

Att upprätthålla ett säkert utskriftssystem

En del i Brothers rapportserie
om digital omvandling



Hinder för investeringar i utskriftssäkerhet

Med tanke på den ökade risken för sekretessbrott och hackerattacker med stora konsekvenser är de flesta små och medelstora företag (SMF) mycket väl medvetna om behovet av att skydda sina IT-system.

Säkerheten för IT-systemet är en utmaning som måste hanteras med ett helhetsgrepp. Skrivare, skannrar och kopiatorer måste vara precis lika säkra som den övriga IT-utrustningen. Om de inte är det riskerar de här enheterna att ge potentiella hackare en enkel väg in i organisationen. SMF blir allt mer medvetna om den här frågans betydelse, och **72 %** anser att det är viktigt att deras skrivare, skannrar och kopiatorer är säkra. Det här har ännu högre prioritet för organisationer som hanterar känsliga uppgifter, till exempel tjänsteföretag (**82 %**) och sjukvårdsaktörer (**81 %**).

Men det är ändå så att närmare en tredjedel av företagen fortfarande inte inser vikten av detta. Samtidigt anser knappt hälften att deras organisation inte har investerat tillräckligt i utskriftshårdvarans säkerhet.

Så om företagen är medvetna om behovet av att investera i utskriftssäkerheten, varför gör de då inte det?

Vår studie visar på två tydliga skäl:



Otydlig ansvarsfördelning för utskriftssäkerheten



Bristande förståelse och kunskap om säkerhetsrisker och -standarder

Målet med den här rapporten är att hjälpa beslutsfattare på SMF att inse vikten av utskriftssäkerhet samt förstå hur de ska implementera säkra utskriftslösningar. Den ingår i en serie rapporter som syftar till att informera beslutsfattare om hur de bäst utnyttjar digital teknik på SMF. Samtliga rapporter bygger på en omfattande forskningsstudie som genomförts bland beslutsfattare på SMF i EMEA-regionen. Serien består av fyra rapporter som behandlar fyra olika teman:

- Digitala arbetsflöden
- Implementera rätt lösning för ditt företag
- Säkerhet
- Hållbarhet



Vem ansvarar för utskriftssäkerheten?

Alltför ofta är ansvarsfördelningen när det gäller utskriftssäkerheten otydlig. Närmare hälften av alla SMF i Västeuropa (**44 %**) anger att det är oklart vem som ansvarar för utskriftssäkerheten i deras organisation. När ansvarsskyldigheten brister leder det sannolikt till att även beslutsfattandet kring och implementeringen av utskriftssäkerheten blir lidande, vilket gör företagen sårbara.

Ansaret för utskriftssäkerheten faller ofta mellan stolarna, eftersom skrivare traditionellt inte har setts som "svaga punkter" på samma sätt som andra enheter, till exempel bärbara datorer. Trots att vår studie visar att beslutsfattarna har börjat inse vikten av utskriftssäkerhet verkar ansvarsfördelningen inom SMF inte återspegla det här ännu.

SMF är särskilt sårbara för bristande ansvarsskyldighet, eftersom det ofta bara är ett fåtal medarbetare som har hand om hela företagets hård- och mjukvara. Om de IT-ansvariga inte är medvetna om riskerna i samband med utskriftssäkerheten får frågan ofta lägre prioritet.

Men alla medarbetare på ett företag har någon form av ansvar för att se till att känsliga uppgifter skyddas.



Även om IT- och teknikspecialisterna ansvarar för säkerheten för själva enheterna är medarbetarna ansvariga för att skydda den information som finns i dem. Datasäkerheten är kanske det största riskområdet för kommersiellt känslig företagsinformation.

Datasäkerheten är föremål för en rad olika hot, bland annat



obehöriga personer som får åtkomst till utskrifter



användare som glömmer att logga ut efter att ha skrivit ut konfidentiella dokument



bristande spårbarhet för vilka som har haft åtkomst till olika dokument i skrivaren.

Närmare 9 av 10 företag har varit med om en skriverrelaterad säkerhetsincident ...



... och **72 %** anser att datasäkerhet är ett större hot än enheternas säkerhet. Ändå svarar färre än ett av tre företag att de är mycket säkra på att deras skrivarinfrastruktur omfattas av tillräckliga säkerhetsåtgärder. Detta kan jämföras med de **53 %** av företagen som anser att de har rätt säkerhetsåtgärder på plats för sin hårdvara.

64 % av alla SMF svarar dessutom att en av deras främsta prioriteringar är att säkerställa att deras data skyddas. Detta ses som en svår utmaning och kan vara ett stort hinder för effektiviteten.

För närvarande svarar **48 %** av alla SMF att de bara har ett fåtal eller helt saknar processer för att kontrollera vilka som skriver ut eller hämtar dokument i skrivaren. Det är ingen överraskning att närmare nio av tio företag (**86 %**) uppger att de har drabbats av en utskriftsrelaterad säkerhetsincident.

De här säkerhetsincidenterna är ofta kopplade till konfidentiella dokument som lämnas obehövade i skrivaren, utskrifter som aldrig blir upphämtade eller medarbetare som hämtar konfidentiella dokument som inte är deras.

Till följd av detta har många SMF (**64 %**) börjat vidta åtgärder för att hantera utskriftsrelaterade säkerhetsrisker, genom att begränsa åtkomsten till vissa skrivare eller införa ID-kort/PIN-koder så att bara rätt person kan hämta en utskrift.

Det här är ett steg i rätt riktning. Under kommande år är det viktigt för alla företag att implementera säkrare processer. De som redan har påbörjat det här arbetet måste upprätthålla och förbättra ansvarsfördelningen och spårbarheten.

Informationssäkerheten har tre huvudsakliga mål, som ofta kallas CIA-triangeln.

Dessa omfattar både enhets- och datasäkerhet:

Konfidentialitet (Confidentiality)

Att skydda konfidentiella affärsdata så att de bara delas med den avsedda mottagaren. Här ingår autentiserings- och auktoriseringsåtgärder som kräver att användarna verifierar sin identitet och bevisar att de är behöriga innan deras dokument skrivs ut.

Integritet (Integrity)

Att säkerställa att enhetens inbyggda programvara är säker och motståndskraftig mot hackare och andra externa hot.

Tillgänglighet (Availability)

Att säkerställa att enheten är i drift och tillgänglig så att behöriga användare kan utföra viktiga arbetsuppgifter.

Bristande kunskap leder till sämre säkerhetsrutiner

32 % av de IT-ansvariga på små och medelstora företag anger att de har avancerade kunskaper om teknisk säkerhet och potentiella hot. Om beslutsfattarna själva saknar tillräcklig kunskap om IT-hoten kommer företagen att ha fortsatta problem med att vidta rätt åtgärder för att skydda verksamheten. Inom SMF har den som fattar beslut i IT-frågor ofta ansvar för många olika tekniska frågor. Det är förståeligt att det saknas specifik och detaljerad kunskap om just utskriftssäkerhet.

Ofta upplevs terminologin som ett hinder. **51 %** av alla SMF upplever att det finns för många svåra termer kring utskriftssäkerhet, och problemet verkar vara särskilt tydligt i Frankrike och Italien.

Närmare 60 % av alla SMF anser att de har god kunskap om relevanta säkerhetsstandarder.

Det innebär att beslutsfattarna sannolikt inte har tillräcklig kunskap för att avgöra vilka leverantörer som är bäst lämpade att tillgodose deras behov av utskriftssäkerhet. Det är alltså ingen överraskning att företagen vänder sig till de varumärken de "känner till" för att få tillgång till säkra skrivare, utan att veta vilka säkerhetsåtgärder de för närvarande tillämpar och inte.

Din utskriftspartner måste kunna hjälpa dig att tyda relevanta säkerhetsstandarder och säkerställa att du väljer den bästa lösningen för just ditt företag.



Brothers tips

Med tanke på hur komplex frågan om utskriftssäkerhet är har Brother sju tips och rekommendationer för att hjälpa SMF att skydda sig från de omfattande konsekvenser som dataförlust kan få i form av ekonomiska och juridiska följder samt skadat rykte.



Få med styrelsen

De enorma skador som cyberattacker och dataintrång orsakar, i kombination med kraven från GDPR-lagstiftningen, innebär att utskriftssäkerhet måste lyftas till en högre nivå än IT-avdelningen. Det måste ses som en strategisk fråga som CIO:n (Chief Information Officer) och CISO:n (Chief Information Security Officer) är involverade i.



Gör en ordentlig kontroll

Det är oerhört viktigt att företag upptäcker potentiella säkerhetsbrister genom att se till att deras utskriftsrutiner genomgår regelbundna säkerhetskontroller. Det är extra viktigt om ditt företag har en blandning av nya och äldre enheter. Managed Print Services (MPS) innebär inte bara att de flesta leverantörer erbjuder en fullständig genomgång, de gör även en utvärdering för att utforma löpande övervakning när alla enheter har optimerats och säkrats.



Ändra förinställda adminlösenord

Standardlösenord eller förinställda adminlösenord är en svag punkt för skrivare, men som tur är kan detta problem lätt åtgärdas. När enheten har installerats är det bara att ändra lösenordet till ett starkt och säkert alternativ.



Uppdatera din inbyggda programvara och patch

Potentiella säkerhetsbrister för skrivare kan minskas avsevärt om den inbyggda programvaran uppdateras och enheten konfigureras för automatiska uppdateringar. Kontakta skrivartillverkaren för att få hjälp om du har frågor kring detta.



Skydda utskrifterna

Det är inte bara själva skrivaren som behöver skyddas, utan även de dokument du skriver ut. Totalsträckskryptering av nätverkstrafiken säkerställer skyddad överföring av utskrifter till skrivaren. Eftersom de flesta skrivare tillfälligt lagrar utskrifterna är det viktigt att se till att uppgifterna krypteras.



Övervaka dina enheter

Genom att känna till statusen för dina skrivare får du en helhetsbild av samtliga enheter. Företag bör använda programfunktioner för att övervaka sina enheter och åtgärda eventuella fel så snart de inträffar. Enheterna genererar en mängd data som ofta kan användas för att identifiera potentiella säkerhetsbrister och möjliggöra snabba åtgärder vid attacker. MPS-användare kan dessutom få regelbundna efterlevnadsrapporter, som bör innehålla intrångsövervakning och -rapportering.



Utbilda personalen

Eftersom många fall av dataförlust inträffar oavsiktligt är det oerhört viktigt att företagen informerar sin personal om vikten av att skydda känslig information och öka kännedomen om potentiella hot. Ofta kan MPS-leverantören hjälpa till med olika typer av utbildning.



Slutord

Utskriftssystemen har tidigare varit en säkerhetsaspekt som många SMF bortsett från, men nu börjar allt fler inse dess betydelse. Trots detta återstår många stora utmaningar vid implementeringen av tillräcklig utskriftssäkerhet.

SMF måste ange en tydlig ansvarsfördelning för utskriftssäkerheten för att säkerställa att enheterna är tillräckligt skyddade mot risker och hot.

Utöver enheternas säkerhet måste man även ta ställning till datasäkerheten, och de egna medarbetarna behöver vara delaktiga för att riskerna ska kunna minimeras.

Även om det finns en tydlig ansvarsfördelning inom vissa SMF är det fortfarande en stor utmaning att förfoga över tillräcklig kunskap för att effektivt kunna hantera utskriftssäkerheten. Utskriftstekniken blir allt mer komplex och präglas ofta av snårig terminologi. Företagen bör därför vända sig till tillförlitliga leverantörer för att få hjälp med att fatta rätt beslut.

En effektiv utskriftslösning måste vara mer än bara säker. Övriga rapporter i serien om digital omvandling innehåller mer information om hur du implementerar digitala arbetsflöden, maximerar produktiviteten och säkerställer att din lösning är hållbar.

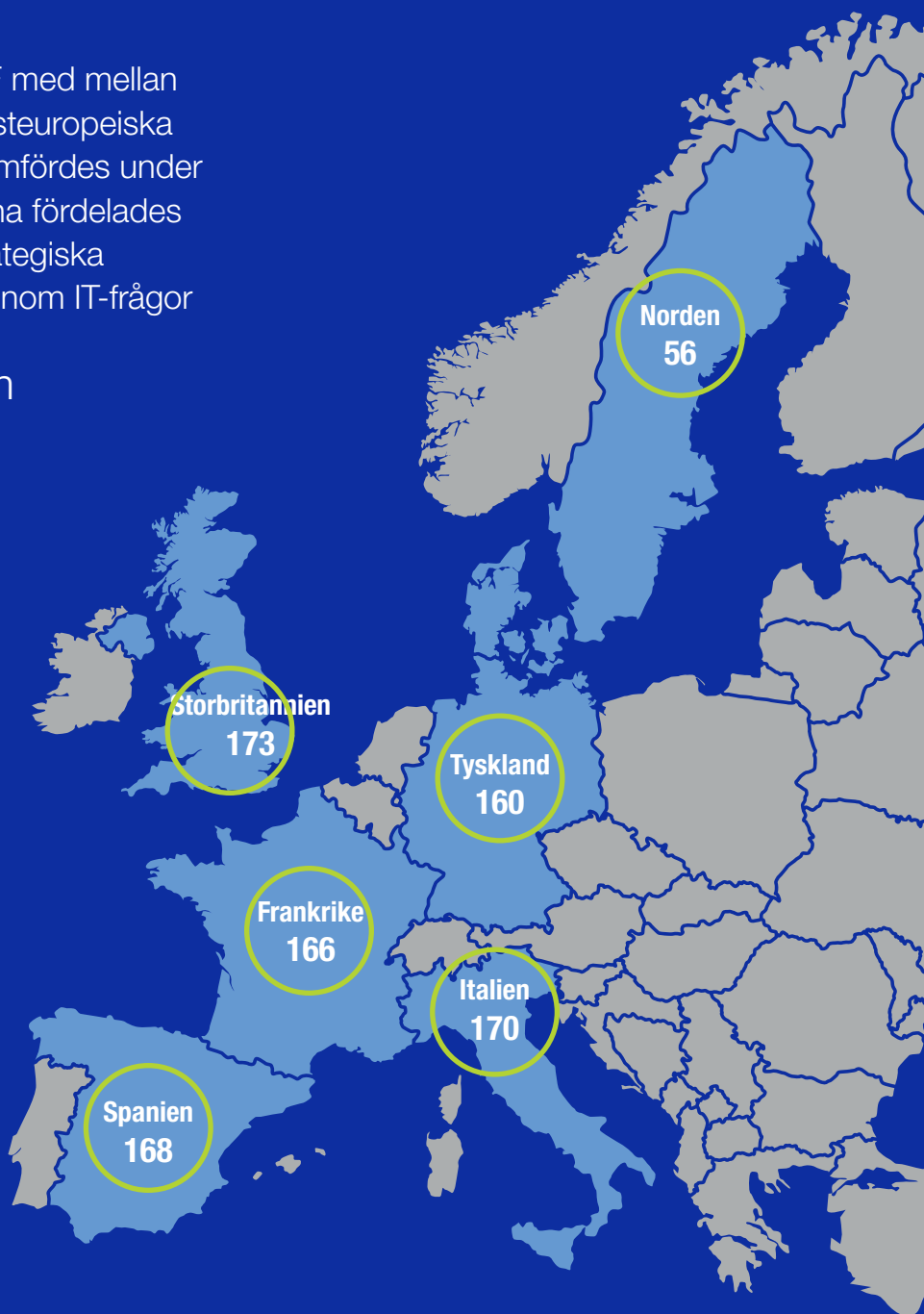
Om rapporten

Den här rapporten bygger på en onlineundersökning i form av 893 intervjuer med beslutsfattare inom IT- och affärsfrågor.

Dessa beslutsfattare arbetar på SMF med mellan 10 och 499 medarbetare på flera västeuropeiska marknader. Undersökningarna genomfördes under 2019 och början av 2020. Intervjuerna fördelades jämnt mellan beslutsfattare inom strategiska affärsfrågor (448) och beslutsfattare inom IT-frågor (445).

Huvudsakliga branscher som intervjuats:

-  Sjukvård – 152
-  Detaljhandel – 117
-  Logistik – 113
-  Hotell och restaurang – 81
-  Transport och lager – 62
-  Tjänsteföretag – 65
-  Tillverkning – 54
-  Finansiella tjänster – 53
-  Utbildning – 51
-  Byggnation – 39

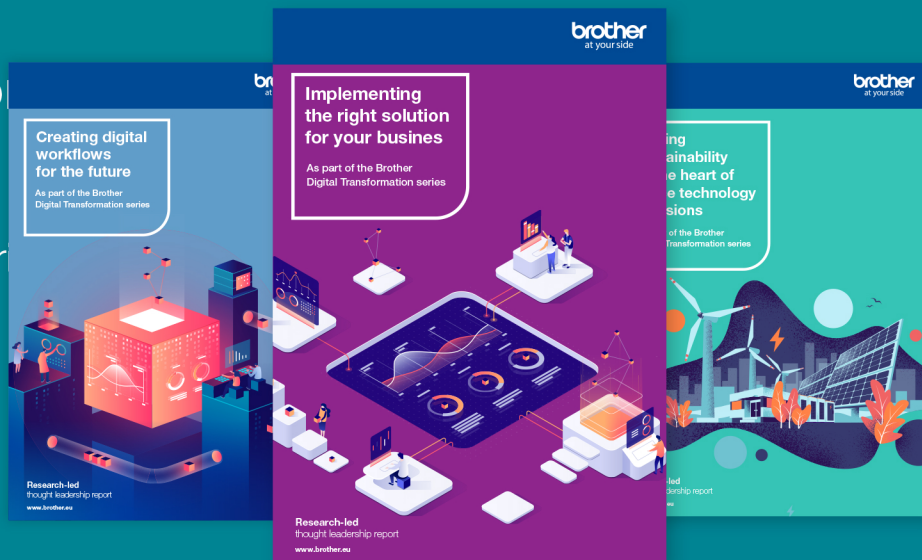


Ytterligare intervjuer genomfördes även inom andra branscher, bland annat energi, läkemedel, jordbruk, försvar, fastigheter, idrott och underhållning.

Få den senaste informationen

Övriga rapporter i Brothers serie om digital omvandling:

Kommer snart



brother

at your side

www.brother.se

Brother Sverige

Hulda Lindgrens gata 6B, 421 31 Västra Frölunda

Tel.: 031-734 12 00

Fax: 031-734 12 50

Samtliga specifikationer är korrekta vid trycktilfället och kan komma att ändras. Brother är ett registrerat varumärke som ägs av Brother Industries Ltd. Produktnamn är registrerade varumärken eller varumärken som ägs av respektive företag.