Faktablad om informationssäkerhet

Nätverkssäkerhet

Skydd av nätverksansluten kontorsutrustning

SHARP
Be Original.

www.sharp.se

Innehåll

Introduktion

I vår alltmer uppkopplade värld är det viktigare än någonsin att företagets information är effektivt skyddad i hela nätverket.

Varje dag förekommer otaliga skadliga incidenter som syftar till att stjäla, illegalt modifiera, avlyssna eller sprida konfidentiell information, eller skaffa sig obehörig åtkomst till privata nätverk och företagsnätverk. I det här faktabladet undersöker vi de utmaningar som företag ställs inför när det gäller skydd av den egna IT-miljön, inklusive nätverksanslutna kontorsmaskiner såsom multifunktionssystem och skrivare.

Vi analyserar:

- **Bakgrund**
  Alla företag ägnar mycket uppmärksamhet och resurser åt nätverkssäkerhet, men de sårbarheter som blottas via moderna nätverksanslutna multifunktionssystem och skrivare förbises ofta. Inkräktare och cyberkriminella utnyttjar sådan utrustning som inkörsport till organisationens nätverk för att stjäla konfidentiella data lagrade på hårddiskar och andra nätverksanslutna enheter, och/eller orsaka skador eller störningar i verksamheten. Inverkan på produktivitet och lönsamhet kan bli enorm.

- **Problem**
  Den risk som oskyddade multifunktionssystem och skrivare utgör missförstås och ignoreras ofta, eller så saknar företaget expertis och resurser för att ta itu med problemet. Dessutom förvärras problemet av användarnas aningslöshet och dåliga vanor som gör att obehöriga kan få åtkomst till dokument och data. Många företag inser vilka steg de måste ta för att utarbeta en policy för säker utskrift, men detta kan vara en komplex och tidskrävande process.

- **Rekommendationer**
  Nedan specificeras program- och hårdvarulösningar samt effektiva rutiner som företaget kan använda för att skapa en säker utskriftsmiljö och därmed förhindra obehörig åtkomst och intrång i nätverksanslutna enheter. Detta avsnitt innehåller konkreta åtgärder för några av de viktigaste säkerhetshoten:

  - Sex steg för att ta fram en hållbar policy för utskriftssäkerhet med hjälp av en kombination av Sharp-teknik och Sharps optimerade mjukvarulösningar.
  - Driftklara funktioner och inställningar hos alla nuvarande nätverksanslutna Sharp-utrustningar, till exempel lösenordsskydd, dataöverskrivning och kryptering.
  - Tillvalslösningar för en enhetlig policy för säker utskrift och enkel och effektiv administration av en hel maskinpark, till exempel Sharp Remote Device Manager (SRDM).
  - Avancerade tillvalslösningar för multifunktionssystem och skrivare, till exempel datasäkerhetskit (DSK).
  - Tillvalstjänster via Sharps säljkanaler, till exempel säkerhetsanalys, säkerhet som tjänst och dataradering vid leasingperiodens slut.

- **Slutsats**
  Vi kan ge en sammanfattning enligt följande:

  - Sårbarhetsresultat avseende företagets alla nätverksanslutna multifunktionssystem och skrivare
  - Rekommendationer baserade på inbyggda Sharp-funktioner och ytterligare säkerhetslösningar från Sharp
  - Nästa steg till en policy för säker utskrift; kan utarbetas via interna resurser eller med hjälp av Sharp Professional Services-teamet.

Bakgrund

På senare tid har behovet av effektiv IT-säkerhet fått betydligt mer uppmärksamhet; emellertid har ett viktigt område försummats allvarligt.

De flesta säkerhetsmedvetna organisationer har sett till att skydda nätverk och data med hjälp av modern teknik: brandväggar, lösenordsregler, användarautentisering, kryptering och digital signering av data med mera.

Ny teknik i form av molntjänster och mobiler har skapat ytterligare utmaningar för IT-administratörer och säkerhetschefer. Moderna, intelligenta multifunktionssystem och skrivare har emellertid utvecklats i snabb takt och har många funktioner för nätverkskommunikation och datalagring. De har i praktiken utvecklats till kraftfulla datorer med smarta funktioner. Enligt IDC finns det nästan 53 miljoner skrivare och multifunktionssystem i kontors- och hemmiljö i Väst- och Östeuropa[1], och de flesta är nätverksanslutna. Det innebär att de utgör en anslutningspunkt med en IP-adress och är exakt lika känsliga för sabotageprogram och intrångsattacker som datorer eller andra nätverksanslutna slutpunkter. Således behövs lika avancerade säkerhetsfunktioner för data, kommunikation och information för skydd av dessa enheter.

Om ett multifunktionssystem är oskyddat kan inkräktare få tillgång till oövervakade portar och protokoll, och därmed komma åt andra enheter i nätverket, eller konfidentiell information. Kommunikationsuppgifter och data lagrade på multifunktionssystemets hårddisk eller i dess minne kan fångas upp eller skickas vart som helst i världen. Oskyddade nätverksanslutna enheter saknar även skydd mot överbelastningsattacker (DoS). Dessa syftar till att blockera användarnas tillgång till företagets nätverksresurser, vilket följaktligen inverkar negativt på produktiviteten. De kan även utgöra en oskyddad inkörsport för nätfiskeattacker i syfte att komma åt konfidentiell information eller smitta nätverket med virus.

25 % av de IT-incidenter som krävde åtgärder var utskriftsrelaterade.[2]

Och det här är inga överdrifter, utan ett mycket verkligt hot. I en nyligen genomförd IDC-undersökning hade mer än en fjärdedel av de svarande råkat ut för en allvarlig IT-incident som krävde åtgärder, och mer än 25 % av dessa incidenter var utskriftsrelaterade.[2]

Om multifunktionssystem och skrivare inte skyddas kan följden bli förödande skador för såväl verksamheten som företagets rykte och förtroende. Effekterna av ett intrång kan bestå av:

- Intäktsförluster
- Förlorad produktivitet till följd av att användarna inte har tillgång till data och nätverket
- Förlorad konkurrenskraft till följd av stulen information
- Straffavgifter eller böter till följd av brist på regelefterlevnad
- Rättsprocesser
- Obehörig användning av utrustning och nätverksresurser

Problem

Intrång och cyberattacker har blivit "norm", och oavsett ditt företags typ eller storlek så är risken för intrång och attacker som kommer att beröra din verksamhet mycket verklig – och överhängande.

Det kanske förvånar dig att höra att enligt marknadsundersökningsföretaget Quocirca uppgav 63 % av företagen i undersökningen att de hade drabbats av en eller flera utskriftsrelaterade incidenter[3].

Så varför har inte företagen gjort mer för att avvärja detta hot?

Olyckligtvis negligeras ofta den potentiella risken på grund av brist på insikt i de sårbarheter som blottas när utrustning såsom multifunktionssystem och skrivare integreras i företagsnätverket. Många företag har därför inga, eller bristfälliga, system och verktyg för säker utskrift, inklusive utbildad personal, effektiva rutiner och säkerhetsrutiner relaterad till användning av nätverksansluten utrustning. Alternativt används utrustning i verksamheten som i själva verket är konstruerad för hemanvändning och som har begränsade säkerhetsfunktioner.

I synnerhet många små och medelstora företag har inte infört några utskriftssäkerhetsåtgärder alls eller gjort någon säkerhetsanalys. Större organisationer har ofta otillräckligt med personalresurser eller effektiva verktyg för att mäta, hantera och förhindra cyberattacker på nätverksansluten utrustning och likartad teknik.

Dessutom är olämpliga användarmönster ofta ett allvarligt problem för IT-administratören, och kan orsaka stora säkerhetsproblem i företaget. Några exempel är oskyddad utskrift, utskrifter som lämnas obevakade i multifunktionssystemets eller skrivarens utmatningsfack, utskrift från oskyddade USB-minnen, utskrift utan kryptering från slutpunkt till slutpunkt och lagring av känsliga dokument på multifunktionssystemets eller skrivarens hårddisk.

I många organisationer kan radering av data utgöra ett verkligt problem när ett multifunktionssystem eller en skrivare ska ersättas. Vid utskrift kan en kopia av utskriftsdata lagras på multifunktionssystemets eller skrivarens hårddisk. Så vad händer med dessa data när utrustningen ska ersättas?

Nästan två tredjedelar av företagen har drabbats av utskriftsrelaterade incidenter.[3]

Att konfigurera ett enhetligt och effektivt system för nätverkssäkerhet eller en policy för säker utskrift som detekterar och förhindrar obehörig åtkomst till en multifunktionssystems- och skrivarpark kan vara en verkligt komplex och tidskrävande uppgift. I de allra flesta fall behöver du gå igenom följande steg:

- Försök förutse och utvärdera potentiella följdverkningar av att det inte finns något system för nätverkssäkerhet
- Analysera befintliga potentiella risker och på vilket sätt dessa kan påverka nätverksinfrastrukturen negativt
- Var införstådd med att uppgiften är komplicerad, och att tillvägagångssätt och lösningar oundvikligen är olika från ett företag till ett annat
- Ta hjälp av en intern eller extern resurs
- Undersök vilka verktyg som kan övervaka en hel maskinpark, förhindra obehörig åtkomst till nätverkstillgångarna och larma vid misstänkta aktiviteter
- Konfigurera och administrera ett tillförlitligt system för nätverkssäkerhet som inbegriper alla de unika utmaningar som din verksamhet kan ställas inför

Rekommendationer

Allt detta har kanske lett till att du oroar dig för ditt företags nätverkssäkerhet … Ja, risken för verksamheten ska förvisso inte underskattas. Men låt dig inte avskräckas.

Vårt syfte är att presentera ett enkelt sätt att ta fram grundläggande åtgärder för utskriftssäkerhet för ditt företag, och visa hur Sharp kan hjälpa till att förmedla nödvändig insikt och på ett enkelt sätt höja nätverkssäkerheten.

Omedelbart skydd genast

Undersökningar som branschanalysföretaget IDC har utfört visar att "leverantörer av teknik för pappersbaserade utskrifts- och dokumenttjänster försöker skapa säkerhetslösningar som förhindrar att inkräktare tar sig in i företagsnätverket via skrivare" [4]. Många företag negligerar emellertid de inbyggda säkerhetsinställningarna, eller konfigurerar dem felaktigt, vilket kan göra nätverket tillgängligt för attacker.

Nedan är en lista över säkerhetsfunktioner och inställningar som är inbyggda i Sharps alla multifunktionssystem och skrivare som standard och som kan tjäna som en snabb åtgärd på kort sikt. Alla funktionerna kan snabbt aktiveras /inaktiveras eller anpassas av IT-administratören för ett effektivare skydd, beroende på typen av verksamhet:

- Lokala administrationsinställningar: ändring av administratörslösenord, åtkomst av webbsidor från skrivaren, fjärrstyrningssäkerhet
- Standardsäkerhetsfunktioner: portbaserad åtkomst, protokollinställningar, SNMP MIB, behörighetsfilter, SSL, S/MIME, IPSEC, IEEE802.1X, aktivering/inaktivering av protokoll för mobil utskrift, externa tjänster, publik mapp – nätverksadresserad server (delad disk), spårnings-ID (utskriftsspårning), användarinställningar, aktivering/inaktivering av provisoriska lösningar för användarsäkerhet, automatisk radering av lagrade filer, radering av utskriftskön vid fel
- Avancerade säkerhetsinställningar (i standardsäkerhetsläge): överskrivning (radering) av data på hårddisken efter varje jobb (kopiering/utskrift/scanning/faxning), lagringskryptering, lösenordsskydd
- I denna grupp finns dessutom ett antal avancerade tillvalsinställningar. Dessa inställningar ger IT-administratören tillgång till avancerade säkerhetsinställningar för organisationer som kräver högsta möjliga säkerhetsnivå såsom militära organisationer eller myndigheter, eller företag som vill höja sin säkerhetsnivå maximalt:

    - Datasäkerhetskit (DSK): installationsrutin för datasäkerhetskit, utökad datasäkerhet, utökad utskriftssäkerhet, validering av inbyggd programvara
    - Avancerat datasäkerhetskit (Advanced DSK): HCD-PP-certifierade avancerade säkerhetsfunktioner (inkluderar datasäkerhetskit), utökad lagringskryptering, utökat lösenordskrav, säkerhetskontroll av inbyggd programvara

Sex enkla steg

För hög säkerhet i ett längre perspektiv utgör följande sex steg ett strukturerat sätt att utarbeta och införa ett enhetligt ramverk för nätverkssäkerhet i ditt företag.

1. **Säker åtkomst av nätverket**
   Enheter som är anslutna till nätverket är inte säkrare än den sårbaraste punkten i nätverket. Övervakning av portar och protokoll är därför en mycket viktig aspekt om hög nätverkssäkerhet ska garanteras. Genom förnuftig konfigurering kan IT-administratören förhindra oönskade aktiviteter och potentiella attacker på infrastrukturen. Tekniker för att garantera säker kommunikation mellan skrivare och nätverket inkluderar:

    - IP-filtrering för begränsning av åtkomst till specifika IP-adresser, samt MAC-filtrering (Media Access Control). Detta bidrar till att skydda nätverket och kommunikations-kanalerna så att endast trafik via specificerade IP-adresser/intervall eller MAC-adresser medges.

- Genom att inaktivera oanvända portar får du ett extra säkerhetsskikt och ökad kontroll över nätverket genom att obehörig åtkomst till alla anslutna resurser förhindras.
- Säkerställ att IPSec (Internet Protocol Security för säker och krypterad datautväxling), TLS (Transport Layer Security för krypterad dataöverföring) och HTTPS (Hypertext Transfer Protocol Secure för säker nätverkskommunikation) är konfigurerade för maximal säkerhetsnivå.

2. Skydda enheten och dess data
Data lagrade på multifunktionssystemets eller skrivarens hårddisk kan skyddas på två olika sätt:

- Datakryptering krypterar dokument med hjälp av en komplex 256-bitars algoritm
- Dataöverskrivning är en dataraderingsfunktion för skrivarens hårddisk. Alla data lagrade på hårddisken samt digitala kopior av utskriftsjobb raderas permanent genom överskrivning upp till 10 gånger.

För extra säkerhet och trygghet erbjuder Sharp även ett tillval för radering av alla digitala data vid leasingperiodens slut som garanterar att alla data skrivs över och hårddisken förstörs.

3. Säker användarbehörighet (via användaridentifiering och användarautentisering)
Ett av de viktigaste stegen är att ha kontroll över alla användare via användaridentifiering och användarautentisering. De viktigaste funktionerna i denna kategori är:

- Via användaridentifiering har enbart registrerade användare tillgång till multifunktionssystem och skrivare. Användaren måste identifiera sig via antingen lokal autentisering baserad på den lokala användarlistan, eller nätverksautentisering via autentiseringsservern.

- Användaridentifiering används för att medge åtkomst till organisationens nätverksanslutna resurser och övervaka användningen av dessa. Beroende på aktuell konfiguration kan man tillåta åtkomst från enbart vissa användare, begränsa åtkomst till skrivarens olika funktioner eller helt blockera åtkomst. Administratören kan även konfigurera åtkomst till skrivarna via ID-kort där användarens identifieringsinformation är lagrad.

4. Säker utskrift av konfidentiell information
Konfidentiella dokument bör skrivas ut endast via en säker rutin som förhindrar obehörig åtkomst och kopiering. När ett utskriftsjobb skickas så lagras det på skrivarens hårddisk, och skrivs ut först när användaren har angivit sin PIN-kod, sitt användarnamn och lösenord eller kort/bricka vid skrivaren. Efter utskrift av dokumentet raderas alla data automatiskt från hårddisken.

5. Övervakning av nätverksaktiviteten
Korrekt konfigurerade funktioner för nätverkssäkerhet kan ge IT-administratören total kontroll över alla nätverksanslutna enheter direkt från sin dator. Denne kan därmed administrera en hel maskinpark med multifunktionssystem och skrivare, och dessutom detektera och åtgärda de flesta potentiella säkerhetshot på distans. Genom att klona enheter kan administratören arbeta effektivare och tryggare då alla inställningsändringar enkelt kan tillämpas på hela maskinparken.

6. Välj rätt partner
Många företag erbjuder professionella tjänster som är relaterade till utskriftssäkerhet; expertisnivån kan emellertid variera avsevärt. Sharp tar nätverkssäkerhet mycket seriöst och står i centrum för varje ny produktutveckling. I egenskap av tillverkare utvärderas våra utrustningar utifrån riktlinjerna för Common Criteria-certifiering. Våra nätverksanslutna multifunktionssystem med inbyggda säkerhetsfunktioner har utvärderats enligt det oberoende, globalt erkända Japan IT Security Evaluation and Certification (JISEC). Multifunktionssystemen har certifierats och följer den senaste standarden Protection Profile for Hardcopy Devices 1.0 (HCD-PP v1.0) för Common Criteria. Detta innebär att vi kan uppfylla kraven från kunder som hanterar även extremt känslig information.

Experthjälp

Trots att allt detta kan förefalla ganska nedslående är det viktigt att komma ihåg att du inte är ensam, och att det alltid finns experthjälp tillhands.

Sharp erbjuder exempelvis flera olika lösningar, verktyg och tjänster för att kontrollera och bedöma riskerna i ditt nätverk, förbereda ett förbättringsförslag och utarbeta möjliga säkerhetspaket:

- **Workshop i utskriftssäkerhet**
  Vi använder flera olika verktyg och tekniker för att förmedla insikt i vilka säkerhetshot som existerar, sammanställa slutsatser och utarbeta ett förbättringsförslag.

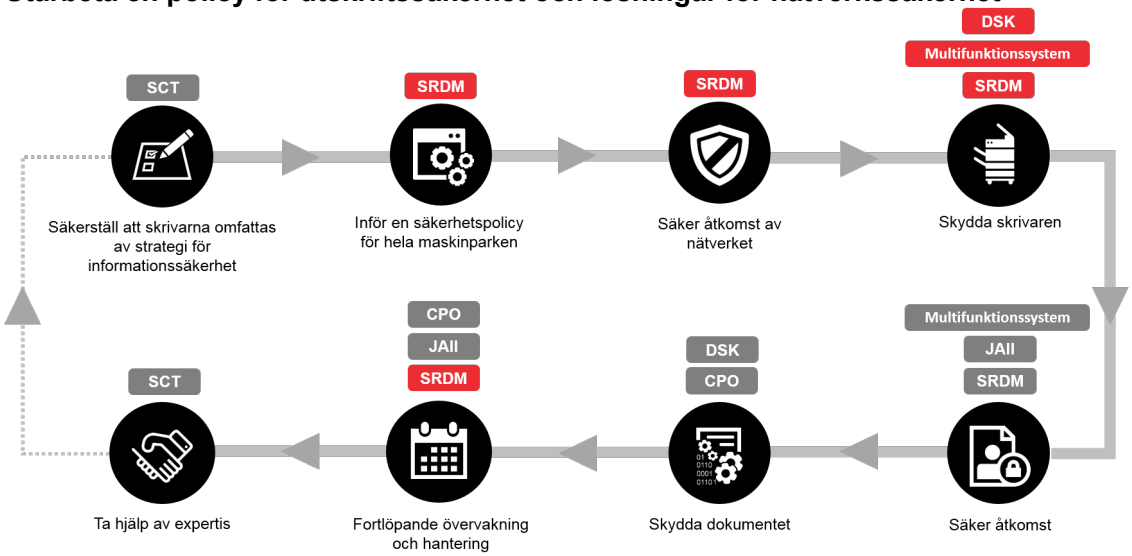
  Genomgången är inriktad på säkerhet avseende alla typer av nätverksansluten kringutrustning. Vi analyserar alla standardfunktioner och avancerade funktioner som finns tillgängliga för dessa enheter samt verktyg för effektiv hotdetektering och förebyggande åtgärder. Vi kontrollerar också om den utrustning som används i verksamheten är lämplig för ändamålet och om den kan ge verksamheten och användarna maximalt skydd. Dessutom specificerar vi nästa steg för en enhetlig policy för utskriftssäkerhet och går igenom alla säkerhetsaspekter i verksamheten:

  - Nätverkssäkerhet – allt som avhandlas i detta dokument
  - Utskriftssäkerhet – alla aktiviteter relaterade till utskriftshantering såsom utskrift, scanning, faxning och e-post
  - Dokumentsäkerhet – hantering av kontorets digitala filer och pappersdokument
  - Efterlevnad av den allmänna dataskyddsförordningen – säkerställer efterlevnad av EU:s nya regelverk för säkerhet och skydd av personuppgifter

- **Säkerhetspaket**
  En kombination av en kundworkshop och installation av Sharp Remote Device Manager, samt som tillval konfigurering och driftsättning av utskriftshanteringssystem som omfattar ytterligare aspekter av verksamhetens säkerhet; nätverkssäkerhet och utskriftssäkerhet.

- **Sharp Remote Device Manager (SRDM)**
  Med det här Sharp-verktyget implementerar du viktiga säkerhetsinställningar på några sekunder. Denna tjänst tillhandahålls av ett utbildat Sharp-team. Beroende på företagets behov och krav integreras alla relevanta säkerhetsinställningar i din IT-miljö, inklusive alla Sharp multifunktionssystem och skrivare.

Utarbeta en policy för utskriftssäkerhet och lösningar för nätverkssäkerhet



SCT – Sharp Consulting Team, **SRDM** – Sharp Remote Device Manager, **DSK** – Datasäkerhet, Multifunktionssystem, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Slutsats

Så vad har vi lärt oss? Den goda nyheten är att inte allt är dåliga nyheter!

Även om multifunktionssystem och skrivare förvisso utgör ett allvarligt – och underskattat – hot för företaget kan du vidta flera konkreta åtgärder för att minska risken.

- **Du är inte ensam – hoten finns överallt.** Varje dag kan vi läsa om dataintrång, cyberattacker, virus och andra typer av incidenter i företag av alla storlekar. Det som är viktigast att förstå är hur ditt företag skulle påverkas om det attackeras, och fråga dig själv "är mitt företag verkligen redo att försvara sig?”

- **Lösningen är inte alltid enkel.** Att förstå, konfigurera och utarbeta effektiva säkerhetsåtgärder och säkerhetsfunktioner kan ta lång tid och medföra stora implementeringssvårigheter. Alla organisationer är olika, och de verktyg och strategier som används måste vara anpassade för de specifika hot som kan vara aktuella för din verksamhet. Oavsett dina behov kan emellertid Sharp hjälpa dig att utarbeta en effektiv säkerhetslösning som skyddar företagets multifunktionssystem och skrivare.

- **Om ditt företag inte är förberett, försök förstå problemet.** Varför är företaget sårbart? Finns tillräckliga verktyg och resurser för att utarbeta eller förbättra säkerhetspolicyn för nätverk och utskrift? Eller gör du bäst i att låta Sharps specialister gå igenom företagets nätverk och nätverksanslutna kringutrustning och ta fram relevanta säkerhetsfunktioner?

- **Ställ upp egna säkerhetsmål.** Om du ska förstå företagets potentiella sårbarheter och vad som behöver skyddas måste du besvara frågorna “hur ser vår organisation ut om några år” och “hur kan jag förbereda företaget på de steg som behöver vidtas för att ta fram lämpliga åtgärder och verktyg som kan

Sharp Security Framework

förhindra cyberattacker, intrång etc i framtiden”.

- **Se till att ha tillgång till kompetent expertis.** Om du har tillgång till erforderliga resurser internt kan du själv utarbeta en policy för utskriftssäkerhet. Alternativt kan du låta Sharp Professional Services-teamet utarbeta ett effektivt säkerhetssystem och använda verktyg som är relevanta för din verksamhet och dina behov, såsom:

  - Säkra, nätverksanslutna Sharp-enheter som uppfyller de senaste säkerhetscertifieringarna
  - Utnyttja Sharps mjukvaror, lösningar och tjänster för att ta fram en policy för utskriftssäkerhet: Datasäkerhetskit, SRDM, säkerhetsanalys etc

- **Vi finns här när du behöver oss.** Vi kan säkerställa att du inte drabbas av oväntade förseningar vid analys och implementering av säkerhetspolicyn. Sharps experter hjälper dig att förstå företagets nuvarande säkerhetsnivå,

analysera den och föreslå en strategi för en enhetlig policy för utskriftssäkerhet som passar företagets behov och krav. Våra specialister hjälper till att välja relevanta verktyg och tjänster, såsom:

- Sharps standardsäkerhetsfunktioner
- Extra verktyg såsom SRDM
- Ytterligare utökningar såsom datasäkerhetskit
- Sharps säkerhetspaket för nätverk
- Sharps säkerhetsanalys
- Policy för utskriftssäkerhet

- **Beakta helheten, och skaffa dig en helhetsbild.** För att undvika potentiella risker inom andra områden av din organisation kan vi hjälpa till att höja den generella säkerhetsnivån med verktyg och tjänster från Sharps portfölj:

  - Nätverkssäkerhet
  - Utskriftssäkerhet
  - Dokumentsäkerhet
  - Efterlevnad av den allmänna dataskyddsförordningen.

Mer information om alla våra säkerhetslösningar finns i vårt faktabladsbibliotek, samt på sidorna med informationssäkerhet på vår webbplats: https://www.sharp.se/cps/rde/xchg/se/hs.xsl/-/html/skydda-din-information.htm

Du kan även kontakta din lokala Sharp återförsäljare.

Referenser

1. “Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years” IDC-rapport, 4:e kvartalet 2018
2. “IT and Print Security Survey 2015” IDC, september 2015
3. “Printing: a false sense of security”, Quocirca, 2013
4. “Transformative Technology in Document Security”, IDC, maj 2015

www.sharp.se

SHARP

Be Original.