Forretningsverdien av skriversikkerhet

Sponset av: **HP**

Forfattere:
Angèle Boyd
Keith Kmetz
Matthew Marden

November 2015

IDC-OPINION

Ifølge IDC-undersøkelser har 80 % av de spurte selskapene angitt at IT-sikkerhet er viktig for forretningsprosessene, mens bare 59 % av disse selskapene uttalte at skriversikkerhet er viktig for forretningsprosessene. Det er dessuten nesten 40 % mer sannsynlig at seniorledelsen er involvert i beslutningsprosessen for generell IT enn for skriversikkerhet. Vi mener at disse funnene viser en mangel på bevissthet rundt skriversikkerhet som kan gjøre virksomhetene sårbare. IDC-forskning har avslørt at det er tre tvingende årsaker til at bedrifter bør være oppmerksomme på skriversikkerhet, for et sikkert utskriftsmiljø gir betydelige IT- og forretningsfordeler. Eksempel:

- IDC-undersøkelser viste at over halvparten av selskapene i undersøkelsen hadde opplevd et IT-sikkerhetsbrudd som omfattet utskriftssikkerhet i løpet av de siste tolv månedene.
- En organisasjons utskrifts-/dokumentmiljø er fullt av sårbarheter. Disse sårbarhetene kan komme fra skadelige angrep i eller utenfor organisasjonen, samt uforsiktig bruk av utskriftsenheter og utskrifter. Potensielle utskriftsrelaterte brudd kan skje gjennom enhetens nettverksporter, oppfanging av utskrifts-/kopierings-/skannejobber, skriver/MFP-harddisker og minne (RAM), utskrevne eller kopierte dokumenter som blir liggende i utskuffer, eller ulovlig bruk av sikre medier (sjekker, resepter) og så videre.
- Dybdeintervjuer på virksomhetsnivå som IDC gjennomførte i organisasjoner med samme nivå av sikkerhet for utskrifts- og relatert dokumentarbeidsflyt, avdekket to typer virksomheter som håndhever utskrifts-/dokumentsikkerhet:
  - selskaper med sikkerhets- og samsvarsproblemer som har en virksomhetsomfattende sikker IT-infrastruktur
  - selskaper motivert av kostnads- og IT-effektivitet som oppnås gjennom sikkerhetstiltak
- Intervjuer gjennomført av IDC med organisasjoner som har igangsatt et utskriftssikkerhetsprogram, avdekket at de har oppnådd de mest betydelige fordelene samt forretningsverdi på tre områder: forbedret skriversikkerhet, mer effektivt IT-personell og

kostnadsreduksjoner. Organisasjoner som ble intervjuet, rapporterte en imponerende samling av resultater i utskrifts- og sikkerhetsmiljøene, bl.a.:

- gjennomsnittlig opptil seks ganger færre skriverrelaterte sikkerhetsbrudd etter distribusjon av skriversikkerhetsløsninger
- gjennomsnittlig halvering av arbeidstid som er nødvendig for å støtte skrivermiljøene, etter distribusjon av skriversikkerhetsløsninger
- gjennomsnittlig 15 % besparelser på papir, toner og blekk

» Måten løsninger for utskriftssikkerhet implementeres på, avgjør ikke bare effektiviteten, men hvor mye de ansattes produktivitet påvirkes. Man må ta nøkkelteknologi, -personer og -prosesskrav med i betraktningen for å sikre maksimale fordeler.

I denne hviteboken

Denne hviteboken er basert på primære og sekundære undersøkelser IDC har utført mtp. IT-sikkerhet og utskriftsrelatert sikkerhet. IDC gjennomførte dybdeintervjuer fra juli til september 2015 med personer ansvarlige for implementering og administrering av skriversikkerhetsløsninger i 16 organisasjoner. Intervjuene var utformet slik at IDC skulle forstå den kvantitative og kvalitative innvirkningen av organisasjonenes bruk av skriversikkerhetsløsninger i virksomheten. Intervjuene gjenspeilet opplevelsene i et bredt spekter av organisasjoner. Tabell 1 gir en oversikt over utskriftsmiljøene i de 16 organisasjonene som ble intervjuet.

TABELL 1

Firmografikk av intervjuede organisasjoner – dybdeintervjuer

	Gjennomsnitt	Median	Område
Antall ansatte	60 300	20 500	200 til 290 000
Antall IT-ansatte	4 500	610	40 til 25 000
Antall IT-brukere	57 200	19 500	180 til 290 000
Totalt antall skrivere	8 800	1 200	4 til 100 000
Antall brukere som skriver ut	50 800	9 000	200 til 280 000
Antall sider skrevet ut per år	51 millioner	10 millioner	10 000 til 300 millioner
Bransjer	Telecom, produksjon, finans, forlag, romfart, bioteknologi, utdanning og helse		

n = 16 organisasjoner

kilde: IDCs intervjuer om skriversikkerhet, 2015

IDC Analyze the Future

IDC supplerte dybdeintervjuene med analyser på grunnlag av undersøkelsesarbeid. Kvalifiserte respondenter kom fra fulltidsansatte i over 440 organisasjoner av alle størrelser. Respondentene måtte ha kjennskap til utskriftsutstyret som ble brukt i selskapet, samt kunnskaper om selskapets policyer for IT-sikkerhet.

Situasjonsoversikt

Hvorfor bedrifter bør tenke på skriver-/dokumentinfrastruktursikkerhet

De fleste organisasjoner har gjort IT-sikkerhet til en prioritet i organisasjonene sine, og det med god grunn. Utbredelsen av data-, mobil- og skyteknologier og lignende legger til rette for et IT-miljø der kunnskapsmedarbeidere trenger og krever tilgang til forretningsinformasjon «når som helst og hvor som helst». IDC har imidlertid oppdaget at utskriftsaktiva og utskriftsrelaterte teknologier er et element som ofte blir oversett i en organsiasjons IT-sikkerhetsstrategi.

Så hvorfor bør bedrifter endre den eksisterende tilnærmingen til utskriftssikkerhet og sikre utskriftsenhetene på samme måte som de sikrer andre teknologier (PC-er, servere, mobilenheter osv.)? Svaret er at en usikret utskriftsinfrastruktur innebærer et generelt usikret IT-miljø. Risikoen for skriverrelaterte sikkerhetsbrudd er høyere enn man kanskje forventer, og det er kostbare konsekvenser.

IDC-spørreundersøkelser avdekket at over halvparten av selskapene har opplevd et IT-sikkerhetsbrudd som inkluderte utskriftssikkerhet de siste tolv månedene.

IDC-spørreundersøkelser avdekket at over halvparten av selskapene har opplevd et IT-sikkerhetsbrudd som inkluderte utskriftssikkerhet de siste tolv månedene. Denne sårbarheten kan komme fra skadelige angrep i eller utenfor organisasjonen, samt uforsiktig bruk av utskriftsenheter og utskrifter. Potensielle utskriftsrelaterte brudd kan skje gjennom nettverksporter, oppfanging av utskrifts-/kopierings-/skannejobber, skriver/MFP-harddisker og minne (RAM), utskrevne eller kopierte dokumenter som blir liggende i utskuffer, eller ulovlig bruk av sikre medier (sjekker, resepter) og så videre. Detaljer:

- Usikrede nettverksporter er et inngangspunkt til selskapets nettverk og informasjon.
- Utskrift av konfidensielle dokumenter (f.eks. dokumenter med pasientopplysninger eller finansielle klienttransaksjoner) på delte skrivere der dokumenter blir liggende i utskuffen over tid, utgjør en mulighet for tyveri av konfidensiell informasjon og manglende overholdelse av forskrifter.
- Ukryptert overføring av skriver-/skannerdata er praktisk talt en invitasjon til hackere.

Sikkerhetsbrudd er kostbare. Det finnes tre typer potensielt økonomiske belastninger:

- **Selskapsressurser som brukes til å håndtere bruddet.** Selskaper som opplever et sikkerhetsbrudd, vil bruke et betydeig antall arbeidstimer og penger til å rydde opp etter hendelsen. Potensielt inntektsgenererende muligheter forsinkes eller stoppes for å håndtere den.
- **Bøter/straffer.** Selskaper kan bli straffet økonomisk for manglende overholdelse (f.eks. HIPAA) eller saksøkes etter et brudd på klient-kunde-konfidensialitet.
- **Selskapets omdømme.** I etterkant av hendelsen kan organisasjonen fremdeles lide økonomisk på grunn av redusert omdømme etter dårlig omtale i pressen.

Utløsende faktorer for sikring av utskriftsinfrastruktur

Basert på dybdeintervjuer med organisasjoner som har distribuert ulike nivåer av utskriftssikkerhet, fant vi følgende utløsende faktorer for deres implementering:

- sikkerhets- og samsvarsproblemer (inkludert reaksjon på brudd)
- proaktiv sikkerhetsstandardisering av hele IT-infrastrukturen
- kostnadsbesparelser og IT-effektivitet

Sikkerhets- og samsvarsproblemer

Sikkerhetsproblemer i immateriell eiendom (IP), konfidensiell eller begrenset informasjon, overholdelse av forskrifter samt behov for en virksomhetsomfattende, ensartet og sikker IT-infrastruktur er viktige pådrivere for et utskriftssikkerhetsprogram. Noen organisasjoner distribuerer reaktivt mer robuste utskriftssikkerhetsprogrammer som svar på tidligere hendelser eller brudd.

Sikkerhetsproblemer i immateriell eiendom (IP), konfidensiell eller begrenset informasjon, overholdelse av forskrifter samt behov for en virksomhetsomfattende, ensartet og sikker IT-infrastruktur er viktige pådrivere for et utskriftssikkerhetsprogram.

Som en seniorsystemdirektør i et finansselskap uttalte: «Sikkerhetsproblemer finnes overalt, og skriveren er en offentlig tilgjengelig enhet som brukes til konfidensielt, begrenset og ikke-konfidensielt materiell. Alle nettverksenheter som håndterer konfidensielle/begrensede data, er gjenstand for sikkerhets-, samsvars- og revisjonskrav. Derfor måtte vi gjøre dette.»

Standardisering av hele IT-infrastrukturen

Sikkerhetsstandardisering i en organisasjons generelle IT-infrastruktur fremmer også utskriftssikkerhet og relatert dokumentsikkerhet samt en omfattende policy for løsning av eventuelle problemer relatert til bruken av utstyret. En viseadministrerende IT-direktør i et forlag forklarte det slik: «Vi ønsker policydrevet sikkerhet, automatiske løsninger og grunnleggende sikkerhet gjennom identitetssertifikater [for skrivere] i samsvar med tilnærmingen til andre infrastrukturtjenester.»

Kostnadsbesparelser og IT-effektivitet

Alle IT-tiltak som bidrar til å redusere en organisasjons kostnader, vil være attraktive for toppledelsen. Kostnadsbesparelser er en av de ekstra, men viktige, fordelene ved å etterstrebe en plan for sikker utskrift og relatert dokumentsikkerhet. Denne fordelen er ikke nødvendigvis den primære pådriveren for gjennomføring av et utskrifts- og dokumentsikkerhetsprogram, men virkningen var den største fordelen nevnt av én tredjedel av respondentene i undersøkelsen.

Kostnadsbesparelser er en av de ekstra, men viktige, fordelene ved å etterstrebe en plan for sikker utskrift og relatert dokumentsikkerhet.

En senior IT-direktør i et finansselskap forklarte: «Behovet for å beskytte immateriell eiendom og de potensielle økonomiske konsekvensene relatert til datasikkerhetsbrudd dannet grunnlaget for årsaken til at disse løsningene ble implementert. Vi er ganske sikre på at kontrolltiltakene som begrenser tankeløs og unødvendig utskrift, har medført besparelser i både papir- og materialkostnader.»

Det finnes selvsagt også mindre direkte kostnadsbesparelser som kommer som følge av et utskriftssikkerhetstiltak. Flere organisasjoner har pekt på at IT-effektivitet som følge av sentralisering og standardisering av utskrifts- og sikkerhetsadministrasjon, har gitt kostnadsfordeler. Gjennom mer aktiv administrering og sikring av utskrift, er IT-personalet frigitt til andre teknologibehov av høy prioritet i organisasjonen. For eksempel som en IT-direktør ved et universitet forklarte det: «Vi forsøker å konsolidere kostnadsstyring og sentral administrasjon i utskriftsmiljøet.»

Forretningsverdien av skriversikkerhet

IDCs dybdeintervjuer med de 16 organisasjonene som bruker skriversikkerhetsløsninger i virksomheten, avdekket at de oppnår betydelig forretningsverdi gjennom distribusjon av disse løsningene. Intervjuene hvor IDC ba organisasjonene om å beskrive utskriftsmiljøene før og etter distribusjonen av skriversikkerhetsløsninger, viste at organisasjonene oppnår målene med å skape sikrere utskriftsmiljøer, samtidig som de oppnår effektivitet på feltene utskriftsrelaterte kostnader og arbeidstimer.

- **Sikkerhet.** Skrivermiljøer er blitt sikrere, og kostnader relatert til å bøte på databrudd og sikre forskriftsmessig og revisjonsmessig samsvar, er blitt redusert.
- **Effektivt IT-personell.** Mengden arbeidstimer som er nødvendig for å administrere og vedlikeholde skrivermiljøene samt opprette, endre og ta i bruk skriverrelaterte policyer, er redusert, noe som frigjør tid slik at personale kan arbeide med andre tiltak.
- **Kostnadsbesparelser.** Kostnader knyttet til utskrift er redusert gjennom forbedret synlighet og endret utskriftsatferd, inkludert besparelser i form av skrivere og skriverrekvisita.

Risikoreduksjon: Forbedret skriversikkerhet og samsvar

Organisasjoner som ble intervjuet, rapporterte at de har benyttet virksomhetsomfattende skriversikkerhetsløsninger til å redusere konsekvensen av skriverrelaterte sikkerhetsbrudd og gjøre samsvarsarbeidet mer effektivt og lønnsomt.

IDC spurte intervjudeltakerne om hvor ofte skriverrelaterte sikkerhets- og databrudd oppstår i deres organisasjoner, og om organisasjonene har opplevd noe de ville karakterisert som betydelige skriverrelaterte sikkerhetsbrudd. Disse organisasjonene rapporterte en gjennomsnittlig reduksjon i hyppigheten av skriverrelaterte sikkerhetsbrudd med opptil seks ganger etter distribusjon av virksomhetens skriversikkerhetsløsninger. Distribusjon av skriverjobbkryptering, brukergodkjenning og «pull»-utskrift har gitt et nivå av sporbarhet og kontroll som sikrer og bidrar til å hindre at det oppstår brudd. Skriversikkerhet har dessuten bidratt til å komplettere noen av organisasjonenes IT-infrastrukturomfattende sikkerhetstiltak, og derigjennom eliminert resterende sårbarheter. Intervjuede organisasjoner ga eksempler på skriverrelaterte sikkerhetsbrudd som de har opplevd, bl.a.:

Disse organisasjonene rapporterte en gjennomsnittlig reduksjon i hyppigheten av skriverrelaterte sikkerhetsbrudd med opptil seks ganger etter distribusjon av virksomhetens skriversikkerhetsløsninger.

- **Utskrift av konfidensiell informasjon med forsett om misbruk.** En IT-direktør i et produksjonsselskap forklarte at organisasjonen hans mistet immateriell eiendom blant annet som følge av at ansatte skrev ut svært konfidensiell og fortrolig informasjon, og ga den til selskapets konkurrenter.
- **Utskrift og feilhåndtering av sikre data.** En IT-direktør i et finansselskap forklarte at ansatte i organisasjonen utsatte design og annen immateriell eiendom for risiko ved å skrive ut kritikkløst eller la utskrifter ligge på skriveren.

Intervjuede organisasjoner ga flere eksempler på hvordan deres bruk av utskriftssikkerhetsløsninger har hjulpet dem å minimere konsekvensene av sikkerhetsbrudd gjennom skrivere:

- **Beskyttelse av informasjon gjennom hele utskriftsprosessen.** En viseadministrerende IT-direktør i et forlag forklarte det slik: «Løsningen har blitt et viktig verktøy for å beskytte arbeidsflyten av innhold og data til og fra skriverne i nettverket, slik at vi kan redusere muligheten for brudd.»
- **Hindre unødvendig eller upassende utskrift.** En IT-direktør i et finansselskap sa: «Ofte skulle sensitiv dokumentasjon som vi distribuerer internt, aldri vært skrevet ut. Disse løsningene hjelper oss å minimere brudd som i stadig stigende grad oppstår internt, enten med hensikt eller som et resultat av ukritisk utskrift.»

Som tabell 2 viser: Selv om alle skriverrelaterte sikkerhetsbrudd kan medføre kostnader, er det spesielt viktig for organisasjoner å unngå betydelige sikkerhetsbrudd på grunn av de betydelige kostnadene med å bøte på dem. Ifølge de fem intervjuede organisasjonene som har opplevd det de karakteriserte som et betydelig skriverrelatert sikkerhetsbrudd de siste årene, omfatter de gjennomsnittlige kostnadene for et betydelig sikkerhetsbrudd: produktivitetstap for 54 ansatte, 277 arbeidstimer for løsningstiltak og en administrasjonskostnad på over 500 000 USD per brudd, inkludert bøter.

I tillegg til å redusere hyppigheten av skriverrelaterte sikkerhetsbrudd mente 10 av de 16 organisasjonene som ble intervjuet, at skriversikkerhetsløsningene gjorde forskriftsoverholdelse og revisjonsarbeid mer effektivt. Forbedret sikkerhet og sporbarhet gir følgende fordeler:

TABELL 2

Innvirkning av virksomhetsomfattende skriversikkerhetsløsninger på sikkerhetsbrudd – dybdeintervjuer

Sikkerhetsbrudd totalt	
Gjennomsnittlig antall brudd per år – før implementering av skriversikkerhet	9,9
Gjennomsnittlig antall brudd per år – med skriversikkerhet	1,5
Endring i antall sikkerhetsbrudd	Opptil 6 ganger færre
Betydelige sikkerhetsbrudd	
Antall intervjuede organisasjoner som opplever dette	5
Gjennomsnittlig antall berørte ansatte	54
Gjennomsnittlig arbeidstimer nødvendig for å løse dette (timer)	277
Total gjennomsnittlig kostnad for å håndtere hvert brudd (inkludert bøter)	521 400 USD

n = 16 organisasjoner

kilde: IDCs intervjuer om skriversikkerhet, 2015

- **Forbedret sikkerhet:** En systemdirektør i et finansselskap sa: «I kjernen av implementering av denne sikkerhetsmodellen er fordelen med at du får bygd et svært robust og sikkert miljø som beskytter data og dokumenter, øker konfidensialiteten for design og arkitektur og sikrer skrivere. Dette har i betydelig grad bidratt til at vi kan oppfylle sikkerhetsstandardene våre.»

- **Sporbarhet og synlighet:** En viseadministrerende IT-direktør i et biovitenskapsselskap forklarte det slik: «Vi har kunnet opprette et revisjonsspor, hindre oppfanging av data og vise at vi har begrenset brukertilgang til konfidensielle data. Dessuten inkluderer verifisering og revisjon identifikasjon og trusselanalyse samt anbefalte løsninger på problemer. Vi får detaljert oversikt over systemstatus og kan overvåke systemet i sanntid. Alt dette er samsvarskrav.»

Disse forbedringene har også gitt tids- og kostnadsbesparelser for samsvars- og revisjonsarbeidet i organisasjonene. I gjennomsnitt rapporterte de intervjuede organisasjonene at deres bruk av skriversikkerhetsløsninger ga årlige besparelser på over 200 arbeidstimer for ansatte og nesten 250 000 USD per år i relaterte kostnader, inkludert støttekostnader fra tredjepart for revisjoner og forskriftsoverholdelse.

Produktivitetsfordeler for IT-personell

Organisasjoner som IDC intervjuet, rapporterte at de hadde redusert tidsbelastningen med å administrere og støtte skrivermiljøene etter distribusjonen av skriversikkerhetsløsninger. Denne økte effektiviteten skyldes faktorer som å innføre eller utvide bruken av sentraliserte administrasjonsfunksjoner og automatisering, samt mulighet til å løse skriverrelaterte problemer raskere. En senior IT-direktør i et finansselskap forklarte: «Innvirkningen på personalet [ved å bruke skriversikkerhetsløsninger] har vært stor, både når det gjelder investerte timer i tidskrevende aktiviteter samt frigjøring av teamet slik at de kan fokusere på mer strategiske aktiviteter. Responsen på skriverrelaterte problemer er ikke lenger usammenhengende, men helhetlig og repeterbar.» Som et resultat av distribuerte skriversikkerhetsløsninger, har personalet i gjennomsnitt halvert tiden de bruker på å støtte skrivermiljøene, ifølge organisasjonene IDC har intervjuet.

Som et resultat av distribuerte skriversikkerhetsløsninger, har personalet i gjennomsnitt halvert tiden de bruker på å støtte skrivermiljøene, ifølge organisasjonene IDC har intervjuet.

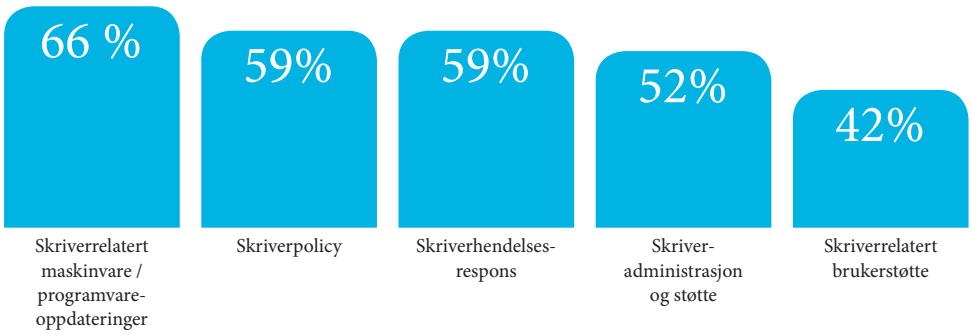
Intervjuede organisasjoner rapporterte at skriversikkerhetsløsninger hadde muliggjort effektivisering for personale som var ansvarlige for sine skrivermiljøer. Reduserte arbeidstimer fulgte av endringer som automatisering av støtte og vedlikehold, inkludert gjennom sertifikatautomatisering samt bruk av andre repeterbare prosesser. En viseadministrerende direktør i et finansselskap som benyttet unike seritifikat- og ansattgodkjenningspolicyer, forklarte for eksempel hvordan hans organisasjon har oppnådd en 60 % reduksjon i tiden personalet bruker på å overvåke enheter: «Vi sparer IT-tid fordi profiler enkelt kan opprettes og overføres til mange enheter samtidig, og vi kan automatisere sertifikatadministrasjon.»

I mellomtiden drar intervjuede organisasjoner også nytte av tidsbesparelser muliggjort av skriversikkerhetsløsning når det gjelder oppretting, bruk og endring av skriverrelaterte policyer. Personale i disse organisasjonene bruker i gjennomsnitt 59 % mindre tid på skriverrelaterte policyer. Utover besparelser av arbeidstimer, har mer effektiv implementering av skriverrelaterte policyer fordeler som å redusere sannsynligheten for brudd samt oppretting av mer effektive retningslinjer for skriverbruk.

Når skriverrelaterte problemer oppstår, rapporterte intervjuede organisasjoner at personalet har dratt nytte av funksjoner i skriversikkerhetsløsningene, som å ha (eller bedre utnyttelse av) sentrale konsoller og ekstern tilgang til skrivere. Disse faktorene, sammen med forbedret skriverrelatert policy, har hjulpet intervjuede organisasjoner med å redusere mengden nødvendig tid til å respondere på skriverrelaterte hendelser og skriverrelaterte henvendelser fra skriverbrukere med et gjennomsnitt på henholdsvis 59 % og 42 % (se figur 1). En viseadministrerende IT-direktør i et forlag som brukte sikkerhetsløsninger som omfattet automatisk løsning og administrasjon av unike sertifikater, forklarte effekten på teamets evne til å støtte skrivere: «Det er nå færre problemer, og de som finnes, tar samlet sett kortere tid å håndtere. Effekten, som er fordelaktig, er at det frigjør tid til andre støtte- og planleggingsaktiviteter.» En IT-sjef i et finansselskap som bruker et produkt for administrasjon av skriversikkerhet, sa: «Kundeservice har nå en klar oversikt over skriverinnstillinger, tillatelser og problemer, og kan enten handle uavhengig eller kontakte et lite skriverstøtteteam på andrelinje.»

FIGUR 1

Gjennomsnittlig tidsbesparelse for skriverrelatert personale – dybdeintervjuer



n = 16 organisasjoner

kilde: IDCs intervjuer om skriversikkerhet, 2015

Utskriftsrelaterte kostnadsreduksjoner

Alle vesentlige IT-tiltak som også reduserer kostnader, gjør dem mer attraktive. Derfor har de intervjuede organisasjonenes mulighet til å oppnå kostnadsbesparelser gjennom distribusjon av skriversikkerhetsløsninger vært en vesentlig merverdi. Rutiner som ansattgodkjenning og «pull»-utskrift var blant de mest brukte av intervjudeltakerne (brukt av over to tredjedeler av organisasjonene som ble intervjuet). Disse løsningene bevarer dokumentkonfidensialitet og fremmer kostnadsbesparelser ved å kreve at utskriftsbrukerne gjennomfører bekreftende tiltak for å skrive ut dokumenter, og ved å redusere antall uavhentede eller feilsendte utskriftsjobber. Skriversikkerhetsløsningenes mulighet til å fungere som et verktøy for reduksjon av skriverrelaterte kostnader, er klar nok til at flere intervjuede organisasjoner nevnte kostnadsoptimering som den primære pådriveren for deres bruk av skriversikkerhetsløsninger.

Intervjuede organisasjoner forklarte at skriversikkerhetsløsninger hjalp dem å redusere kostnader gjennom:

- **Reduksjon av utskrifter ved å endre utskriftsatferd:** En økonomiansvarlig i et selskap i matbransjen sa: «Funksjonen for 'pull'-utskrift vi bruker, gir mulighet til å sende til utskrift, men krever at du går og faktisk plasserer skiltet ditt på skriveren for å få skrevet ut. Jeg tror det har redusert utskriftene, ut fra de siste tallene jeg så, med mellom 21 % og 24 % i forhold til tidligere.»
- **Synlighet i bruken av skrivere:** En IT-direktør ved et universitet rapporterte: «Vi kan nå spore kostnaden for utskrevne sider for å belaste de enkelte avdelingene.» Med mulighet til å fordele utskriftskostnadene avdelingsvis kan universitetet legge byrden på hver avdeling, som da må få skriverbrukerne til å bli så effektive som mulig.
- **Avvikling av overflødige eller foreldede skrivere:** En viseadministrerende direktør i et finansselskap sa: «Vi reduserer antall unødvendige skriverjobber fordi folk vet at utskriftsaktivitet overvåkes, og vi tar ut av drift og erstatter gammel skrivermaskinvare som ikke kan støtte virksomhetens utskriftssikkerhetsrutiner.»

Skriversikkerhetstiltak har gjort ansatte som skriver ut, mer bevisste på hvordan de bruker skriverne, og har bidratt til skriverrelaterte kostnadsbesparelser.

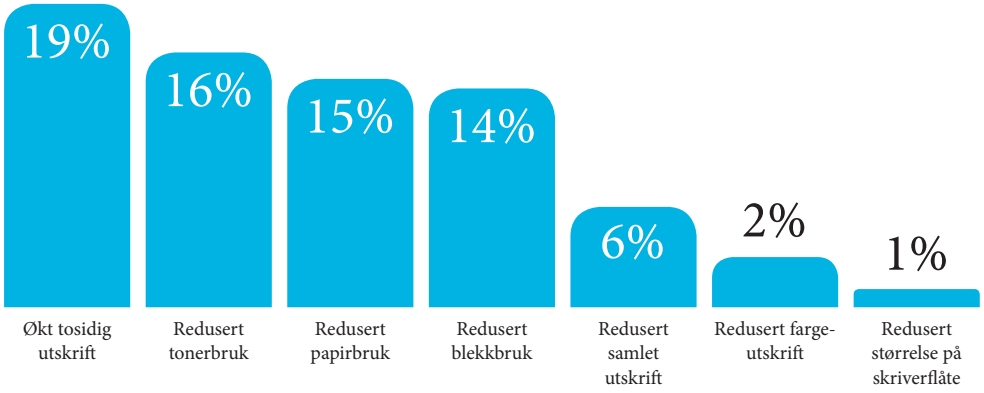
Skriversikkerhetstiltak har gjort ansatte som skriver ut, mer bevisste på hvordan de bruker skriverne, og har bidratt til skriverrelaterte kostnadsbesparelser. Gjennomsnittlig sa intervjudeltakerne at de ansatte sender 43 % færre utskriftsjobber til feil skriver. Dermed blir færre utskriftsjobber forkastet eller gjentatt. Som vist i figur 2, har disse typene forbedringer bidratt til mer effektiv skriverbruk generelt, inkludert færre utskrifter totalt (gjennomsnittlig 6 % reduksjon), flere tosidige utskrifter (19 % økning) og litt færre utskrifter i farger (2 % reduksjon). Disse faktorene, samt forbedret synlighet i skrivermiljøene, har gjort det mulig for intervjuede organisasjoner å oppnå store kostnadsbesparelser i utskriftsmiljøene. Dette inkluderer antall skrivere de distribuerer og vedlikeholder (1 % reduksjon eller 115 skrivere i

gjennomsnitt per organisasjon) samt kostnadene knyttet til papir, blekk og toner (henholdsvis 15 %, 14 % og 16 % reduksjon).

FIGUR 2

Gjennomsnittlige kostnadsbesparelser i skrivermiljø og skrivereffektivitet – dybdeintervjuer

(% effektivitet eller forbedring)



n = 16 organisasjoner

kilde: IDCs intervjuer om skriversikkerhet, 2015

Utfordringer

Med så å si alle organisasjonsutrullinger kan enkelte utfordringer unngås ved å planlegge. Studiegruppens utfordringer strakte seg over alle tre fasene i en skriversikkerhetsutrulling: planlegging, implementering og etterimplementering.

De studerte selskapene rapporterte at de følte at de hadde dårlig tid til å utvikle strategien og planen. Betydelig tid på forhånd er nødvendig for å oppnå reduksjon i IT-arbeidsbelastningen etter implementering. Håndheving av ansattes overholdelse bør dessuten være en automatisert prosess som innbefatter overvåkingsverktøy, en eskaleringsprosess og tiltak for å redusere utskriftsrelaterte henvendelser til brukerstøtte.

For en organisasjons skriverbrukere har vi notert to punkter det bør planlegges for:

- **Balanser streng utskriftssikkerhet samtidig som ansattes produktivititetspåvirkning minimeres:** Bedriftssikkerhet må være av høyeste viktighet, men en organisasjon bør arbeide i et system på en måte som har minst negativ produktivitetsinnvirkning. Noen organisasjoner som implementerer «pull»-utskrift for å håndtere utskriftssikkerhetsbehovene, kan for eksempel støte på motstand fra brukerne på grunn av behovet for å bekrefte (dvs. oppgi et passord) og så vente på at hele dokumentet skrives ut. Fordelen i dette scenarioet er beskyttelsen av informasjonen i dokumentet (f.eks. kan

ingen lese utskrevne dokumenter som ligger i papirskuffen uten tilsyn) kontra det å vente på at et dokument skrives ut (f.eks. at utskriften ikke starter før brukeren har bekreftet sin identitet på enheten).

- **Ansattopplæring:** Relatert til ansattes produktivitet må utskriftssikkerhetsplanen inkludere prosessen og tiden som er nødvendig til å lære opp ansatte i alle nye policyer og prosedyrer. Virksomheter må være forberedt på å gjenta opplæringen og til å bruke ulike formater for å håndtere forskjeller i ansattes alder og læringsstil.

Viktig veiledning

IDC har identifisert flere overbevisende årsaker til å innarbeide skriver- og relaterte dokumentarbeidsflyter i et organisasjonsomfattende IT-sikkerhetsrammeverk. Én av de største fordelene er åpenbart knyttet til et omfattende IT-sikkerhetsprogram som inkluderer utskrift, men en slik plan har også et antall betydelige fordeler utover sikkerhet. To viktige fordeler er merkbare kostnadsbesparelser og økt IT-effektivitet.

IDC anbefaler at en organisasjon gjør utskrifts-/dokumentsikkerhetsteknologien skuddsikker. Organisasjonen må anerkjenne at målet bare kan nås når personer og prosesser er innarbeidet i planens utførelse.

IDC anbefaler at en organisasjon gjør utskrifts-/dokumentsikkerhets-teknologien skuddsikker.

Teknologi

Når det gjelder sikkerhet, er implementering av teknologiløsninger hovedsakelig en svart-hvitt-sak: En organisasjon er enten sikker eller ikke sikker.

IDC anbefaler at følgende funksjonalitet implementeres i hele organisasjonen så snart som mulig. IT-personell og leverandører av utskriftsinfrastruktur må sikre at følgende funksjoner og muligheter er konfigurerte og aktive for alle utskriftsenheter i hele organisasjonen:

- Sikre at alle utskriftsenheter i nettverket har følgende funksjoner, eller minst har oppgradert fastvare for å gjenspeile dem.
- Kontrollere at enheter bare bruker krypterte kommunikasjonsprotokoller, og deaktivere resten.
- Implementere et system som sletter eller destruerer enhetens data på harddisken som del av å ta enheten ut av drift.
- Støtte minst én type brukergodkjenning (fortrinnsvis to eller tre), og vurdere implementering av «pull»-utskrift for utskriftsmiljøer med et stort volum av konfidensiell informasjon eller samsvarskrav.

- Sikre at fastvare er oppdatert og at bare legitim fastvare brukes.
- Kontrollere at alle skriverharddisker er sikre (data skal krypteres og slettes regelmessig).
- Distribuere funksjoner som viser om utskriftene er tuklet med, eller bruke skrivere med skuffer som kan låses for spesialmedier hvis organisasjonens utskrifter krever det. Dette sikrer utskrifter som er et potensielt mål for svindel, som sjekker, medisinresepter og så videre.
- Bruke et verktøy for flåteadministrasjon til å administrere, overvåke og løse problemer på enheten sentralt, for å sikre samsvar med sikkerhetspolicyer. På denne måten kan organisasjonen unngå å måtte konfigurere og vedlikeholde hver enhet manuelt. Verktøyet bør muliggjøre enkel oppretting og administrasjon av sikkerhetspolicyen, oppdage når enheter legges til i nettverket, gi mulighet for unik enhetssertifikatadministrasjon samt loggføre ikke-samsvarende hendelser og løse hendelsene gjennom en eskalerings- og løsningsprosess. Verktøyet bør fungere sammen med virksomhetsomfattende verktøy for IT-sikkerhetsadministrasjon som overvåker endepunkter for ikke-samsvarende hendelser og uregelmessigheter, slik at potensielle sikkerhetsbrudd identifiseres raskt.
- Kontrollere at utskrifter og skanninger på både stasjonære og mobile enheter (enten i bevegelse eller i ro) er krypterte, for å sikre at utskriftsrelaterte data er fullt beskyttet. Dette betyr at også vedlegg som skal skrives ut, må åpnes og avbildes for et ekstra beskyttelsesnivå. Et verktøy som overvåker utskrift- og skanningsinnhold er et viktig element i å sikre det høyeste nivået av sikkerhet, og for å være i samsvar med etablerte bedriftspolicyer og bransjestandarder.

Folk

En organisasjon som tar IT-sikkerhet på alvor, må sikre at sikkerhetsteamet inkluderer personell som har ekspertise innen sikring av utskriftsenheter og relaterte dokumentarbeidsflyter. Dette sikkerhetsteamet kan bestå av organisasjonens eget personale og/eller eksterne sikkerhetsressurser med riktige kunnskaper. Teamets ressurser vil bli brukt til å gi råd om fremtidige sikkerhetsproblemer relatert til utskrift og arbeidsflyt, samt bidra til integreringen av en virksomhetsomfattende IT-sikkerhetsplan.

For å sørge for at sikring av utskriftsenheter og relaterte dokumentarbeidsflyter ikke får negativ innvirkning på ansattes produktivitet bør organisasjonen innhente innspill fra utvalgte ansatte i organisasjonen som del av planleggingsprosessen. Det anbefales også å involvere en ekspert på endringsstyring, spesielt hvis mengden eller typen endringer som kreves, er betydelig. En slik ekspert kan også gi råd i forbindelse med distribuerings- og opplæringstilnærmingen som bør brukes.

De fleste organisasjoner har ikke de nødvendige kunnskapene og ferdighetene til å sikre utskrifts- og dokumentinfrastrukturen på egen hånd. Organisasjoner bør derfor vurdere å spørre leverandøren av utskriftsenheten om ressurser som IT-avdelingen kan benytte. Ressurser strekker seg over sikkerhetsfunksjoner som er tilgjengelig i en organisasjons skriver-/MFP-maskinvare, sikkerhetsprogramverktøy og sikkerhetstjenester (f.eks. profesjonelle sikkerhetstjenester, sikkerhetsvurderinger, endringsstyring og ekspertise innen overholdelse av forskrifter for spesifikke bransjer).

Prosess

Det er viktig at en organisasjon starter sikkerhetstiltaket ved å vurdere gjeldende status i utskriftsmiljøet, og utvikle en plan som oppnår et nivå av sikkerhet på linje med resten av IT-miljøet. Dette tiltaket bør inkludere en forståelse av de vesentlige sikkerhetskravene spesifikke for organisasjonens bransje, samt en plan for å overvåke, eskalere, løse og håndheve disse policyene løpende.

Planen bør evalueres på nytt med jevne mellomrom ved å bruke data samlet inn i perioden, for å avgjøre om det er nødvendig med justeringer og for å lære av utskrifts-/dokumentbrudd utenfor selskapet. Eventuelle justeringer påvirkes av dataene som samles inn, samt organisasjonens akseptable nivå av risiko og sikkerhet.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Om IDC

International Data Corporation (IDC) er den fremste globale leverandøren av markedsinformasjon, rådgivningstjenester og arrangementer for IT-, telekommunikasjons- og forbrukerteknologimarkedene. IDC hjelper IT-personell, bedriftsledere og investormiljøet med å treffe faktabaserte beslutninger om teknologianskaffelser og forretningsstrategi. Over 1100 IDC-analytikere gir global, regional og lokal ekspertise innen teknologi og bransjemuligheter og trender i over 110 land over hele verden. I 50 år har IDC levert strategisk innsikt for å hjelpe klientene å nå sine forretningsmål. IDC er et datterselskap av IDG, verdens ledende selskap innen medier, forskning og arrangementer knyttet til teknologi.