Faktablad om informationssäkerhet

Utskriftssäkerhet

Skydda utskrifter och filer

www.sharp.se

SHARP
Be Original.

Innehåll

Introduktion

Behovet av att skydda pappersdokument eller filer genererade av multifunktionssystem och skrivare är ett ofta förbisett område när det gäller informationssäkerhet.

Sharp definierar utskriftssäkerhet som säkerhet relaterad till utskrifter och filer genererade av multifunktionssystem eller skrivare. Den här kategorin omfattar alla utskrivna dokument och digitala kopior av data som överförs från en dator till en skrivare (inklusive utskrifter via dedikerade skrivarservrar), scanning (inklusive scanning till mapp, scanning till e-post, scanning till molntjänster, scanning till hårddisk) och faxning.

Huvudpunkterna i detta faktablad är:

- **Bakgrund**
  Beskriver varför utskriftshantering är ett ofta förbisett område när det gäller informationssäkerhet. Här belyses också de potentiella risker som varje IT-administratör måste vara medveten om, bland annat:

  - Det växande antalet organisationer som konsoliderar sina multifunktionssystems- och skrivarparker
  - Det växande antalet anslutna användare som alla behöver identifieras och hanteras
  - Det växande antalet dokument som skrivs ut och behöver övervakas
  - Bristen på verktyg för att spåra och rapportera alla utskriftsaktiviteter

- **Problem**
  Undersöker utmaningar avseende utskriftshantering som IT-chefer, användare och företagsledningar kan ställas inför. Dessa inkluderar hantering av användarbehörighet för utskrivna dokument, spårning av användaraktivitet, rapporteringsaktivitet, utskrift från mobila enheter, scanning av dokument till flera destinationer och faxning av dokument utanför organisationen.

  Här inkluderas också forskning som visar ämnets komplexitet och problemets omfattning.

- **Lösning**
  Beskrivning av en uppsättning Sharp-produkter (mjukvarulösningar) samt effektiva rutiner som kan bidra till en säker utskriftsmiljö och förhindra obehörig åtkomst till multifunktionssystem och skrivare samt dokument (inklusive digitala kopior av utskrifter), kopior, fax, scanningfiler och utskrifter som framställs och lagras.

  Vi undersöker hur Sharp kan lösa problem genom att hjälpa dig att:

  - Välja rätt lösning som passar företagets krav och som hjälper dig att skapa en stark och effektiv policy för säker utskrift. Ett utskriftshanteringssystem kan övervaka behörighet, tillämpa utskriftsregler, begränsa funktionalitet och säkerställa korrekt spårning och rapportering av alla utskrivna dokument.
  - Välja rätt leverantör av lösningar för utskriftshantering och relaterade utskriftsaktiviteter.

- **Slutsats**
  Ger en sammanfattning av ämnet som fokuserar på:

- De huvudsakliga risker som existerar i samband med utskrift
- En sammanfattning av de rekommendationer som baseras på Sharps säkerhetslösningar
- Nästa steg som krävs för att utarbeta en enhetlig policy för säker utskrift, inklusive tillförlitliga verktyg som kan tillämpas inom företagets alla områden.

Bakgrund

När företag listar potentiella hot mot informationssäkerhet tänker de sällan eller aldrig på nätverksbaserade multifunktionssystem och skrivare som ett problem – för att inte nämna utskrivna dokument.

Enligt marknadsundersökningsföretaget Quocirca har 60 % av företagen haft minst en incident till följd av oskyddad utskrift – och detta är ett reellt hot för både små och stora företag[1]. Emellertid är det inte alltid tillräckligt att implementera säkerhetslösningar för att skydda data från tekniskt avancerade inkräktare eller cyberkriminella.

Några av de vanligaste överträdelserna är något så enkelt som att en utskrift plockas upp av fel person. Om känsliga dokument lämnas i multifunktionssystemets eller skrivarens utmatningsfack tillräckligt länge kan vem som helst få tag i dem och använda informationen till sin fördel, vilket kan orsaka allvarliga problem.

56 % av storföretagen ignorerar skrivare i sin säkerhetsstrategi .[2]

Från en potentiell förövares synvinkel är utmatningsfacket det överlägset enklaste målet om de vill komma över konfidentiell information. En ofta underskattad utmaning för IT-administratören är därför att se till att utskrifter inte lämnas i oskyddade multifunktionssystem eller skrivare där de kan hamna i fel händer.

Utmaningarna som varje modern organisation ställs inför när det gäller att säkerställa utskriftssäkerhet blir emellertid större för var dag av flera olika anledningar:

1. **Växande maskinparker**
   Antalet företag som konsoliderar sina multifunktionssystem- och skrivarparker växer, och många företag strävar efter enhetlighet och standardisering. Detta leder till flera olika utmaningar på grund av brist på verktyg för övervakning av multifunktionssystem och skrivare:

   - Funktionalitet
   - Utskrift
   - Säkerhet (som del av nätverket).

2. **Antal nätverksanslutna användare**
   I vissa företag kan antalet anställda vara betydande, med hundratals användare som skriver ut från 10–100 eller fler enheter. Om man till detta adderar det ökande antalet regelverk, såsom den allmänna dataskyddsförordningen, så kan utmaningarna bli verkligt stora när det gäller:

   - Användarautentisering
   - Hantering av användarkonton (inklusive hantering av antalet anslutna användare)
   - Integrering av användare i befintlig kontorsutrustning
   - Begränsade möjligheter för organisationer att hantera personuppgifter i sina system, såsom krav på redigering av personuppgifter i syfte att efterleva den allmänna dataskyddsförordningen.

3. **Antal utskrifter att hantera**
   Det snabbt växande antalet användare och det genomsnittliga antalet utskrivna sidor per användare betyder att ett mycket stort antal utskrivna dokument måste övervakas:

   - Kopior
   - Utskrifter
   - Scanningfiler
   - Fax

- Dokument utskrivna via mobiler och surfplattor (dvs mobil utskrift och användning av egen utrustning)

4. **Brist på övervakningsverktyg**
   Det råder generellt brist på verktyg för spårning och rapportering av all utskrift.

Problem

Utskriftssäkerhet bör betraktas som en av de viktigaste fokuspunkterna i varje modernt företag som använder multifunktionssystem och skrivare.

Rätt verktyg är avgörande

Forskningsanalytiker betonar behovet av effektiva verktyg och åtgärder för hantering av en mängd utskriftsfiler med många skrivare och många användare.

Utskriftsbehörighet

Utmaningen för varje IT-administratör är hanteringen av en mängd konton och användare i företagets nätverk. Antalet användare påverkar självfallet den administrativa arbetsbelastningen. Dessutom blir både användarhantering och alla utskriftsrelaterade aktiviteter såsom kopiering, utskrift, scanning och faxning mer komplicerade. Utmaningen består således av hur utskriftssäkerheten ska hanteras på ett effektivt sätt.

Vissa av de vanligaste teknikerna, såsom PIN-kod, användarnamn/lösenord, kort/bricka eller ID-kort är effektiva sätt att säkra utskriftshanteringen. Dessa metoder kan emellertid vara en veritabel mardröm för IT-administratören om de implementeras och hanteras på ett bristfälligt sätt. Speciellt då många IT-administratörer strävar efter att ansluta enheter till befintliga system, till exempel Microsoft-konton.

Dokumentantal och obevakad utskrift

Det växande antalet utskrifter är en stor utmaning. Detta inkluderar både traditionella pappersdokument som antingen skrivs ut eller kopieras, och filer som överförs till multifunktionssystem och skrivare via företagets nätverk eller överförs via scanning- och faxfunktionerna.

Nya regelverk såsom den allmänna dataskyddsförordningen har dessutom aktualiserat en rad frågor om hur obevakade utskrifter ska skyddas, och hur säkra personuppgifterna i de nämnda kommunikationskanalerna är i realiteten.

Riskinsikt

Om ett effektivt skydd ska kunna införas är det viktigt att fullt ut förstå de risker som är förknippade med olika aktiviteter:

- **Kopiering**
  Kopiering var på 80- och 90-talet det vanligaste sättet att dela dokument, men detta har nu ersatts av utskrift. Trots detta är kopiering ett viktigt område att övervaka via utskriftshanteringssystem, speciellt när det gäller känsliga affärsdokument.

- **Utskrift**
  Utskrift är uppenbart ett mycket vanligt sätt att distribuera affärsdokument idag. Emellertid är utskrift förknippad med många risker när den inte övervakas centralt. Exempel på risker:

  - Oskyddad och oövervakad åtkomst till multifunktionssystem och skrivare och relaterade funktioner och enheter, exempelvis hårddiskar
  - Fri tillgång till utskriven dokumentation, där all kontorspersonal (och möjligtvis även besökare) har tillgång till dokument som lämnas obevakade
  - Ingen möjlighet att spåra och rapportera användaraktiviteter, såsom vilka som har skrivit ut vad under en specificerad tidsperiod.
  - Ingen möjlighet att spåra och förhindra dataintrång, vilket kan leda till betydande straffavgifter till följd av överträdelse av den allmänna dataskyddsförordningen eller andra regelverk
  - Ingen möjlighet att spåra mobila användare eller utskrift från mobila enheter såsom mobiltelefoner och surfplattor.

- **Scanning**
  Scanning kan göra säkerhetsprocessen ännu mer komplicerad, då dokument kan scannas inte bara till nätverksmappar och e-post utan

också till externa, molnbaserade system. Det föreligger risk även för:

- Scanning av affärskritiska dokument till externa destinationer såsom privata e-postadresser istället för företagets e-postdomän
- Scanning till flera mappar istället för till en specificerad personlig företags- eller nätverksmapp, utan att IT-administratören har godkänt dessa destinationer
- Scanning utan indexering, vilket kan orsaka allvarliga problem när man senare vill hitta och spåra scannade dokument och scanningrelaterad aktivitet (scanningfiler och scanningsdestinationer).

- **Faxning**
  I likhet med scanning kan faxning vara en potentiellt svag punkt i företagets strategi för utskriftssäkerhet. Oavsett överföringsmetod – analog faxning eller sändning av fax via e-post – är faxade dokument exponerade för samma risker som scanningfiler.

- **Mobil utskrift – egen utrustning (BYOD)**
  Mobilitet betraktas av många marknadsundersökningsföretag som en av framtidens grundpelare när det gäller utskrift. Integration av mobila utskriftslösningar i en modern organisation medför emellertid utmaningar för företaget, och även hur mobila användare ska spåras och hanteras korrekt. En annan viktig fråga är hur en strategi för mobil utskrift passar in i organisationens övergripande strategi. Olyckligtvis inser många företag inte att personalens rörlighet är en växande trend, och till och med ett reellt krav i affärsvärlden. Behovet av utskriftssäkerhet inom detta område förbises därför ofta.

- **Spårning och rapportering**
  Ett reellt problem för många företag är inte bara hur säkra de egna utskriftsaktiviteterna är, utan också spårningen och rapporteringen av dessa aktiviteter.

  Det är också viktigt att spårningsinformationen är korrekt och säker:

  - Vem har tillgång till den?
  - Är data korrekta?
  - Kan informationen redigeras?
  - Vem hanterar systemet?

Rekommendationer

Det är synnerligen viktigt att förstå att utskriftssäkerhet bara är ett av många säkerhetsområden, vilka i hög grad kan variera från en organisation till en annan.

Vissa företag har inställningen att om säkerhetsåtgärderna för nätverket tas på allvar och noggrant implementeras så är de tillräckliga. I takt med att verksamheten expanderar ökar emellertid även antalet producerade dokument – och därmed sammanhängande säkerhetsrisker.

Ett vidare perspektiv avseende säkerhet krävs, där inte bara nätverket är skyddat utan också alla genererade utdata och dokument som delas utanför organisationen.

Med andra ord så är det högst nödvändigt att skydda både nätverket och all nätverksansluten kringutrustning. Utskriftssäkerhet är ett naturligt steg till ökad nätverkssäkerhet, inte bara i stora organisationer utan även i snabbväxande små och medelstora företag.

Med hjälp av tillämpningar för utskriftshantering, exempelvis en av Sharps lösningar för Optimised Printing eller Optimised Scanning, kan du enkelt skydda alla utdata, integrera dina enheter med befintliga system, till exempel Windows, samt snabbt införa en enhetlig policy för säker utskrift och scanning.

Den viktigaste aspekten av utskriftssäkerhet är övervakning, eftersom allt som kan övervakas kan mätas för att därefter skyddas. Med hjälp av våra system får du fullständig kontroll över alla utskrivna dokument och all annan information: kopior, utskrifter, scanningfiler och fax.

Tack vare den transparenta integrationen med företagets befintliga maskinpark sparar utskriftshanteringssystemet värdefull tid. Exempelvis kan alla användare snabbt och enkelt importeras via LDAP (Lightweight Directory Access Protocol). Alla användare kan på några sekunder läggas till, identifieras och integreras med systemet. Dessutom överförs alla inloggningsuppgifter via TLS (Transport Layer Security) för att undvika avlyssning.

Det verkliga fina med det här utskriftshanteringssystemet är emellertid de avancerade funktioner som gör livet betydligt lättare för både IT-administratören och användaren:

- **Användarautentisering**
  Detta är hörnstenen för åtkomst av utskriftshanteringssystemet. Mjukvaran gör det möjligt att identifiera användarna och tilldela behörigheter för de anslutna enheterna på flera olika sätt. Den snabbaste och vanligaste metoden är kort/bricka eller ID-kort. Dessa innehåller alla personuppgifter, och autentisering görs via en kortläsare installerad i skrivaren. IT-administratören kan också välja mellan flera alternativa autentiseringsmetoder såsom PIN-kod och användarnamn/lösenord.

  Det går också att använda befintliga kort som för närvarande används i företaget för tillträde till byggnader, avdelningar, skyddade rum etc. Det finns flera olika kort- och kortläsarstandarder som använder olika kommunikationsmetoder och frekvenser. Vi rekommenderar att du kontaktar din lokala Sharp återförsäljare om du behöver hjälp med att välja rätt system för ditt företag.

- **Säker kö**
  När ett dokument skickas till skrivaren från datorn på normalt sätt startar kommunikationen mellan datorns drivrutin och utskriftshanteraren. Endast registrerade användare kan skriva ut, och endast med godkända enheter konfigurerade med erforderlig mjukvara. Användaren skickar jobbet till utskriftshanteringsservern, och vid inloggning till multifunktionssystemet eller skrivaren (via kort/bricka, PIN-kod eller användarnamn och lösenord) identifierar systemet användaren som registrerad och med rätt att skriva ut.

- **Säker utskrift**
  En säker kö och placering av jobb i kön på en server ger ytterligare en mycket viktig fördel i form av säker utskrift (Follow Me) via valfri nätverksansluten enhet. Det innebär att användaren kan skriva ut från valfri enhet, som kan vara placerad på en annan avdelning, ett annat våningsplan eller till och med i en annan byggnad (förutsatt att den delar samma nätverk), eller valfri plats med ett installerat utskriftshanteringssystem.

  Tack vare funktionen för säker utskrift reduceras även utskriftsrelaterad stilleståndstid. När någon av skrivarna inte är i drift, till exempel på grund av underhållsarbete, kan användaren helt enkelt gå till närmast tillgängliga skrivare och skriva ut jobbet där.

- **Automatisk jobbradering**
  Ytterligare en utmaning för IT-administratören är det stora antalet sidor som tillfälligt lagras i väntan på utskrift eller indexering. Men inte vid användning av utskriftshanteraren. Tack vare funktionen för automatisk radering kan IT-administratören konfigurera en policy för kvarhållande av dokument. Om ett dokument exempelvis skickas till skrivaren klockan 8 på morgonen och inte skrivs ut inom 24 timmar raderas det automatiskt från serverkön. Funktionen är helt konfigurerbar enligt organisationens behov och krav.

84 % av alla organisationer prioriterar säkerheten högst under åren fram till år 2025, och säkerhetsexpertis kommer att vara det främsta urvalskriteriet för 58 % av organisationerna.[3]

- **Eliminering av duplicerade utskrifter**
  Ytterligare en fördel med en utskriftshanteringslösning är eliminering av duplicerade utskrifter. Efter autentisering och inloggning till den valda skrivaren kan användarna se hela listan med skickade utskriftsjobb. De kan enkelt se om något dokument har skickas flera gånger och välja vilka dokument som ska skrivas ut och vilka som ska tas bort. Dessutom kan användaren välja om jobbet ska tas bort från kön efter utskrift eller behållas i kön.

- **Säker scanning, faxning och kopiering**
  Med utskriftshanteraren kan enhetens alla funktioner övervakas. Kopierings-, scanning- och faxaktiviteter övervakas via samma användarbehörighet för enheten, och alla dessa aktiviteter kan övervakas i enlighet med detta. Dessutom:

  - För säker kommunikation använder Sharps multifunktionssystem och skrivare TLS-protokoll för SMTP- och S/MIME-kryptering för att säkerställa säker e-postkommunikation
  - Multifunktionsstyrenhetens komponent för lokalt nätverk är helt isolerad från faxlinjen. Detta förhindrar potentiella inkräktare från att få tillgång till multifunktionssystemets interna system eller det lokala nätverket.

- **Spårning och rapportering**
  För många organisationer är spårning och rapportering de viktigaste funktionerna. Med ett utskriftshanteringssystem spåras alla aktiviteter. Oavsett om du skriver ut, scannar, kopierar eller faxar registreras alla jobben i systemet. Detaljerade rapporter kan genereras baserat på ditt personliga konto, avdelning eller specifika kunddebiteringsalternativ.

- **Redigering av personuppgifter avseende den allmänna dataskyddsförordningen**
  Artikel 17 i den allmänna dataskyddsförordningen innehåller detaljerade instruktioner för hantering av personuppgifter.

Detta inkluderar "rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter." Med Sharps utskriftshanteringssystem är detta inte något problem. Systemet medger redigering av alla personuppgifter, och efterlever det strikta regelverket. Även när personuppgifter har tagits bort kan IT-administratören fortfarande använda vissa utskriftsdata för att generera användningsstatistik.

- **Mobil utskrift**
  Detta är ett mycket enkelt koncept; användarna kan skriva ut som vanligt via sin egen utrustning såsom mobiltelefon eller surfplatta. IT-administratören kan bestämma vilken tillämpning som är bäst för organisationen. Sharps tillämpning Optimised Mobile är tack vare avancerade konfigureringsmöjligheter spårbar via utskriftshanteraren. Detta betyder att alla mobilutskrivna dokument registreras i systemet och kan användas för statistik och rapporter.

Ännu högre säkerhet

Utskriftssäkerhet spelar en mycket viktig roll när det gäller att definiera, utarbeta och implementera din egen policy för utskriftssäkerhet:

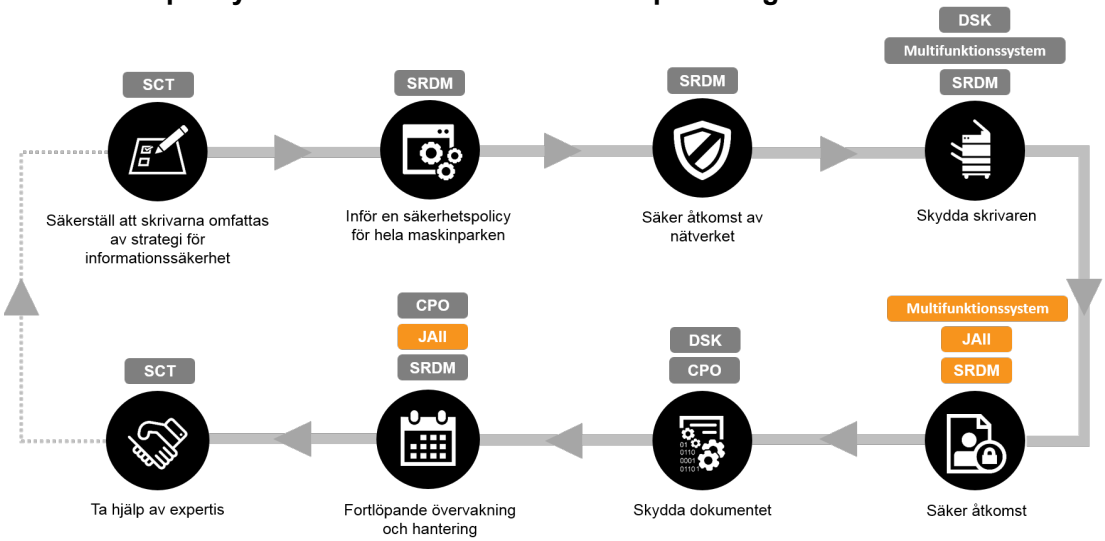
- Utskriftshanterarprodukterna i Sharps Optimised-portfölj är mycket användbara vid tillämpning av en sådan policy, främst på grund av att de utökar funktionaliteten för stegen "säker åtkomst" och "fortlöpande övervakning och hantering".

- Med ytterligare produkter i portföljen, såsom Sharp-multifunktionssystem, datasäkerhetskit (DSK), Sharp Remote Device Manager (SRDM) och Cloud Portal Office (CPO) kan du skapa ett unikt, stabilt och enhetligt säkerhetssystem som är perfekt anpassat till såväl IT-avdelningen som verksamheten.

För högsta möjliga säkerhetsnivå bör företag således samarbeta med leverantörer som inte bara kan leverera påtagliga fördelar när det gäller utskriftshantering; de behöver dessutom vara betrodda och erfarna integratörer.

Sharp har mångårig erfarenhet av att tillverka synnerligen säkra multifunktionssystem och skrivare, utveckla tillämpningar för utskriftshantering och implementera komplexa lösningar. Vi har en mycket stor kunskapsbas att ösa ur, och kan därför råda och vägleda våra kunder avseende alla aspekter av säkerhet, inklusive policy för utskrift och utskriftssäkerhet.

Utarbeta en policy för utskriftssäkerhet och Sharp-lösningar för utskriftssäkerhet



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

Slutsats

De nya skeendena i företagsvärlden innebär att varje gång någon skriver ut, kopierar, scannar eller faxar ett dokument så löper det risk att stjälas eller på annat sätt utsättas för fara.

Företagen måste vara mycket mer medvetna om de risker som uppstår när fysiska dokument eller digitala filer lämnas oskyddade eller obevakade. De viktigaste punkterna är:

- Utskriftssäkerhet är helt avgörande för alla moderna företag oavsett storlek. Det växande antalet dokument som genereras medför betydande utmaningar vid övervakning av IT-miljön. Utmaningarna inkluderar i synnerhet hantering av ett växande antal användare, större filer, mängden information som delas, överbelastning av nätverk och maskinparker.

- Ett utskriftshanteringssystem ger dig maximal konfigureringsflexibilitet. IT-administratören kan inte bara begränsa åtkomst till slutna grupper av användare, utan också spåra all aktivitet på multifunktionssystemet inklusive kopiering, utskrift, scanning och faxning.

- Sharp vet hur viktig säkerheten är för det moderna kontoret och erbjuder en unik, helhetsmässig strategi. Vi behärskar allt från nätverkssäkerhet, som omfattar alla typer av företagsnätverk och ansluten kringutrustning till utskriftssäkerhet som beskrivs i detta faktablad, och dokumentsäkerhet som omfattar alla aspekter av dokumentrelaterad säkerhet.

- Detta grundläggande säkerhetsperspektiv säkerställer att organisationen drar nytta av den högsta nivån av efterlevnad av gällande regelverk såsom den allmänna dataskyddsförordningen (GDPR).

Sharp Security Framework

För att undvika potentiella risker inom andra verksamhetsområden rekommenderar vi att du skaffar dig mer kunskap om ytterligare säkerhetsåtgärder relaterade till:

- Nätverkssäkerhet
- Dokumentsäkerhet
- Efterlevnad av den allmänna dataskyddsförordningen

Se sidan Information Security 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. “Print 2025: Print Security in the IoT Era”, Quocirca, 2018
2. "Annual Global IT Security Benchmark Tracking Study", Ponemon Institute, mars 2015
3. “Print 2025: The future of print in the digital workplace”, Quocirca, 2018

www.sharp.se

SHARP

Be Original.