Sponsrat av: **HP**

Författare:

Angèle Boyd

Keith Kmetz
Matthew Marden

november 2015

Affärsnyttan med skrivarsäkerhet

IDC OPINION

Enligt IDC:s rön uppgav 80 % av de medverkande företagen att IT-säkerheten är viktig för deras affärsprocesser. Men bara 59 % ansåg att skrivarsäkerheten är viktig för deras affärsprocesser. Företagsledningen är nästan 40 % mer involverad i beslutsfattandet kring övergripande IT-säkerhet än kring skrivarsäkerhet. Vi anser att de här rönen tyder på en syn på skrivarsäkerhet som gör företagen sårbara. IDC:s undersökning visar att det finns tungt vägande skäl för företag att titta närmare på skrivarsäkerheten, eftersom det finns stora IT- och verksamhetsmässiga fördelar med en säker utskriftsmiljö, som:

» IDC:s undersökning visar att mer än hälften av de medverkande företagen har upplevt ett IT-säkerhetsintrång som inbegrep skrivarsäkerhet under de senaste tolv månaderna.

» Alla organisationers utskrifts-/dokumentmiljö är sårbar. Sårbarheten kan gälla attacker inifrån eller utanför företaget, eller vårdslös användning av skrivare och utskrivna dokument. Intrången kan till exempel ske via skrivarnas nätverksportar, genom att utskrivna/kopierade/skannade dokument fångas upp från skrivarutrustningens hårddisk och RAM-minne, att obehöriga kommer åt utskrivna dokument i skrivarfacket eller att skyddade dokument (checkar, läkemedelsrecept) används på otillåtna sätt.

» IDC:s djupintervjuer med organisationer som har infört någon form av säkerhet i samband med utskrifter och relaterade dokument visade att företagen som vidtar åtgärder kring utskrifts-/dokumentsäkerhet kan delas in i två grupper:

- Företag med säkerhets- och efterlevnadsproblem som inför en företagstäckande och säker IT-infrastruktur
- Företag som vill uppnå den kostnads- och IT-effektivitet som säkerhetsåtgärderna ger

» IDC:s intervjuer med organisationer som har infört en skrivarsäkerhetslösning visade att de har uppnått de största fördelarna och den största affärsnyttan inom tre områden: förbättrad skrivarsäkerhet, effektivare IT-verksamhet och lägre kostnader. Organisationerna

som intervjuades räknade upp en imponerande lista med förbättringar i sin utskrifts- och säkerhetsmiljö, bland annat:

- I genomsnitt upp till sex gånger färre skrivarrelaterade intrång efter att man införde skrivarsäkerhetslösningar
- I genomsnitt hälften så mycket tid på support för skrivarmiljön efter att man införde skrivarsäkerhetslösningar
- I genomsnitt 15 procent lägre kostnader för papper, toner och bläck

» Sättet på vilket företagen inför skrivarsäkerhetslösningarna avgör inte bara hur effektiva de blir, utan påverkar också medarbetarnas effektivitet. För att lösningarna ska ge största möjliga fördelar finns det avgörande faktorer i fråga om teknik, medarbetare och rutiner som är viktiga att ta hänsyn till.

I detta faktablad

Det här faktabladet baseras på primära och sekundära undersökningar utförda av IDC inom IT-säkerhet och utskriftsrelaterad säkerhet. Djupintervjuerna genomfördes mellan juli och september 2015 med personer som ansvarade för införande och hantering av skrivarsäkerhetslösningar på 16 företag. Intervjuerna utformades för att visa den kvantitativa och kvalitativa effekten av företagens användning av företagstäckande skrivarsäkerhetslösningar. Intervjuerna speglade erfarenheterna från skilda typer av

TABELL 1

Fakta om medverkande företag – djupintervjuer

	Genomsnitt	Median	Intervall
Antal anställda	60 300	20 500	200 till 290 000
Antal IT-ansvariga	4 500	610	40 till 25 000
Antal IT-användare	57 200	19 500	180 till 290 000
Totalt antal skrivare	8 800	1 200	4 till 100 000
Antal användare med utskriftsbehov	50 800	9 000	200 till 280 000
Antal utskrivna sidor per år	51 miljoner	10 miljoner	10 000 till 300 miljoner
Branscher	Telekom, tillverkning, finanstjänster, förlagsverksamhet, luftfartsindustri, bioteknik, utbildning, hälso- och sjukvård		

n = 16 organisationer

Källa: IDC:s Printer Security Interviews, 2015

IDC Analyze the Future

organisationer. Tabell 1 visar en översikt över skrivarmiljön hos de 16 företag som deltog i intervjuerna.

IDC kompletterade djupintervjuerna med analyser från tidigare undersökningar. Respondenterna kom från fler än 440 organisationer av alla storlekar och var heltidsanställda De var insatta i vilken skrivarutrustning som användes i företaget och företagets policyer kring IT-säkerhet.

Översikt

Varför företag ska bry sig om utskrifts-/dokumentsäkerhet

De flesta organisationer lägger stor vikt vid IT-säkerhet … av goda skäl. Mångfalden av dator-, mobil- och molntekniker och andra tekniker underlättar en IT-miljö där kunskapsarbetare behöver och kräver åtkomst till företagsinformationen när som helst och var som helst. Men IDC såg att skrivarresurser och utskriftsrelaterade tekniker ofta förbises i organisationernas strategi kring IT-säkerhet.

Varför bör företagen ändra sin befintliga syn på skrivarsäkerhet och skydda skrivarutrustningen på samma sätt som de skyddar andra tekniker (som datorer, servrar och mobila enheter)? Därför att en oskyddad utskriftsinfrastruktur är lika med en oskyddad IT-miljö. Risken för skrivarrelaterade säkerhetsintrång är högre än man kan tro, och följderna är kostsamma.

IDC:s undersökning visade att fler än hälften av företagen har upplevt IT-intrång som inbegrep skrivarsäkerhet under de senaste tolv månaderna.

IDC:s undersökning visar att fler än hälften av företagen har upplevt IT-intrång som inbegrep skrivarsäkerhet under de senaste tolv månaderna. Sårbarheten kan gälla attacker inifrån eller utanför företaget, eller vårdslös användning av skrivare och utskrivna dokument. Intrången kan till exempel ske via nätverksportar, genom att utskrivna/kopierade/skannade dokument fångas upp från skrivarutrustningens hårddisk och RAM-minne, att obehöriga kommer åt utskrivna dokument i skrivarfacket eller att skyddade dokument (checkar, läkemedelsrecept) används på otillåtna sätt. I detalj:

- Oskyddade nätverksportar är en ingång till företagets nätverk och information.
- Utskrifter av dokument (till exempel patientinformation eller kunders ekonomiska transaktioner) på delade skrivare där dokumenten ligger kvar i utmatningsfacket en längre tid utgör en risk för stöld av konfidentiell information och överträdelse av lagar och regler.

» Sändning av okrypterade utskrifts-/skanningsdata är i princip en inbjudan till hackning.

Säkerhetsintrång är kostsamma. Det finns tre typer av potentiella ekonomiska konsekvenser:

» **Företagets resurser spenderas på att åtgärda intrånget.** Företag som drabbas av säkerhetsintrång lägger betydande arbetstid och summor på att "städa upp" efter incidenten. Potentiella möjligheter till intäkter fördröjs eller avbryts när resurserna går till att åtgärda incidenten.

» **Böter/straffavgifter.** Företag kan åläggas straffavgifter för att de inte följer lagar och regler (till exempel HIPAA) eller kan bli stämda av kunden för brott mot tystnadsplikten.

» **Företagets rykte.** Företaget kan drabbas ekonomiskt också efter incidenten i form av ett skadat rykte.

Utlösande faktorer för att införa skydd av utskriftsinfrastukturen

Baserat på djupintervjuer med företag som har infört olika nivåer av skrivarsäkerhet, hittade vi följande faktorer som låg till grund för åtgärderna:

» Problem med säkerhet och efterlevnad (bland annat till följd av intrång)

» Proaktiv standardisering av säkerheten i hela IT-infrastrukturen

» Kostnadsbesparingar och IT-effektivitet

Säkerhetsfrågor i samband med immateriell egendom, konfidentiell eller klassificerad information, efterlevnad av lagar och regler samt behovet av en företagstäckande, enhetlig och säker IT-infrastruktur är de primära faktorerna bakom strategier för skrivarsäkerhet. Kostnadsbesparingarna är en sekundär. men viktig, fördel med att införa en plan för utskrifts- och dokumentsäkerhet.

Problem med säkerhet och efterlevnad

Säkerhetsfrågor i samband med immateriell egendom, konfidentiell eller klassificerad information, efterlevnad av lagar och regler samt behovet av en företagstäckande, enhetlig och säker IT-infrastruktur är de primära faktorerna bakom strategier för skrivarsäkerhet. Vissa organisationer genomför mer omfattande säkerhetslösningar efter tidigare incidenter eller intrång.

En systemchef på ett företag i finansbranschen uttryckte det så här: "Säkerhetsrisker finns överallt, och skrivarna är tillgängliga för alla och används för både konfidentiella,

IDC Analyze the Future

klassificerade och allmänna ändamål. Alla nätverksenheter som kommer i kontakt med konfidentiella/klassificerade data omfattas av krav på säkerhet, efterlevnad och möjlighet till granskning. Vi var helt enkelt tvungna att vidta åtgärder."

Standardisering av hela IT-infrastrukturen

Standardisering av säkerheten i företagets allmänna IT-infrastruktur är en annan faktor som bidrar till att man inför utskrifts-/dokumentsäkerhet samt en heltäckande policy för att lösa problem med anknytning till sådan utrustning. En IT-chef i förlagsbranschen förklarade: "Vi ville få policybaserade säkerhetsmekanismer, automatiserad lösning av supportfrågor och grundläggande säkerhet för identitetscertifikat [för skrivare] som ligger i linje med våra övriga infrastrukturtjänster."

Kostnadsbesparingar och IT-effektivitet

Alla IT-initiativ som bidrar till att sänka företagets operativa kostnader välkomnas av ledningen. Kostnadsbesparingarna är en sekundär. men viktig, fördel med att införa en plan för utskrifts- och dokumentsäkerhet. Det kanske inte är den främsta anledningen till att man vidtar säkerhetsåtgärder, men en tredjedel av undersökningsdeltagarna menade att det var den viktigaste fördelen.

En IT-chef på ett företag i finansbranschen förklarade: "Behovet av att skydda immateriell egendom plus de eventuella ekonomiska följderna av intrång i datasäkerheten var de främsta anledningarna till att vi införde lösningarna … Vi är övertygade om att de kontroller som begränsar ogenomtänkta och onödiga utskrifter har lett till besparingar både vad gäller pappersförbrukning och materialkostnader."

Skrivarsäkerhetslösningen medför givetvis också mindre direkta kostnadsbesparingar. Flera företag påpekade att centraliseringen och standardiseringen av utskrifts- och säkerhetshanteringen ledde till en effektivisering av IT-verksamheten, vilket i sin tur ger lägre kostnader. Genom att hantera och skydda utskriftsmiljön mer aktivt, frigör man IT-resurser till andra viktiga behov i verksamheten. En IT-chef på ett universitet sa så här: "Vi ville få kontroll över kostnaderna och centralisera hanteringen av utskriftsmiljön genom en samlad lösning."

Affärsnyttan med skrivarsäkerhet

IDC:s djupintervjuer med 16 organisationer som har infört företagstäckande skrivarsäkerhetslösningar visade att det finns stor affärsnytta att vinna med att införa lösningarna. I intervjuerna bad IDC företagen beskriva sin skrivarmiljö före och efter att man införde säkerhetslösningar. Det framkom att organisationerna har lyckats med föresatsen att skapa säkrare utskriftsmiljöer, samtidigt som de sänker de utskriftsrelaterade kostnaderna och minskar personalens arbetsbörda.

Organisationerna rapporterade att antalet skrivarrelaterade säkerhetsintrång hade minskat i genomsnitt upp till sex gånger efter att man infört företagstäckande skrivarsäkerhetslösningar.

- **Säkerhet.** Skrivarmiljön har blivit allt säkrare och kostnaderna för att åtgärda dataintrång och säkerställa efterlevnad och redovisning har sänkts.
- **Effektivare IT-verksamhet.** Mängden arbetstid som krävs för att hantera och underhålla skrivarmiljöer samt skapa, ändra och införa skrivarrelaterade policyer har minskat, vilket ger personalen tid att arbeta med andra uppgifter.
- **Kostnadsbesparingar.** Utskriftskostnaderna, bland annat kostnaderna för skrivare och skrivartillbehör, har sänkts som ett resultat av ökad insyn och ett förändrat utskriftsbeteende.

Riskbegränsning: Bättre skrivarsäkerhet och efterlevnad

Företagen som intervjuades rapporterade att de har tagit hjälp av företagstäckande skrivarsäkerhetslösningar för att begränsa konsekvenserna av skrivarrelaterade säkerhetsintrång och göra insatserna för att efterleva lagar och regler mer effektivt och kostnadseffektivt.

IDC bad deltagarna uppge hur ofta företagen utsattes för skrivarrelaterade säkerhets- och dataintrång och om de hade drabbats av vad de själva skulle karakterisera som avsevärda skrivarrelaterade säkerhetsintrång. Organisationerna rapporterade att antalet skrivarrelaterade säkerhetsintrång hade minskat i genomsnitt upp till sex gånger efter att man infört företagstäckande skrivarsäkerhetslösningar. Kryptering av utskrifter, användarautentisering och pull printing har bidragit till större spårbarhet och ansvarighet och till att förhindra nya intrång. I vissa av organisationerna var säkerhetslösningarna den sista pusselbiten när det gällde att täppa igen luckorna i IT-infrastrukturen. De tillfrågade företagen gav exempel på skrivarrelaterade säkerhetsintrång som de hade upplevt:

- **Utskrift av konfidentiell information med bedräglig avsikt.** En IT-chef på ett tillverkningsföretag förklarade att hans organisation hade förlorat immateriell

IDC Analyze the Future

egendom, bland annat till följd av att anställda skrev ut hemligstämplad och konfidentiell information som sedan överlämnades till konkurrenterna.

» **Utskrift och felaktig hantering av skyddade data.** En IT-chef i finansbranschen uppgav att personal på hans företag äventyrade ritningar och annan immateriell egendom genom att skriva ut dokument och lämna kvar utskrifterna vid skrivaren.

Organisationerna gav flera exempel på hur användningen av företagstäckande skrivarsäkerhetslösningar har hjälpt dem att begränsa effekten av skrivarrelaterade säkerhetsintrång:

» **Skydda data under hela utskriftsprocessen.** En IT-chef i förlagsbranschen sa: ”Lösningen är ett nödvändigt verktyg för att skydda flödet av innehåll och data till och

TABELL 2

Effekt av företagstäckande skrivarsäkerhetslösningar på antalet säkerhetsintrång – djupintervjuer

Totala säkerhetsintrång	
Genomsnittligt antal intrång per år – före införandet av skrivarsäkerhet	9,9
Genomsnittligt antal intrång per år – med skrivarsäkerhet	1,5
Förändring av antalet säkerhetsintrång	Upp till sex gånger färre
Avsevärda säkerhetsintrång	
Antal berörda företag	5
Genomsnittligt antal anställda som påverkades	54
Genomsnittlig tid för åtgärd (timmar)	277
Total genomsnittlig kostnad för åtgärd per intrång (inklusive straffavgifter)	521 400 USD

n = 16 organisationer

Källa: IDC:s Printer Security Interviews, 2015

från skrivarna i nätverket. Det skapar tillit och hjälper oss att minska risken för intrång."

» **Förhindra onödiga och felaktiga utskrifter.** En IT-chef på ett företag i finansbranschen sa: "I många fall borde känsliga dokument som distribueras internt aldrig skrivas ut över huvud taget. Säkerhetslösningarna hjälper oss att minimera intrång som i allt högre grad sker internt, antingen med uppsåt eller genom att man skriver ut dokument utan tanke på följderna."

Som tabell 2 visar är varje skrivarrelaterat säkerhetsintrång visserligen förknippat med kostnader, men det är särskilt viktigt att företagen undviker allvarliga intrång eftersom de är mycket kostsamma att åtgärda. Enligt de fem tillfrågade organisationer som hade drabbats av vad de själva karakteriserade som ett avsevärt skrivarrelaterat säkerhetsintrång under det senaste året, uppgick kostnaderna till i genomsnitt mer än 500 000 USD per intrång, inklusive straffavgifter, plus förlorad produktivitet för 54 anställda och 277 arbetstimmar för åtgärder.

Utöver att skrivarsäkerhetslösningarna har resulterat i färre skrivarrelaterade säkerhetsintrång, ansåg tio av de 16 tillfrågade organisationerna att de dessutom gjorde arbetet med regelefterlevnad och redovisning mer fokuserat och tidsbesparande. Förbättrad säkerhet och spårbarhet ger följande fördelar:

» **Förbättrad säkerhet:** En systemchef på ett företag i finansbranschen påpekade: "Den stora fördelen med vår säkerhetsmodell är att vi har fått en mycket stabil och säker miljö som skyddar data och dokument, stärker skyddet av design och arkitektur och skyddar skrivarna, vilket har hjälpt oss att följa våra säkerhetsregler."

Företagen uppgav för IDC att de anställda i genomsnitt har halverat tiden för att ge support till skrivarmiljön efter att man införde skrivarsäkerhetslösningarna.

» **Spårbarhet och insyn:** En IT-chef på ett företag inom livsvetenskap förklarade: "Vi har kunnat skapa en spårbarhetskedja, förhindra att data kommer i orätta händer och visa att vi ger begränsad användaråtkomst till konfidentiell information. Och våra verifierings- och granskningsfunktioner inbegriper riskidentifiering och hotanalys samt rekommenderade åtgärder vid problem. Vi får en detaljerad överblick över systemets status och kan övervaka det i realtid, vilket är två av kraven som ställs för efterlevnad."

Förbättringarna har dessutom gett organisationerna både tids- och kostnadsbesparingar i samband med efterlevnads- och granskningsarbetet. Företagen rapporterade att skrivarsäkerhetslösningarna har gett besparingar på i genomsnitt 200 arbetstimmar per år och närmare 250 000 USD per år i kringkostnader, inräknat kostnader för extern support vid granskning och efterlevnad.

IDC Analyze the Future

Effektivare IT-verksamhet

Organisationerna i IDC:s undersökning uppgav att de har minskat arbetsbördan vid hantering och support av skrivarmiljön sedan de införde skrivarsäkerhetslösningar. Effektivitetsvinsterna är bland annat ett resultat av nya eller utökade centraliserade hanteringsfunktioner och automatisering, samt möjligheten att lösa skrivarrelaterade problem snabbare. En IT-chef i finansbranschen förklarade: "Användningen [av skrivarsäkerhetslösningar] har inneburit stora förbättringar för medarbetarna, både vad gäller antalet timmar som läggs på tidskrävande uppgifter och när det gäller att frigöra resurser för mer strategiskt viktigt arbete." Åtgärderna vid skrivarrelaterade problem är inte längre splittrade, utan är upprepningsbara och sker i ett helhetsperspektiv." Företagen berättade för IDC att de anställda i genomsnitt har halverat tiden för att ge support till skrivarmiljön efter att man införde skrivarsäkerhetslösningarna.

Organisationerna rapporterade att lösningarna har lett till effektivitetsvinster för de medarbetare som ansvarar för skrivarmiljön. Besparingarna i arbetstid är ett resultat av automatiseringen av support och underhåll genom bland annat automatisk certifikathantering och andra löpande rutiner. En vice vd på ett företag i finansbranschen som har infört policyer för unika certifikat och användarautentisering, förklarade att hans organisation har lyckats sänka tiden som personalen lägger på att övervaka skrivarna med 60 procent: "Vi sparar arbetstid för IT-avdelningen eftersom det är enkelt att skapa profiler och skicka ut dem till flera skrivare samtidigt, och eftersom vi kan automatisera certifikathanteringen."

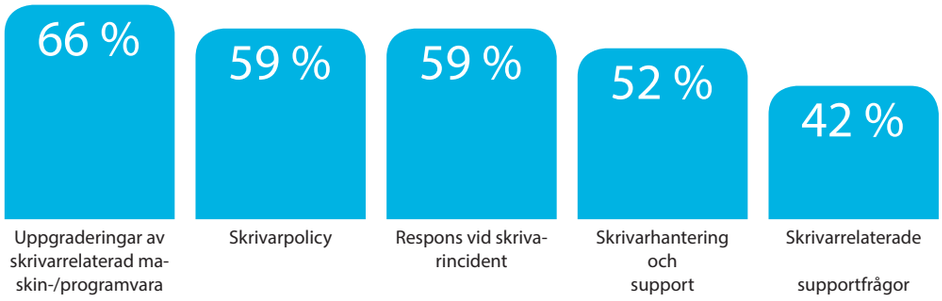
Organisationerna i undersökningen meddelade också att skrivarsäkerhetslösningarna hjälper dem att spara tid i samband med att skapa, införa och ändra skrivarrelaterade policyer. Personalen lägger i genomsnitt 59 procent mindre tid på skrivarrelaterade policyer. Det effektivare införandet av skrivarrelaterade policyer medför också att man minskar risken för intrång och skapar mer effektiva riktlinjer för skrivaranvändningen.

De tillfrågade företagen angav att när det inträffar skrivarrelaterade problem, kan medarbetarna dra fördel av egenskaper hos lösningarna, som att man får (eller bättre kan utnyttja) centrala konsoler och fjärråtkomst till skrivare. Dessa faktorer i kombination med förbättrade policyer kring skrivarhanteringen har hjälpt företagen att minska tiden som krävs för att vidta åtgärder vid skrivarrelaterade incidenter med 59 procent respektive med 42 procent vid skrivarrelaterade supportsamtal från användarna (se bild 1). En IT-chef på ett företag i förlagsbranschen som använde säkerhetslösningar med bland annat automatisk lösning av supportproblem och hantering av unika certifikat, beskrev effekten på gruppens förmåga att erbjuda skrivarsupport: "Nu inträffar färre problem, och de problem som uppstår går snabbare att åtgärda. Den positiva effekten är att vi får tid till annat support- och planeringsarbete." En IT-chef på ett företag i finansbranschen som använde en

skrivarsäkerhetslösning påpekade: ”Vår supportavdelning har fått en tydlig överblick över skrivarinställningar, behörigheter och problem och kan vidta åtgärder självständigt eller skicka vidare ärendet till en skrivarsupportgrupp för nivå 2-support.”

BILD 1

Genomsnittlig besparing i arbetstid för skrivarrelaterade uppgifter – djupintervjuer



n = 16 organisationer

Källa: IDC:s Printer Security Interviews, 2015

Minskade utskriftskostnader

Alla omfattande IT-initiativ som dessutom leder till sänkta kostnader är mer attraktiva. Därför var det en viktig bonus för företagen i undersökningen att man kunde uppnå kostnadsbesparingar med sina skrivarsäkerhetslösningar. Användarautentisering och pull printing var två av de vanligaste funktionerna bland de intervjuade organisationerna och användes av mer än två tredjedelar av företagen. Lösningarna upprätthåller dokumentskyddet och ger lägre kostnader, eftersom skrivaranvändarna måste identifiera sig för att skriva ut och eftersom färre utskrifter skickas till fel skrivare eller aldrig hämtas från skrivaren. Kostnadsbesparingarna med skrivarsäkerhetslösningarna är så stora att flera av de intervjuade företagen noterade detta som den främsta anledningen till att de använder säkerhetslösningar.

Organisationerna uppgav att lösningarna har hjälpt dem att sänka sina kostnader genom att:

» **Minska antalet utskrifter till följd av ett förändrat utskriftsbeteende:** En finanschef på ett företag i livsmedelsbranschen sa: ”Med pull printing kan man skicka dokument

till skrivaren för utskrift, men för att faktiskt skriva ut dem måste man gå fram till skrivaren och sätta i sitt kort. Enligt den senaste uppgiften jag har sett, har det minskat antalet utskrifter med 21–24 procent jämfört med tidigare."

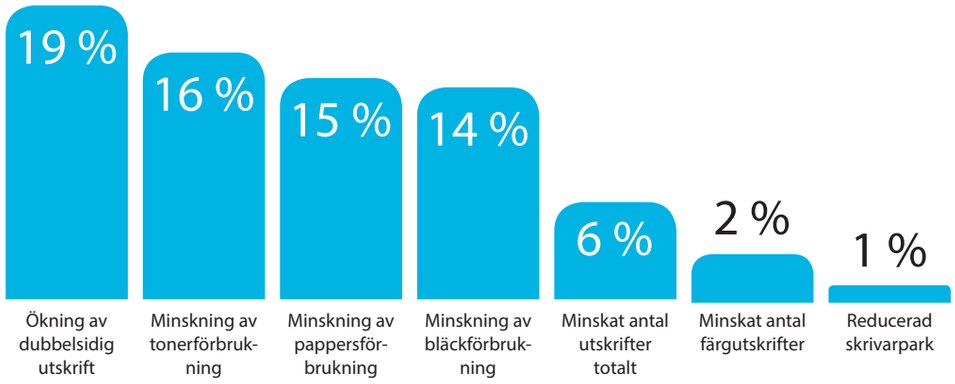
- **Få insyn i skrivaranvändningen:** En IT-chef på ett universitet rapporterade: "Nu kan vi spåra kostnaderna för utskrift och debitera enskilda institutioner." Eftersom utskriftskostnaderna kan kopplas direkt till institutionerna, kan universitetet ge institutionerna i uppdrag att effektivisera skrivaranvändningen.
- **Fasa ut överflödiga eller föråldrade skrivare:** En vice vd på ett företag i finansbranschen påpekade: "Vi har minskat antalet onödiga utskrifter eftersom medarbetarna vet att utskriftsaktiviteten är övervakad. Dessutom drar vi tillbaka eller byter ut äldre skrivare som inte har de funktioner som krävs för att följa våra policyer kring skrivarsäkerhet."

Skrivarsäkerhetsinitiativen har gjort medarbetarna mer medvetna om hur de använder skrivarna och har bidragit till minskade skrivarrelaterade kostnader. Intervjudeltagarna uppgav att deras anställda skickar i genomsnitt 43 procent färre utskriftsjobb till fel skrivare. Det resulterar i att färre utskrifter aldrig hämtas upp eller att de skickas på nytt. Som framgår av bild 2 har den här typen av förbättringar bidragit till en effektivare skrivaranvändning över lag, bland annat färre utskrifter totalt (i genomsnitt sex procents minskning), fler dubbelsidiga utskrifter (19 procents ökning) samt en viss minskning av antalet färgutskrifter (två procents minskning). Dessa faktorer i kombination med ökad insyn i skrivarmiljön har medfört stora kostnadsbesparingar i utskriftsmiljön på företagen, bland annat när det gäller antalet skrivare som används och underhålls (en procents minskning eller i genomsnitt 115 skrivare per organisation) samt kostnaderna för papper, bläck och toner (15, 14 respektive 16 procents minskning).

BILD 2

Genomsnittliga kostnadsbesparingar i skrivarmiljö och skrivareffektivitet – djupintervjuer

(% effektivitetsvinst eller förbättring)



n = 16 organisationer

Källa: IDC:s Printer Security Interviews, 2015

IDC rekommenderar att företagen felsäkrar sin utskrifts-/ dokumentsäkerhetsteknik.

Utmaningar

I det stora flertalet av alla organisatoriska förändringar på företagen är det möjligt att undvika vissa svårigheter genom att man planerar i förväg. Utmaningarna för de intervjuade företagen fanns inom alla de tre faserna i införandet av en skrivarsäkerhetslösning: planering, implementering och efterföljande arbete.

Företagen rapporterade att de kände tidspress när det gällde att ta fram en strategi och en plan för säkerheten. I det första skedet är det viktigt att avsätta tillräckligt med tid på att minska IT-avdelningens arbetsbörda efter införandet av säkerhetslösningen. Efterlevnaden av lagar och regler bör dessutom säkerställas automatiskt genom övervakningsverktyg, eskaleringsrutiner och problemlösning som minskar antalet utskriftsrelaterade supportsamtal.

När det gäller skrivaranvändarna, noterar vi två områden som är viktiga att ta hänsyn till:

» **Balansera hög skrivarsäkerhet med personalens produktivitetstopp:** Företagets säkerhetsbehov måste ha högsta prioritet, men man bör också införa ett system

som ger minsta möjliga negativa inverkan på produktiviteten. Till exempel kanske vissa organisationer som använder pull printing som skrivarsäkerhetslösning möter motstånd från användarna, eftersom funktionen kräver att man autentiserar sig (till exempel skriver ett lösenord) och sedan väntar på att dokumentet ska skrivas ut. Här är det frågan om en avvägning mellan å ena sidan skyddet av informationen i dokumentet (ingen kan läsa utskrivna dokument som ligger obevakade i skrivarfacket), och å andra sidan att man är tvungen att vänta på att dokumentet ska skrivas ut (utskriften startar först efter att användaren har autentiserat sig på enheten).

- **Utbildning av medarbetarna:** När det gäller de anställdas produktivitet, måste skrivarsäkerhetsplanen ta hänsyn till de insatser och den tid som krävs för att utbilda personalen i alla nya regler och rutiner. Företagen måste vara beredda att erbjuda återkommande utbildningstillfällen och använda olika utbildningsformat som passar personalens olika ålder och utbildning.

Rekommendationer

IDC har identifierat flera tungt vägande anledningar att inkludera utskrifts-/dokumentrelaterade arbetsflöden i företagets IT-säkerhetsstrategi. En av de uppenbara fördelarna är tillgången till ett heltäckande IT-säkerhetsprogram som inbegriper utskriftshantering. En sådan strategi har flera andra viktiga fördelar utöver säkerhet. Två stora fördelar är avsevärda kostnadsbesparingar och effektivare IT-verksamhet.

IDC rekommenderar att företagen felsäkrar sin utskrifts-/dokumentsäkerhetsteknik. För att åstadkomma detta krävs det att personalen är involverad och att processerna ligger i linje med säkerhetsplanen.

Teknik

När det gäller säkerhet, är införandet av tekniska lösningar en fråga om "antingen eller": Företaget är antingen skyddat eller inte.

IDC rekommenderar att organisationerna inför följande funktioner så snart som möjligt. Ansvariga för IT och utskriftsinfrastruktur ska säkerställa att följande funktioner och egenskaper konfigureras och aktiveras för alla skrivare i hela företaget:

- Kontrollera att alla nätverksanslutna skrivare har följande funktioner eller åtminstone har uppgraderad fast programvara med dessa funktioner.

- Se till att skrivarna endast använder krypterade kommunikationsprotokoll och inaktivera övriga protokoll.
- Inför ett system som raderar eller förstör data på skrivarnas hårddisk när skrivarna tas ur bruk.
- Ge stöd för minst en metod för användarautentisering (helst två eller tre) och överväg att införa pull printing i utskriftsmiljöer med hög andel konfidentiell information eller stränga regelmässiga krav.
- Kontrollera att fast programvara är uppdaterad och att endast tillåten fast programvara installeras.
- Säkerställ att alla skrivarhårddiskar är säkra (kryptera och radera data regelbundet).
- Inför funktioner som visar om dokumenten har manipulerats, eller använd skrivare med låsbara lådor för specialmaterial om utskriftsbehoven kräver det. Detta skyddar utskrifter som riskerar att utsättas för bedrägeri, som checkar, läkemedelsrecept och liknande.
- Använd ett hanteringsverktyg för central hantering, övervakning och åtgärd av skrivarutrustningen för att säkerställa efterlevnad av företaget säkerhetsregler. På så sätt behöver varje enskild skrivare inte konfigureras och underhållas manuellt. Verktyget ska innehålla funktioner för att enkelt skapa och administrera säkerhetsregler, identifiera enheter som läggs till i nätverket, hantera unika skrivarcertifikat, logga incidenter och åtgärda dessa genom eskalering och lösning. Verktyget ska fungera tillsammans med företagstäckande verktyg för IT-säkerhetshantering som övervakar incidenter och onormala händelser på varje enskild

Om IDC

International Data Corporation (IDC) är den främsta globala leverantören av marknadsinformation, rådgivning och evenemang inom IT, telekom och konsumentteknik. IDC hjälper IT-ansvariga, företagschefer och investerare att fatta faktabaserade beslut om teknikköp och affärsstrategi. Fler än 1 100 IDC-analytiker tillhandahåller global, regional och lokal expertis om teknik- och branschmöjligheter och trender i fler än 110 länder i hela världen. I 50 år har IDC levererat strategiska insikter för att hjälpa våra kunder att nå sina affärsmål. IDC är ett dotterbolag till IDG, världens ledande företag inom teknikmedia, research och evenemang.

Internationellt huvudkontor

5 Speen Street

Framingham, MA 01701

USA

508.872.8200

Twitter: @IDC

idc-insights-community.com

www.idc.com

IDC Analyze the Future

skrivare så att eventuella säkerhetsintrång snabbt kan identifieras.

» Se till att utskrifter och skanningar från både stationära och mobila enheter (i rörelse eller vila) är krypterade så att utskriftsrelaterade data är fullständigt skyddade. Detta betyder att också bilagor som ska skrivas ut ska öppnas och skannas som extra skydd. Ett verktyg som övervakar utskrifts- och skanningsinnehåll är en nödvändighet för att säkerställa största möjliga skydd och följa branschstandarder och företagsinterna policyer.

Personal

Organisationer som tar IT-säkerheten på allvar måste se till att säkerhetsteamet inbegriper personer som har kunskap om hur man skyddar skrivarutrustningen och relaterade dokumentarbetsflöden. Teamet kan bestå av företagets egna medarbetare och/eller externa säkerhetsansvariga med nödvändig kompetens. Gruppens uppgift ska vara att bistå vid eventuella säkerhetsproblem i samband med utskriftshantering och arbetsflöden samt att underlätta införandet av en företagstäckande IT-säkerhetsplan.

För att säkerställa att skyddandet av skrivare och relaterade dokumentarbetsflöden inte får negativa konsekvenser för personalens produktivitet, ska företaget inhämta synpunkter från utvalda medarbetare i olika delar av organisationen under planeringsfasen. Vi rekommenderar också att man anlitar en expert inom förändringshantering, i synnerhet om förändringarna i verksamheten är omfattande eller komplicerade. Experten kan även ge råd om hur införandet och utbildningen ska läggas upp.

De flesta organisationer har inte de kunskaper och den kompetens som krävs för att skydda sin utskrifts- och dokumentinfrastruktur på egen hand. Företagen bör därför höra med skrivarleverantören vilka resurser de kan ställa i förfogande till IT-avdelningen. Resurserna kan omfatta alla säkerhetsfunktioner som ingår i företagets skrivarutrustning, säkerhetsprogramvara och säkerhetstjänster (som professionella säkerhetstjänster, säkerhetsbedömningar, förändringshantering och expertkunskaper i regelefterlevnad i särskilda branscher).

Förfarande

Det är viktigt att företaget inleder sitt säkerhetsarbete med att utvärdera den befintliga utskriftsmiljön och ta fram en plan för hur man ska uppnå samma nivå av säkerhet som i den övriga IT-miljön. Man bör bilda sig en uppfattning om de grundläggande säkerhetskraven i den aktuella branschen och formulera en plan för hur man löpande ska övervaka, eskalera, åtgärda och genomdriva dessa säkerhetsregler.

Planen ska utvärderas regelbundet utifrån data från föregående period så att man kan fastställa om det finns behov av justeringar och dra lärdom av utskrifts-/dokumentintrång utanför företaget. Eventuella justeringar ska baseras på den insamlade informationen samt på företagets acceptabla risknivå och säkerhetskostnader.