk – 113
-  Hotell og restaurant – 81
-  Transport og lager – 62
-  Tjenestebedrifter – 65
-  Produksjon – 54
-  Finansieringsvirksomhet – 53
-  Utdanning – 51
-  Bygg og anlegg – 39



Det ble også gjennomført intervjuer i bransjer som energi, legemiddelindustri, jordbruk, forsvar, eiendom, sport og underholdning.

Forskningen ble gjennomført av markedsundersøkelsesfirmaet Savanta.

Få oppdatert kunnskap

De neste rapportene i Brother sin serie om digital transformasjon.

Kommer snart



brother

at your side

www.brother.no

Brother Norge, filial til Brother Nordic A/S

Karvesvingen 5, 0579 Oslo

www.brother.no

Alle spesifikasjoner er korrekte på utgivelsestidspunktet og kan endres. Brother er et registrert varemerke for Brother Industries Ltd. Produktmerkenavn er registrerte varemerker eller varemerker for sine respektive selskaper.