Gesponsord door: **HP**

Auteurs:
Angèle Boyd
Keith Kmetz
Matthew Marden

November 2015

De bedrijfswaarde van printerbeveiliging

OPINIE VAN IDC

In een onderzoek van IDC gaf 80% van de ondervraagde bedrijven aan dat IT-beveiliging belangrijk is voor hun bedrijfsprocessen, maar slechts 59% van deze groep vond dat ook printbeveiliging relevant was voor de bedrijfsprocessen. Daarbij komt dat het senior management bijna 40% meer betrokken is bij beslissingen over IT-beveiliging als geheel dan over printbeveiliging. Volgens ons wijst dit op een gebrek aan aandacht voor printbeveiliging, wat bedrijven onnodig kwetsbaar maakt. Uit onderzoek van IDC blijkt dat er dwingende redenen zijn waarom bedrijven meer moeten focussen op printbeveiliging omdat een veilige printomgeving IT en bedrijf aanzienlijke voordelen biedt, zoals:

» Onderzoek van IDC wijst uit dat meer dan de helft van de ondervraagde bedrijven de afgelopen 12 maanden te maken heeft gehad met een schending van de IT-beveiliging waarbij ook printbeveiliging een rol speelde.

» De print-/documentomgeving van elke onderneming en organisatie telt een groot aantal kwetsbare elementen. Deze kwetsbaarheden zijn het gevolg van kwaadwillige aanvallen van binnenuit het bedrijf en van buitenaf, maar ook van een onzorgvuldig gebruik van printapparatuur en uitvoer. Potentiële printgerelateerde schendingen van de beveiliging kunnen plaatsvinden via de netwerkpoort van een apparaat, door onderschepping van print-/kopieer-/scantaken, via opslagschijven en geheugen (RAM) in printers en MFP's, doordat afgedrukte of gekopieerde documenten in de uitvoerbak achterblijven of door oneigenlijk gebruik van beveiligde media (cheques, recepten) en dergelijke.

» Uit diepgaande gesprekken die IDC hield met ondernemingen die enige vorm van print- en documentworkflowbeveiliging toepassen kwam naar voren dat twee typen ondernemingen iets doen aan print-/documentbeveiliging:

- Bedrijven die vanwege veiligheids- en compliancevereisten een enterprisebrede beveiligde IT-infrastructuur hebben
- Bedrijven die hun kosten willen verlagen en IT efficiënter willen maken met behulp van

beveiligingsinitiatieven

» Uit gesprekken van IDC met ondernemingen die een printbeveiligingsprogramma hebben opgezet bleek dat deze de grootste voordelen en meeste bedrijfswaarde behalen op drie gebieden: betere printerbeveiliging, efficiëntere IT-teams en kostenbesparing. De ondervraagde bedrijven meldden een aantal belangrijke verbeteringen in hun print- en beveiligingsomgeving, zoals:

- Gemiddeld zesmaal minder printergerelateerde beveiligingsschendingen na installatie van printerbeveiligingsoplossingen
- Gemiddeld een halvering van de tijd die nodig is voor ondersteuning van de printeromgeving na implementatie van printerbeveiligingsoplossingen
- Een gemiddelde besparing van 15% op papier-, toner- en inktkosten

» De manier waarop printerbeveiligingsoplossingen worden geïnstalleerd bepaalt niet alleen de effectiviteit, maar ook de gevolgen voor de productiviteit van werknemers. Om optimaal profijt te halen uit deze oplossingen moeten bedrijven rekening houden met vereisten ten aanzien van technologie, mensen en processen.

In deze whitepaper

Deze whitepaper is gebaseerd op direct en indirect onderzoek van IDC naar IT- en printerbeveiliging. IDC hield van juli t/m september 2015 uitvoerige gesprekken met personen uit 16 ondernemingen die verantwoordelijk zijn voor de implementatie en het

TABEL 1

Ondervraagde bedrijven – diepgaande gesprekken

	Gemiddeld	Mediaan	Bereik
Aantal werknemers	60.300	20.500	200 tot 290.000
Aantal IT-medewerkers	4500	610	40 tot 25.000
Aantal IT-gebruikers	57.200	19.500	180 tot 290.000
Totaal aantal printer	8800	1200	4 tot 100.000
Aantal gebruikers dat print	50.800	9000	200 tot 280.000
Afgedrukte pagina's per jaar	51 miljoen	10 miljoen	10.000 tot 300 miljoen
Branches	Telecom, productie, financiële dienstverlening, uitgeverij, luchtvaart, biotechnologie, onderwijs en gezondheidszorg		

n=16 organisaties

Bron: IDC's interviews over printerbeveiliging, 2015

IDC Analyze the Future

beheer van printerbeveiligingsoplossingen. De gesprekken hadden tot doel om IDC inzicht te geven in de kwantitatieve en kwalitatieve gevolgen van het gebruik van printerbeveiligingsoplossingen in deze ondernemingen. In de interviews kwamen de ervaringen van uiteenlopende organisaties ter sprake. Tabel 1 bevat een overzicht van de printomgevingen van de 16 ondervraagde bedrijven.

IDC vulde de gesprekken aan met analyses van gegevens uit andere enquêtes. De gekwalificeerde respondenten waren afkomstig uit meer dan 440 grote en kleine organisaties, waar zij als fulltime medewerkers werkzaam waren. De ondervraagden moesten kennis hebben van de gebruikte printapparatuur en het IT-beveiligingsbeleid in hun bedrijf.

De situatie

Waarom moeten bedrijven de beveiliging van hun print-/documentinfrastructuur serieus aanpakken

De meeste ondernemingen geven IT-beveiliging een hoge prioriteit en dat is niet zonder reden. Door de sterke toename van computing, mobiliteit, cloud en andere technologieën ontstaat een IT-omgeving waarin kenniswerkers altijd en overal toegang moeten hebben tot bedrijfsinformatie. IDC merkt echter dat printapparaten en printgerelateerde technologie in de IT-beveiligingstrategie van ondernemingen vaak worden vergeten.

Uit onderzoek van IDC bleek dat ruim de helft van de ondervraagde bedrijven in de afgelopen 12 maanden te maken had met een inbreuk op de IT-beveiliging waarbij ook printbeveiliging een rol speelde.

Waarom moeten bedrijven hun printerbeveiliging anders benaderen en hun printapparatuur net zo beveiligen als hun andere technologie (pc's, servers, mobiele devices en dergelijke)? Het antwoord luidt: "omdat een niet-beveiligde printinfrastructuur de veiligheid van de hele IT-omgeving in gevaar brengt". Het risico van printergerelateerde schendingen van de beveiliging is groter dan men zou verwachten en kan leiden tot dure schadeclaims.

Uit onderzoek van IDC bleek dat ruim de helft van de ondervraagde bedrijven in de afgelopen 12 maanden te maken had met een inbreuk op de IT-beveiliging waarbij ook printbeveiliging een rol speelde. Deze kwetsbaarheid is het gevolg van kwaadwillige aanvallen van binnenuit het bedrijf en van buitenaf, maar ook van een onzorgvuldig gebruik van printapparatuur en uitvoer. Potentiële printgerelateerde schendingen van de beveiliging kunnen plaatsvinden via netwerkpoorten, door onderschepping van print-/kopieer-/scantaken, via opslagschijven en geheugen (RAM) in printers en MFP's, doordat afgedrukte of gekopieerde documenten in de uitvoerbak achterblijven of door oneigenlijk gebruik van beveiligde media (cheques, recepten) en dergelijke. Om dit nader preciseren:

- Niet-beveiligde netwerkpoorten geven toegang tot het bedrijfsnetwerk en informatie.
- Het printen van vertrouwelijke documenten (bijvoorbeeld met patiëntgegevens of financiële transacties van klanten) op gedeelde printers waar de documenten in de uitvoerbak blijven liggen werkt diefstal van vertrouwelijke informatie in de hand en maakt dat bedrijven niet aan de regelgeving voldoen.
- Verzending van niet versleutelde print-/scangegevens is bijna een uitnodiging voor hackers.

Inbreuken op de beveiliging zijn duur. Er zijn drie typen potentieel kostbare schadeposten:

- **Personeel dat in actie moet komen na de schending.** In bedrijven waar een inbraak plaatsvindt is veel tijd en geld gemoeid met 'opruimingswerkzaamheden' na een incident. Kansen om inkomsten te genereren gaan voorbij of worden pas later benut.
- **Boetes/schadeclaims.** Bedrijven kunnen boetes krijgen omdat ze zich niet aan de wet (bijvoorbeeld HIPAA) houden en klanten wiens privacy geschonden is kunnen een rechtszaak aanspannen.
- **Reputatieschade voor het bedrijf.** In de nasleep van een incident kan het bedrijf nog meer financieel verlies lijden door reputatieschade.

Zorgen over de beveiliging van intellectueel eigendom en vertrouwelijke informatie, het voldoen aan regelgeving en de behoefte aan een consistente, enterprisebrede, veilige IT-infrastructuur zijn de voornaamste drijfveren voor het opzetten van rintbeveiligingsprogramma.

Redenen om de printerinfrastructuur te beveiligen

Uit diepgaande gesprekken met ondernemingen die verschillende niveaus van printerbeveiliging toepassen is gebleken dat zij dit om de volgende redenen doen:

- Zorgen over veiligheid en compliance (vaak als reactie op een inbreuk)
- Proactieve standaardisering van de beveiliging in de hele IT-infrastructuur
- Kostenbesparing en IT-efficiëntie

Veiligheid en compliance

Zorgen over de beveiliging van intellectueel eigendom en vertrouwelijke informatie, het voldoen aan regelgeving en de behoefte aan een consistente, enterprisebrede, veilige IT-infrastructuur zijn de voornaamste drijfveren voor het opzetten van een printbeveiligingsprogramma. Sommige organisaties implementeren een nog krachtigere printbeveiliging na een incident of inbraak in hun systeem.

IDC Analyze the Future

In de woorden van een senior systeemdirecteur bij een financiële dienstverlener: "De veiligheid wordt overal bedreigd en de printer is een vrij toegankelijk apparaat dat wordt gebruikt voor vertrouwelijke en niet-vertrouwelijke documenten. Voor alle netwerkapparaten die vertrouwelijke gegevens bevatten gelden beveiligings-, compliance- en auditvereisten; daarom moesten we dit doen."

Kostenbesparingen zijn een van de bijkomende, maar belangrijke voordelen van het opzetten van een print- en documentbeveiligingsplan.

Standaardisering in de hele IT-infrastructuur

Standaardisering van de beveiliging in de hele IT-infrastructuur van een bedrijf omvat ook print- en documentbeveiliging en een beleid voor het oplossen van problemen bij het gebruik van deze apparatuur. Een vicepresident informatietechnologie bij een uitgeverij zei hierover: "Wij waren op zoek naar policygestuurde beveiliging, automatische probleemoplossing en de elementaire beveiliging van identiteitscertificaten [voor printers] die aansloot bij onze aanpak van andere infrastructuurservices."

Kostenbesparing en IT-efficiëntie

Elke IT-initiatief dat helpt om de operationele kosten van een onderneming te reduceren kan rekenen op de steun van het senior management. Kostenbesparingen zijn een van de bijkomende, maar belangrijke voordelen van het opzetten van een print- en documentbeveiligingsplan. Dit voordeel is niet de voornaamste reden voor het creëren van een print- en documentbeveiligingsprogramma, maar eenderde van de ondervraagden noemde het wel het belangrijkste pluspunt.

Een senior IT-directeur in een instelling voor financiële dienstverlening zei: "De noodzaak om intellectueel eigendom te beschermen en de potentiële financiële gevolgen van dataschendingen te beperken was onze aanleiding om deze oplossingen te kiezen … wij merken dat de controlemechanismes die onnodig en gedachteloos printen inperken ons veel geld besparen op de papier- en materiaalkosten."

Natuurlijk zijn er ook 'indirecte' kostenbesparingen als gevolg van printbeveiligingsinitiatieven. Verschillende ondernemingen wezen erop dat IT na de centralisatie en standaardisering van printer- en beveiligingsbeheer efficiënter werkt en dat ook dit kostenvoordelen oplevert. Als de printomgeving actiever wordt beheerd en beveiligd, houdt IT meer tijd over om in andere belangrijke technologiebehoeften van de organisatie te voorzien. Een IT-directeur van een universiteit beschreef het als volgt: "Wij wilden controle over de kosten en centraal beheer van onze printomgeving consolideren."

De bedrijfswaarde van printerbeveiliging

Uit IDC's uitvoerige gesprekken met 16 ondernemingen die gebruikmaken van enterprise printerbeveiligingsoplossingen blijkt dat deze oplossingen een aanzienlijke bedrijfswaarde opleveren. IDC vroeg de bedrijven hun printeromgeving voor en na de implementatie van printerbeveiligingsoplossingen te beschrijven. Uit de antwoorden bleek dat ondernemingen hun doel van het creëren van een veilige printomgeving bereiken en tegelijkertijd de efficiëntie verbeteren doordat de printgerelateerde kosten dalen en werknemers tijd besparen.

Gemiddeld meldden deze ondernemingen een zesvoudige afname van het aantal printergerelateerde schendingen van de beveiliging sinds de installatie van enterprise-printerbeveiligingsoplossingen.

- **Beveiliging.** Printeromgevingen zijn veiliger geworden en de kosten voor het afhandelen van dataschendingen en het waarborgen van compliance met regelgeving en audits zijn gedaald.
- **Efficiëntere IT-teams.** Er is minder tijd nodig voor het beheren en onderhouden van printomgevingen en voor het creëren, wijzigen en toepassen van printerbeleid, zodat teams tijd hebben voor andere initiatieven.
- **Kostenbesparingen.** De kosten voor printen zijn gedaald dankzij een betere zichtbaarheid en een ander printgedrag. Daardoor wordt bovendien bespaard op printersupplies.

Minder risico's: Betere printerbeveiliging en compliance

De ondervraagde organisaties zeiden dat zij door het gebruik van enterpriseprinterbeveiligingsoplossingen ook de gevolgen van printergerelateerde beveiligingsschendingen kunnen beperken en dat zij efficiënter en kosteneffectiever aan wet- en regelgeving kunnen voldoen.

IDC vroeg de deelnemers aan het onderzoek hoe vaak printergerelateerde beveiligings- en dataschendingen in hun bedrijf voorkomen en of daar ook ernstige, grote printergerelateerde inbreuken op de beveiliging bij waren. Gemiddeld meldden deze ondernemingen een zesvoudige afname van het aantal printergerelateerde schendingen van de beveiliging sinds de installatie van enterpriseprinterbeveiligingsoplossingen. Door encryptie van printtaken, gebruikersauthenticatie en pull-printen zijn de traceerbaarheid en de verantwoordelijkheid verbeterd. Dat is geruststellend en helpt nieuwe schendingen te voorkomen. Bovendien zijn dankzij printerbeveiliging de infrastructuurbrede beveiligingsinitiatieven van sommige organisaties versterkt en zijn bestaande lacunes

in de beveiliging gedicht. De ondervraagde bedrijven gaven voorbeelden van printergerelateerde inbreuken op de beveiliging die zij hadden meegemaakt:

- **Printen van vertrouwelijke informatie om die te misbruiken.** Een IT-directeur bij een productiebedrijf legde uit dat zijn onderneming intellectueel eigendom kwijtraakte, onder meer doordat werknemers uiterst vertrouwelijke bedrijfsinformatie hadden geprint en die aan concurrenten hadden toegespeeld.
- **Printen en onzorgvuldig behandelen van beveiligde informatie.** Een IT-directeur in een financiële instelling vertelde dat werknemers in zijn organisatie ontwerpen en ander intellectueel eigendom in gevaar brachten door deze te printen en onbeheerd op de printer achter te laten.

TABEL 2

Gevolgen van enterpriseprinterbeveiligingsoplossingen voor inbreuken op de beveiliging – diepgaande gesprekken

Totaal aantal schendingen	
Gemiddeld aantal inbreuken per jaar vóór implementatie van printerbeveiliging	9,9
Gemiddeld aantal inbreuken per jaar met printerbeveiliging	1,5
Verandering in het aantal schendingen	Tot 6 keer minder
Aanzienlijke beveiligingsinbreuken	
Aantal ondervraagde organisaties waar dat voorkwam	5
Gemiddeld aantal werknemers dat last ondervond	54
Gemiddeld aantal manuren om het probleem op te lossen	277
Gemiddelde totale kosten per schending (inclusief boetes)	$521.400

n=16 organisaties

Bron: IDC's interviews over printerbeveiliging, 2015

De ondervraagde ondernemingen gaven verschillende voorbeelden waar het gebruik van een enterpriseprintbeveiligingsoplossing had geholpen om de gevolgen van inbreuken op de beveiliging via printers in te perken:

» **Bescherming van informatie tijdens het hele printproces.** Een vicepresident informatietechnologie bij een uitgeverij zei hierover: "De oplossing is een onmisbaar hulpmiddel om de informatie- en dataworkflow van en naar onze printers in het netwerk te beschermen … waardoor de kans op schendingen aanzienlijk daalt."

» **Voorkomen van onnodig en onterecht printen.** Een IT-directeur in een instelling voor financiële dienstverlening zei: "De gevoelige documentatie die wij intern distribueren zou eigenlijk niet moeten worden geprint. Deze oplossingen helpen ons schendingen, die steeds vaker opzettelijk of door onachtzaamheid intern plaatsvinden, tot een minimum te beperken."

In tabel 2 is te zien dat weliswaar alle printergerelateerde schendingen kosten veroorzaken, maar dat ondernemingen met name grote inbreuken op de beveiliging moeten vermijden omdat de afhandeling daarvan zeer hoge kosten met zich meebrengt. Volgens de vijf ondervraagde organisaties die in de afgelopen vijf jaar te maken hadden gehad met ernstige printerschendingen, belopen de gemiddelde kosten daarvoor: productiviteitsverlies voor 54 werknemers, 277 manuren voor het afhandelen en oplossen van het probleem en ruim $500.000 aan boetes per incident.

Naast een afname van het aantal printergerelateerde schendingen van de beveiliging meldden 10 van de 16 ondervraagde bedrijven dat zij dankzij hun printerbeveiligingsoplossingen effectiever en efficiënter werden ten aanzien van compliance en audits. Betere beveiliging en traceerbaarheid bieden de volgende voordelen:

Ondervraagde ondernemingen vertelden IDC dat hun werknemers na installatie van printerbeveiligingsoplossingen gemiddeld de helft minder tijd nodig hebben om hun printeromgeving te ondersteunen.

» **Verbeterde veiligheid:** Een systeemdirecteur in een financiële instelling merkte op: "Het voornaamste voordeel van dit beveiligingsmodel is dat wij nu een uiterst robuuste en veilige omgeving hebben waarin data en documenten beschermd zijn, ontwerpen vertrouwelijk blijven en printers beveiligd zijn. Daarmee voldoen wij aan onze eigen beveiligingsstandaarden."

» **Traceerbaarheid en zichtbaarheid:** Een vicepresident informatietechnologie bij een instelling voor biowetenschappen legde uit: "Wij konden een audittraject opzetten, wij voorkomen dat data worden onderschept en kunnen aantonen dat de gebruikerstoegang tot vertrouwelijke data beperkt is. Onze verificatie- en auditprocessen omvatten identificatie van risico's en analyse van bedreigingen, plus aanbevolen oplossingen voor problemen. Wij krijgen een diepgaand inzicht in de systeemstatus en kunnen deze in real-time bewaken – allemaal voorwaarden voor

compliance."

Deze verbeteringen leiden ook tot tijd- en kostenbesparingen bij de compliance- en auditactiviteiten van de organisaties. Gemiddeld meenden de ondervraagde bedrijven dat het gebruik van printerbeveiligingsoplossingen hen meer dan 200 werkuren per jaar en bijna $250.000 per jaar aan kosten bespaart, met inbegrip van de kosten van externe partijen voor ondersteuning van audits en compliance.

Hogere productiviteit bij IT-teams

Door IDC ondervraagde ondernemingen zeggen dat zij na installatie van printerbeveiligingsoplossingen minder tijd kwijt zijn aan het beheren en ondersteunen van hun printeromgeving. De efficiëntieverbetering is onder andere te danken aan de introductie of uitbreiding van centrale beheerfunctionaliteit en automatisering en aan het feit dat zij printerproblemen sneller kunnen oplossen. Een senior IT-directeur in een instelling voor financiële dienstverlening zei: "Wij zijn (dankzij onze printerbeveiligingsoplossingen) minder tijd kwijt aan arbeidsintensieve printertaken en ons team kan aan strategische activiteiten werken. De aanpak van printerproblemen is niet langer heterogeen, maar holistisch en herhaalbaar." Ondervraagde ondernemingen vertelden IDC dat hun werknemers na installatie van printerbeveiligingsoplossingen gemiddeld de helft minder tijd nodig hebben om hun printeromgeving te ondersteunen.

Ze merken dat de medewerkers die verantwoordelijk zijn voor hun printeromgeving efficiënter werken dankzij de printerbeveiligingsoplossingen. Tijdbesparing is het gevolg van veranderingen zoals automatisering van ondersteuning en onderhoud, automatisering van certificaten en toepassing van andere herhaalbare processen. Een vicepresident van een financiële dienstverlener waar unieke certificaten en werknemersverificatie worden toegepast, legde bijvoorbeeld uit hoe in zijn organisatie 60% minder tijd wordt besteed aan apparatuurbewaking: "Ons IT-team bespaart tijd omdat profielen gemakkelijk kunnen worden gemaakt en naar veel apparaten tegelijk worden gestuurd nu het certificatenbeheer automatisch verloopt."

Bovendien bespaarden de ondervraagde ondernemingen dankzij printerbeveiligingsoplossingen tijd bij het maken, toepassen en veranderen van printerbeleid. Gemiddeld besteedden werknemers in deze bedrijven 59% minder tijd aan printergerelateerd beleid. Een effectievere implementatie van printerbeleid bespaart niet alleen op arbeid maar vermindert ook de kans op schendingen en maakt het mogelijk heldere richtlijnen voor printergebruik te hanteren.

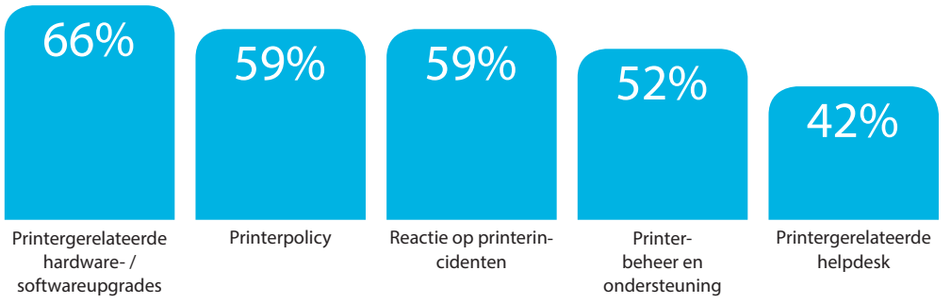
De ondervraagden zeggen dat hun medewerkers bij printerproblemen veel voordeel

Printerbeveiligingsinitiatieven hebben werknemers meer bewust gemaakt hoe zij printers gebruiken en hoe ze kunnen bijdragen aan het besparen op printkosten.

hebben van de printerbeveiligingsoplossingen dankzij (beter gebruik van) centrale consoles en remote toegang tot printers. Daardoor, en door een beter printerbeleid, besteden bedrijven gemiddeld respectievelijk 59% en 42% minder tijd aan het afhandelen van printerincidenten en printergerelateerde hulpvragen van gebruikers (zie Afbeelding 1). Een vicepresident IT bij een uitgeverij die beveiligingsoplossingen met zelfherstelmogelijkheden gebruikte en waar unieke certificaten werden beheerd vertelde dat zijn team printers gemakkelijker kan ondersteunen: "Er zijn nu minder problemen en de problemen die optreden zijn gemakkelijker te verhelpen. Het positieve gevolg is dat er meer tijd overblijft voor andere ondersteunings- en planningsactiviteiten." Een IT-directeur in een financiële instelling waar een printerbeveiligingsbeheerproduct wordt gebruikt, merkte op: "Onze helpdesk heeft nu een duidelijk overzicht van de printerinstellingen, gebruiksrechten en problemen en kan zelf in actie komen of contact opnemen met een klein bedrijfsteam voor Level 2 support."

Afbeelding 1

Gemiddelde tijdbesparing van printerteams – uitvoerige gesprekken



n=16 organisaties

Bron: IDC's interviews over printerbeveiliging, 2015

Printergerelateerde kostenbesparingen

Elk IT-initiatief is extra aantrekkelijk als het kostenbesparingen oplevert. Daardoor waren de kostenbesparingen die bedrijven bereikten door installatie van printerbeveiligingsoplossingen een aanzienlijke bonus. Authenticatie van werknemers en pull-printing werden het meest toegepast door de ondervraagde bedrijven (meer dan tweederde van de geïnterviewden maakt er gebruik van). Deze oplossingen zorgen dat documenten vertrouwelijk blijven en dat de kosten dalen doordat printergebruikers specifieke stappen moeten nemen om hun documenten te printen en doordat minder prints op de verkeerde plek terechtkomen of niet worden opgehaald. Het is duidelijk dat printerbeveiligingsoplossingen bijdragen aan het terugdringen van de printkosten:

verschillende ondervraagden noemden kostenoptimalisatie als primaire drijfveer voor hun gebruik van printerbeveiligingsoplossingen.

Ze legden uit dat printerbeveiligingsoplossingen hen als volgt helpen om de kosten te reduceren:

- **Minder printen door veranderd printgedrag:** Een vermogensbeheerder bij een bedrijf in de levensmiddelensector zei: "De pull-printingfunctie die wij gebruiken maakt het mogelijk een document naar de printer te sturen; maar om het daadwerkelijk te printen moeten mensen naar de printer toelopen en hun badge op de printer leggen. Uit de nieuwste cijfers blijkt dat wij daardoor ongeveer 21% tot 24% minder prints maken dan vroeger."

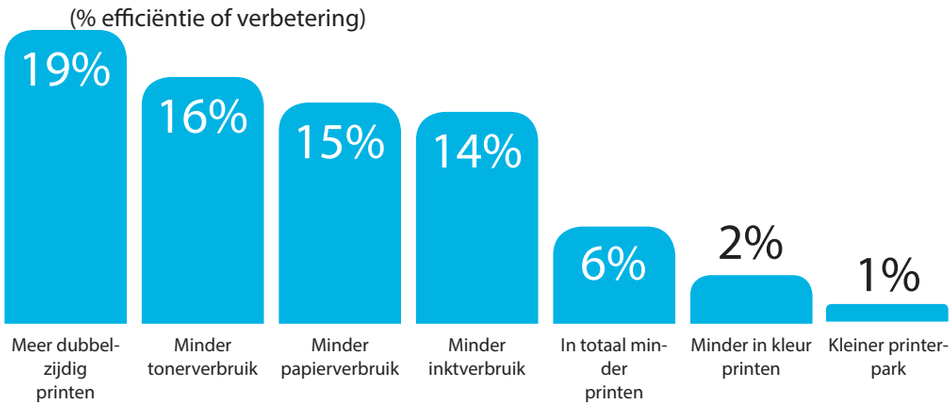
- **Meer inzicht in het printergebruik:** Een IT-directeur van een universiteit zei: "We kunnen nu het aantal afgedrukte pagina's traceren en de kosten doorbelasten aan afzonderlijke afdelingen." Doordat de printkosten per afdeling worden gedeclareerd, kan de universiteit elke afdeling onder druk zetten om te zorgen dat hun gebruikers zo efficiënt mogelijk printen.

- **Buiten gebruik stellen van overbodige en verouderde printers:** Een vicepresident van een financiële instelling vertelde: "Er worden minder onnodige prints gemaakt omdat de mensen weten dat de printeractiviteit wordt gecontroleerd en wij vervangen oudere printerhardware die het enterpriseprintbeveiligingsbeleid niet ondersteunt."

Printerbeveiligingsinitiatieven hebben werknemers meer bewust gemaakt hoe zij printers gebruiken en hoe ze kunnen bijdragen aan het besparen op printkosten. Gemiddeld zeiden de deelnemers die uitvoerig werden ondervraagd dat hun werknemers 43% minder printtaken naar de verkeerde printers sturen. Daardoor worden minder prints niet opgehaald of opnieuw afgedrukt. Zoals Afbeelding 2 laat zien, dragen deze verbeteringen bij aan een efficiënter algeheel printergebruik en aan een afname (gemiddeld 6%) van het totaal aantal gemaakte prints. Verder wordt er vaker dubbelzijdig geprint (19%) en iets minder in kleur (2% daling). Dankzij deze factoren en het betere inzicht in de printeromgeving bespaarden bedrijven aanzienlijk op de kosten van hun printomgeving, hoefden zij minder printers te installeren en te onderhouden (1% minder of gemiddeld 115 printers per organisatie) en bespaarden zij op de kosten voor papier, inkt en toner (respectievelijk 15%, 14% en 16%).

Afbeelding 2

Gemiddelde kostenbesparingen en efficiëntieverbetering in de printomgeving – uitvoerige gesprekken



n=16 organisaties

Bron: IDC's interviews over printerbeveiliging, 2015

Uitdagingen

IDC adviseert bedrijven hun print/ document beveiligingstechnologie waterdicht te maken.

Bij vrijwel iedere uitrol kunnen door een goede planning problemen worden vermeden. In de onderzochte groep traden problemen op in elk van de drie fasen van de printbeveiligingsuitrol: planning, implementatie en post-implementatie.

De ondervraagde bedrijven stonden onder zware tijdsdruk bij het ontwikkelen van de strategie en de planning. Van tevoren is voldoende tijd nodig, wil men na de implementatie de gewenste verlichting van de werklast voor IT bereiken. Bovendien moet het afdwingen van werknemerscompliance een automatisch proces zijn dat bewakingstools, een escalatieprocedure en herstel omvat om het aantal printgerelateerde helpdeskvragen te verminderen.

Wat betreft de printergebruikers in een onderneming moet u twee voorzorgsmaatregelen treffen:

» **De juiste printbeveiliging installeren met zo min mogelijk productiviteitsverlies voor het personeel:** Beveiliging heeft de hoogste prioriteit, maar bedrijven moeten een systeem bedenken dat zo weinig mogelijk impact heeft op de productiviteit. Sommige bedrijven die pull-printing installeren om hun prints beter te beveiligen, stuiten op weerstand vanwege de verplichte authenticatie (bijvoorbeeld door een wachtwoord in te voeren), waarna men moet wachten tot het hele document is afgedrukt. Er moet een afweging worden gemaakt tussen de bescherming van de informatie in het document (niemand kan documenten lezen die onbeheerd op de printer liggen) en wachten tot een document gereed is (het printen begint pas nadat de gebruiker op het apparaat is geverifieerd).

» **Training van werknemers:** Om de productiviteit van werknemers te waarborgen moet in het printbeveiligingsplan ook tijd worden gereserveerd voor het trainen van werknemers in nieuw beleid en nieuwe procedures. Bedrijven moeten bereid zijn om herhaald training te geven en training op verschillende manieren aan te bieden die afgestemd zijn op verschillen in leerstijl tussen werknemers.

Essentiële roadmaps

IDC heeft een aantal goede argumenten om printers en documentworkflows op te nemen in een bedrijfsbrede IT-beveiligingstructuur. Uiteraard is het voornaamste voordeel de beschikbaarheid van een alomvattend IT- beveiligingsprogramma waarin ook printen is opgenomen. Een dergelijk programma heeft echter naast veiligheid nog andere voordelen. De twee belangrijkste zijn forse kostenbesparingen en een efficiëntere IT.

IDC adviseert bedrijven hun print/documentbeveiligingstechnologie waterdicht te maken. De onderneming moet beseffen dat dit doel alleen effectief wordt bereikt wanneer mensen en processen bij de uitvoering van het plan worden betrokken.

Technologie

Ten aanzien van beveiliging is de implementatie van technologieoplossingen in feite een zwart-witkwestie … een organisatie is veilig of niet.

IDC adviseert zo spoedig mogelijk de volgende functionaliteit in de hele organisatie te installeren. IT-personeel en leveranciers van printinfrastructuur dienen de volgende functies en mogelijkheden voor alle printapparaten in de hele organisatie te configureren en te activeren:

» Alle netwerkprinters moeten de volgende kenmerken bevatten of tenminste een firmwareupgrade ondergaan die deze ondersteunt.

» Zorgen dat alle apparaten alleen versleutelde communicatieprotocollen gebruiken en de rest uitschakelen.

» Een systeem installeren dat de gegevens van de opslagschijf in het apparaat wist of vernietigt wanneer het apparaat wordt afgedankt.

» Mimimaal één vorm van gebruikersauthenticatie ondersteunen (liever twee of drie) en de implementatie van pull-printing overwegen in omgevingen waar veel vertrouwelijke documenten zijn of compliancevereisten gelden.

» Zorgen dat altijd de nieuwste firmware geïnstalleerd is en dat uitsluitend legitieme firmware wordt geladen.

» Alle opslagschijven in printers beveiligen (data versleutelen en regelmatig wissen).

» Maatregelen nemen om misbruik te voorkomen of afsluitbare papierladen gebruiken voor speciale media indien daarmee wordt gewerkt. Zo worden prints die een mogelijk doelwit vormen voor fraude, zoals cheques, receptenpapier en dergelijke beschermd.

» Printerparkbeheersoftware gebruiken om apparaten centraal te beheren, te bewaken en te herstellen en te waarborgen dat aan het beveiligingsbeleid wordt voldaan. De onderneming hoeft dan niet elk apparaat apart te configureren en te onderhouden. De tool moet het mogelijk maken eenvoudig beveiligingsbeleid te creëren en te beheren, te detecteren wanneer apparaten aan het netwerk worden toegevoegd, uniek apparaatcertificatenbeheer te bieden, ongebruikelijk incidenten te registreren en deze op te lossen via een escalatie- en herstelproces. De tool moet samenwerken met enterprisebrede IT-beveiligingsbeheertools die endpoints bewaken om incidenten en afwijkingen op te sporen, zodat potentiële schendingen van de beveiliging snel worden gesignaleerd.

» Zorgen dat zowel prints als scans van mobiele en desktopapparaten (tijdens

IDC wereldwijd hoofdkantoor

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

Informatie over IDC

International Data Corporation (IDC) is de belangrijkste wereldwijde leverancier van marktkennis, adviesservices en evenementen voor de informatietechnologie-, telecommunicatie- en consumententechnologiemarkt. IDC helpt IT-professionals, bedrijfsdirecties en investeerders gefundeerde beslissingen te nemen over technologieaankopen en bedrijfsstrategie. Meer dan 1100 analisten van IDC in meer dan 110 landen in de hele wereld bieden wereldwijde, regionale en lokale expertise over technologie- en industrietrends en kansen. IDC levert al 50 jaar strategische inzichten om haar klanten te helpen hun bedrijfsdoelstellingen te halen. IDC is een dochteronderneming van IDG, het grootste technologiemedia-, onderzoeks- en evenementenbedrijf ter wereld.

IDC Analyze the Future

verzendingen of in rust) versleuteld zijn om printdata goed te beschermen. Dit betekent dat ook bijlagen die worden afgedrukt moeten worden geopend en als extra bescherming in afbeeldingen moeten worden omgezet. Een programma dat de inhoud van prints en scans bewaakt is een essentieel element om het hoogste beveiligingsniveau te waarborgen en zich te houden aan het bedrijfsbeleid en industriestandaarden.

Mensen

Een bedrijf dat zijn IT-beveiliging serieus neemt, moet een beveiligingsteam samenstellen met mensen die veel ervaring hebben in het beveiligen van printapparatuur en de bijbehorende documentworkflows. Het beveiligingsteam kan bestaan uit interne medewerkers en/of deskundige externe beveiligingsexperts. Het team wordt gevraagd om te adviseren over toekomstige print- en workflowbeveiligingsproblemen en te helpen bij de integratie van een enterprisebreed IT-beveiligingsplan.

Om te voorkomen dat de beveiliging van printapparaten en de bijbehorende documentworkflows negatieve invloed heeft op de productiviteit, moet de onderneming in het kader van het planningsproces ook de mening vragen van geselecteerde werknemers uit alle geledingen van de organisatie. Het verdient daarnaast aanbeveling om een expert in veranderingsbeheer in te schakelen, met name als er veel of ingrijpende veranderingen nodig zijn. Deze expert kan ook advies geven over het uitrollen en opzetten van het trainingsprogramma.

De meeste bedrijven beschikken niet over de noodzakelijke kennis en vaardigheden om zelf hun print- en documentinfrastructuur te beveiligen. Daarom moeten zij bij de printerleverancier informeren welke resources de IT-afdeling kan benutten. Het gaat daarbij om de beveiligingskenmerken die beschikbaar zijn in de printer-/MFP-hardware van de organisatie, beveiligingssoftware en beveiligingsservices (bijvoorbeeld professionele beveiligingsservices, beveiligingsevaluaties, veranderingsbeheer en expertise inzake compliance voor specifieke bedrijfstakken).

Proces

Het is belangrijk om een beveiligingsproject te starten met een evaluatie van de huidige printomgeving en vervolgens een plan te ontwikkelen om een beveiligingsniveau te creëren dat aansluit bij de rest van de IT-omgeving. Men moet een goed inzicht krijgen in de specifieke beveiligingsvereisten van de eigen bedrijfstak en een plan opstellen voor het bewaken, escaleren, herstellen en handhaven van het ingestelde beleid.

Het plan dient regelmatig te worden herzien aan de hand van in de voorafgaande periode

verzamelde gegevens om te bepalen of aanpassingen nodig zijn en om te leren van print/documentschendingen bij ander bedrijven. Eventuele aanpassingen worden gebaseerd op de verzamelde gegevens en passen bij het voor de onderneming aanvaardbare risiconiveau en de bestedingsruimte.