Whitepaper Informatiebeveiliging

Outputbeveiliging

Bescherming van geprinte en elektronische output

www.sharp.nl | www.sharp.be

SHARP
Be Original.

Inhoud

Introductie

De behoefte om de fysieke of elektronische output van MFP's en printers te beschermen, is een onderdeel van informatiebeveiliging dat vaak vergeten wordt.

Sharp definieert outputbeveiliging als beveiliging die gerelateerd is aan zowel print- als elektronische output van multifunctionele printers (MFP's) of printers. Deze categorie omvat alle geprinte documenten en elektronische afbeeldingen of informatie die worden verstuurd van een pc naar een multifunctionele printer (MFP) of printer (inclusief printen via speciaal aangewezen printservers), scanner (inclusief scan-to-folder, scan-to-email, scan-to-cloud en scan-to-HDD) en faxmodule.

In dit whitepaper beschrijven we verschillende punten.

- **De achtergrond**
  Beschrijft waarom outputmanagement een vaak vergeten onderdeel van informatiebeveiliging is. En we gaan in op de mogelijke kwetsbaarheden die iedere IT-beheerder moet kennen, zoals:
  - het groeiende aantal organisaties dat hun MFP-/-printerparken consolideert;
  - het groeiende aantal gebruikers, die allemaal moeten worden geïdentificeerd en beheerd;
  - het groeiende aantal geproduceerde documenten en de behoefte om deze te reguleren;
  - het gebrek aan tools om alle outputactiviteiten te volgen en vast te leggen in rapportages.

- **Het probleem**
  Onderzoekt de outputmanagementuitdagingen waar IT-beheerders, eindgebruikers en het management binnen bedrijven mee te maken krijgen. Hieronder vallen het beheren van gebruikerstoegang tot afgedrukte documenten, het volgen van de gebruikersactiviteiten, het rapporteren over activiteiten, het printen via mobiele apparaten, en het scannen van documenten naar meerdere locaties en faxen van documenten naar bestemmingen buiten de organisatie.

  Ook gaat dit onderdeel in op dataonderzoek dat de complexiteit van dit onderwerp aantoont, alsook de schaal van het probleem.

- **De oplossing**
  Beschrijft een serie Sharp-producten (softwareoplossingen) en best practices die u kunnen helpen een veilige outputomgeving op te bouwen en ongeautoriseerde toegang te voorkomen tot MFP's en printers en de documenten (inclusief elektronische afbeeldingen), kopieën, faxen, scans en prints die zij produceren en opslaan.

  Dit onderdeel onderzoekt hoe Sharp problemen kan oplossen door u te helpen met;
  - het selecteren van de oplossing die aansluit op uw eisen en u helpt een goed printbeveilingsbeleid te creëren. Een outputmanagementsysteem beheert de toegang, past printregels toe, beperkt de functionaliteiten, volgt alle outputdocumenten en legt deze activiteiten vast voor eventuele rapportages.
  - het selecteren van de juiste oplossingsleverancier voor uw outputmanagement en gerelateerde outputactiviteiten.

- **De conclusie**

  Biedt een samenvatting van het onderwerp, inclusief:

  - De belangrijkste zakelijke kwetsbaarheden die ontstaan bij elke documentoutput.
  - Een samenvatting van aanbevelingen gebaseerd op de Sharp-beveiligingsoplossingen.
  - De stappen die nodig zijn om een consistent printbeveiligingsbeleid te creëren, inclusief betrouwbare tools die zijn toe te passen op alle aspecten van uw bedrijf.

Achtergrond

Wanneer bedrijven hun potentiële beveiligingsrisico's inventariseren, zien ze met het netwerk verbonden MFP's en printers (bijna) nooit als probleem – laat staan geprinte documenten.

Volgens onderzoeksbureau Quocirca heeft 60 procent van de organisaties tenminste één datalek ervaren als gevolg van niet-beveiligde printpraktijken. Dit is een serieuze bedreiging voor kleine én grote bedrijven (1). Maar zelfs als u maatregelen neemt om uw data te beschermen tegen geavanceerde hackers of cybercriminelen is dat niet altijd voldoende.

Als gevoelige documenten te lang bij een MFP/printer blijven liggen, kan iedereen ze in handen krijgen en de informatie voor eigen gewin gebruiken. Dit kan leiden tot serieuze problemen en komt vaker voor dan u denkt.

56% van de bedrijven negeren printers in hun endpoint-beveiligingsstrategie

Probeer u te verplaatsen in een potentiële dief: de uitvoerlade is het eenvoudigste doelwit voor het stelen van vertrouwelijke informatie. Een vaak onderschatte uitdaging voor IT-beheerders is dan ook om ervoor te zorgen dat geprinte documenten niet bovenop een MFP of printer blijven liggen, waar ze in verkeerde handen zouden kunnen vallen.

Maar de outputbeveiligingsuitdagingen waar elke moderne organisatie mee te maken krijgt worden met de dag groter. En om verschillende redenen.

1. Groeiend aantal apparaten
Het aantal organisaties dat hun MFP's en printers consolideert, groeit. Daarnaast streven ze naar standaardisering. Dit brengt verschillende uitdagingen met zich mee, vanwege het gebrek aan tools om de functionaliteiten, output en beveiliging (als onderdeel van het netwerk) van de MFP en printer te beheren.

2. Aantal verbonden gebruikers
Sommige bedrijven hebben een grote hoeveelheid medewerkers, waardoor honderden gebruikers printen op tien, soms meer dan honderd apparaten. Voeg daaraan het toenemende aantal beveiligings-verordeningen, zoals de AVG, aan toe, en de uitdagingen worden steeds groter op het gebied van:

- Gebruikersauthenticatie;
- Beheren van gebruikersaccounts (inclusief het reguleren van het aantal verbonden gebruikers)
- Integreren van gebruikers met bestaande kantoorsystemen
- De beperkingen omtrent hoe organisaties gebruiksdata in hun systemen kunnen beheren, zoals het verwijderen van gebruikersdata voor compliance met de AVG.

3. Aantal te reguleren geprinte documenten

Het alsmaar stijgende aantal gebruikers en het gemiddeld aantal geprinte pagina's per gebruiker wijzen erop dat er een groot aantal outputdocumenten moet worden gereguleerd, waaronder:

- Gekopieerde documenten
- Geprinte documenten
- Gescande documenten
- Gefaxte documenten

4. Gebrek aan beheertools
Er bestaat over het algemeen een gebrek aan tools die alle output nauwkeurig kunnen volgen en vastleggen.

Probleem

Outputbeveiliging moet worden erkend als één van de kernfocuspunten binnen elk modern bedrijf dat MFP's en printers gebruikt.

De juiste tools bieden

Onderzoekanalisten benadrukken de behoefte om voldoende tools en maatregelen te implementeren. Op die manier is het mogelijk meerdere gebruikers te bedienen en om te gaan met meerdere printbestanden, op meerdere printapparaten.

De outputtoegang beveiligen

De uitdaging voor iedere IT-beheerder is het omgaan met meerdere accounts en gebruikers die geregistreerd zijn op het bedrijfsnetwerk. Het aantal gebruikers beïnvloedt namelijk hun werkomvang. Ook compliceert een groot aantal gebruikers het gebruikersbeheerproces en alle output gerelateerde gebruikersactiviteiten, zoals kopiëren, printen, scannen en faxen. De vraag is dus: hoe gaat een IT-beheerder zo effectief mogelijk om met outputbeveiliging?

Sommige van de meest populaire technieken, zoals pincodes, log-ins en wachtwoorden, pasjes en toegangsbadges zijn effectief in het beveiligen van de documentoutput. Maar ze kunnen een IT-beheerder ook nachtmerries bezorgen als ze foutief geïnstalleerd zijn en verkeerd beheerd worden. Met name omdat veel IT-beheerders ook apparaten en hun output willen verbinden met bestaande systemen, zoals Microsoft-accounts.

Aantal documenten en achtergelaten prints

Het toenemende aantal prints vormt een serieuze uitdaging. Hieronder vallen zowel traditionele papieren documenten die op de apparaten zijn geprint of gekopieerd, als elektronische documenten die naar MFP's/printers zijn verstuurd via het zakelijke netwerk of via scan- en faxfuncties.

Nieuwe voorschriften, zoals de AVG, roepen daarnaast vragen op over hoe onbeheerde prints te beschermen en hoe goed beveiligd de persoonlijke gegevens die in de bovengenoemde outputcommunicatie staan nu eigenlijk zijn.

De risico's begrijpen

Om effectieve bescherming te bieden, is het zaak om de risico's die verschillende activiteiten met zich mee brengen volledig te begrijpen.

- **Kopiëren**
  Kopiëren was in de jaren tachtig en negentig de populairste manier om documenten te delen, maar is door printen van de troon gestoten. Toch is kopiëren nog een belangrijk gebied om te beheren via outputmanagementsystemen, met name in het geval van

- **Printen**
  Printen is een veelvoorkomende hedendaagse manier om bedrijfsdocumenten te verspreiden. Er doen zich echter talloze risico's voor als printen niet goed of centraal wordt beheerd.

  - Niet-beveiligde en ongecontroleerde toegang tot MFP's en printers, alsook de apparaatfuncties en -features, zoals de harde schijven.
  - Onbeperkt toegang tot geprinte documentatie, waardoor alle kantoorgebruikers / medewerkers (en mogelijk bezoekers) toegang hebben.
  - Geen mogelijkheid om gebruikersactiviteiten te volgen en vast te leggen, zoals wie wat heeft geprint en op welk tijdstip.
  - Geen mogelijkheid om gebruikersdatalekken te monitoren en voorkomen, wat kan leiden tot hoge boetes vanwege strenge beveiligingsverordeningen, zoals de AVG.
  - Geen mogelijkheid om mobiele gebruikers en printopdrachten te volgen van mobiele apparaten, zoals smartphones en tablets.

- **Scannen**
  Scannen kan het beveiligingsproces compliceren, omdat documenten niet alleen naar netwerkmappen en e-mails gescand kunnen worden, maar ook naar externe clouddiensten. Ook bestaan er risico's op het gebied van:

  - Scannen van bedrijfsgevoelige documenten naar externe locaties, zoals scannen naar privémailadressen in plaats van zakelijke mailadressen.
  - Scannen naar meerdere mappen in plaats van naar geselecteerde privébedrijfsmappen of netwerkmappen zonder een documentlocatie- en structuur die door de IT-beheerder is goedgekeurd.
  - Scannen zonder indexering, wat kan leiden tot grote problemen bij het opzoeken en auditen van gescande documenten en scan gerelateerde activiteiten (scanoutput en -locaties).

- **Faxen**
  Ook faxen kan een zwak punt zijn in de outputbeveiligingsstrategie van een bedrijf. Gefaxte documenten worden blootgesteld aan hetzelfde niveau van beveiligingslekken als gescande documenten, ongeacht de overdrachtsmethode (analoog faxen of faxen via e-mail).

- **Mobiel printen – Bring Your Own Device (BYOD)**
  Mobiliteit wordt door veel onderzoeksbureaus gezien als een van de belangrijkste printmethoden van de toekomst. Maar ook deze methode zorgt voor uitdagingen, bijvoorbeeld omtrent de integratie van mobiele-printoplossingen in een moderne organisatie, of het volgen en beheren van de activiteiten van mobiele gebruikers. Daarnaast is het de vraag hoe een mobiele-printstrategie past in de overkoepelende strategie van een organisatie. Helaas zien veel bedrijven niet in dat medewerkersmobiliteit een groeiende trend is, of een must-have voor een organisatie. De behoefte aan outputbeveiliging wordt dan ook vaak over het hoofd gezien.

- **Volgen en rapporteren**
  Een groot probleem voor bedrijven is niet alleen hoe veilig hun document-outputkanalen zijn, maar ook hoe ze al hun outputinformatie kunnen volgen en vastleggen.

  Het is daarnaast van belang dat het auditrapport juist en beveiligd is:

  - Wie heeft toegang?
  - Is de data juist?
  - Is de data te bewerken?
  - Wie beheert het systeem?

Aanbevelingen

Het is belangrijk om te begrijpen dat outputbeveiliging slechts één van de vele elementen is in kantoorbeveiliging. De elementen kunnen per organisatie verschillen.

Sommige bedrijven zijn van mening dat het voldoende is om hun netwerkbeveiligingsmaatregelen serieus te nemen en nauwkeurig te implementeren. Maar wanneer het bedrijf groeit, groeit ook het aantal documenten dat geproduceerd wordt – net als de bijbehorende beveiligingsuitdagingen.

Die groei vraagt om een bredere beveiligingsaanpak, waarbij niet alleen het netwerk wordt beveiligd, maar ook alle outputinformatie en de documenten die buiten de organisatie worden gegenereerd en gedeeld.

Met andere woorden: de beveiliging van een netwerk en de daarmee verbonden periferieën is essentieel. Outputbeveiliging is een logische stap om uw netwerkbeveiliging te vergroten. Niet alleen voor grote organisaties, maar ook voor snelgroeiende mkb-bedrijven.

Het gebruik van outputmanagement-/printmanagementoplossingen, zoals een van de Optimised Printing- of Optimised Scanning-oplossingen van Sharp, helpt u om al uw kantooroutput te beveiligen, uw apparaten met bestaande systemen te integreren en snel een consistent print- en scanbeveiligingsbeleid te introduceren.

De belangrijkste factor van outputbeveiliging is controle. Alles wat u kunt controleren, kunt u ook meten en vervolgens beveiligen. Onze systemen geven u volledige controle over elk outputdocument en alle informatie: kopie, print, scan en fax.

Dankzij de naadloze integratie met uw bestaande printervloot bespaart outputmanagement u een hoop tijd. Zo is het importeren van alle gebruikers via Lightweight Directory Access Protocol (LDAP) snel een eenvoudig. Iedereen kan binnen enkele seconden worden toegevoegd, geïdentificeerd en geïntegreerd met het systeem. Daarnaast worden alle gebruikersgegevens verzonden via Transport Layer Security (TLS) om te voorkomen dat ze worden onderschept.

De echte waarde van dit outputmanagementsysteem zit hem echter in de geavanceerde features die het leven van de IT-beheerder en de eindgebruiker een stuk gemakkelijker maken.

- **Gebruikersauthenticatie**
  De belangrijkste factor in de toegang tot een outputmanagementsysteem. De software biedt u meerdere mogelijkheden om de gebruiker te identificeren en toegang te geven tot de verbonden apparaten. De snelste en populairste optie zijn toegangspassen en -badges. Een pas of badge is gekoppeld aan de gegevens van een gebruiker, en de authenticatie vindt plaats met behulp van de kaartlezer op het apparaat. IT-beheerders kunnen ook kiezen uit alternatieve authenticatiemethodes, zoals pincodes, gebruikerslogin- en wachtwoord en biometrische scanners.

  Ook is het mogelijk om gebruik te maken van bestaande pasjes binnen uw bedrijf, die toegang bieden tot gebouwen, bepaalde afdelingen of beveiligde ruimten. Er bestaan meerdere kaart- en kaartlezerstandaarden die gebruikmaken van verschillende communicatiemethoden en -frequenties. We adviseren u dan ook om contact op te nemen met onze Solutions Consultants om erachter te komen welk systeem het best bij uw bedrijf past.

- **Beveiligde printwachtrij**
  Wanneer een document op de normale wijze via een pc of laptop naar de printer wordt verstuurd, begint de communicatie tussen de driver op de pc en het outputmanagement. Alleen geregistreerde gebruikers kunnen het systeem gebruiken en enkel via gelicenseerde apparaten die zijn geconfigureerd met de benodigde software. De gebruiker stuurt de opdracht naar de outputmanagementserver. Wanneer de gebruiker inlogt op het apparaat (met een smart card, pincode of

gebruikerslogin en -wachtwoord), identificeert het systeem hem of haar als geregistreerde gebruiker met printbevoegdheden.

- **Pull-print-functionaliteit**
  De mogelijkheid voor een beveiligde wachtrij en opdrachtopslag op een server biedt nog een belangrijk voordeel, namelijk de 'pull-print'-functionaliteit (beter bekend als follow-me-printen). De gebruiker kan daarmee printen vanaf elk apparaat binnen het bedrijf, zolang het maar verbonden is met hetzelfde netwerk. Of vanaf elke locatie waar het outputmanagementsysteem is geïnstalleerd. Deze functionaliteit leidt daarnaast tot minder printgerelateerde downtime. Als een van de printapparaten niet werkt of in onderhoud is, loopt u simpelweg naar het dichtstbijzijnde apparaat en print u daar uw documenten.

- **Automatische opdrachtdetectie**
  Nog een uitdaging voor IT-beheerders is het grote aantal pagina's dat tijdelijk staat opgeslagen, wachtend op output of indexering. Die uitdaging wordt weggenomen met outputmanagement.

  Dankzij een automatische opdrachtverwijderfunctie kunnen IT-beheerders een bewaarbeleid instellen voor de documenten. Als er bijvoorbeeld om 8 uur 's ochtends een printopdracht is aangemaakt, maar het document niet binnen 24 uur wordt geprint, wordt het automatisch verwijderd uit de wachtrij. Deze functionaliteit is naar eigen inzicht in te stellen, afhankelijk van de behoefte van de organisatie.

84% van de organisaties ziet tussen nu en 2025 beveiliging als prioriteit. Beveiligingsexpertise wordt voor 58% van de organisaties de belangrijkste eis bij het selecteren van een leverancier (3)*.*

- **Elimineren van dubbele printopdrachten**
  Nog een voordeel van outputmanagementoplossingen is het elimineren van dubbele printopdrachten. Na te hebben ingelogd op het gekozen apparaat, zien gebruikers de lijst met bestanden die ze hebben doorgestuurd. Ze zien eenvoudig of de documenten meerdere keren zijn verstuurd en bepalen welke documenten moeten worden geprint of verwijderd. Daarnaast kunnen gebruikers documenten printen en verwijderen uit de wachtrij, of ze printen en in de wachtrij laten staan.

- **Beveiligd scannen, faxen en kopiëren**
  Outputmanagement geeft u controle over alle functionaliteiten van het apparaat. De kopieer-, scan- en faxactiviteiten worden beheerd via dezelfde gebruikerstoegang. Zo zijn alle activiteiten eenvoudig te monitoren. Daarnaast:

- maken Sharp-apparaten gebruik van het TLS-protocol voor SMTP en S/MIME-e-mailversleuteling voor beveiligde e-mailcommunicatie;
- is het LAN-netwerkinterfacecomponent van de MFP-controller volledig geïsoleerd van de Fax PSTN-telefoonlijn. Dit voorkomt dat aanvallers toegang krijgen tot de interne systemen van de MFP of het lokale netwerk.

- **Volgen en vastleggen**
  Voor veel organisaties zijn volgen en vastleggen de belangrijkste factoren. Met een outputmanagementsysteem worden alle activiteiten gevolgd. Of u nu print, scant, kopieert of faxt, alle opdrachten worden opgeslagen in het systeem. Gedetailleerde rapportages hiervan zijn te genereren op basis van uw persoonlijke account, afdeling of specifieke factureringsoptie.

- **Verwijderen van gebruikersdata voor de AVG**
  In artikel 17 van de AVG staan gedetailleerde instructies over de omgang met persoonsgegevens. Inclusief "het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen." Met het outputmanagementsysteem van Sharp is dit geen enkel probleem. Hiermee bewerkt u eenvoudig alle gebruikersgegevens en

voldoet u aan deze strikte regelgeving. En zelfs als de gebruikersdata is verwijderd kunnen IT-beheerders nog verschillende printinzichten en -statistieken raadplegen om gebruiksrapportages te genereren.

- **Mobiel printen**
  Dit is een eenvoudig concept: gebruikers kunnen net als normaal printen met hun eigen smartphone of tablet (Bring Your Own Device). IT-beheerders bepalen welke applicatie het best past bij de organisatie. De Optimised Mobile-applicatie van Sharp is dankzij zijn uitgebreide configuratie te koppelen aan de outputmanagementsoftware. Op die manier worden alle via mobiele apparaten geprinte documenten vastgelegd in het systeem en is deze informatie te gebruiken voor statistieken en rapportages. Bovendien kunnen documenten geprint vanaf mobiele apparaten niet onbeheerd op de uitvoer van een multifunctionele printer komen te liggen.

Nog robuustere beveiliging

Outputbeveiliging speelt een grote rol in het definiëren, creëren en implementeren van uw eigen printbeveiligingsbeleid.

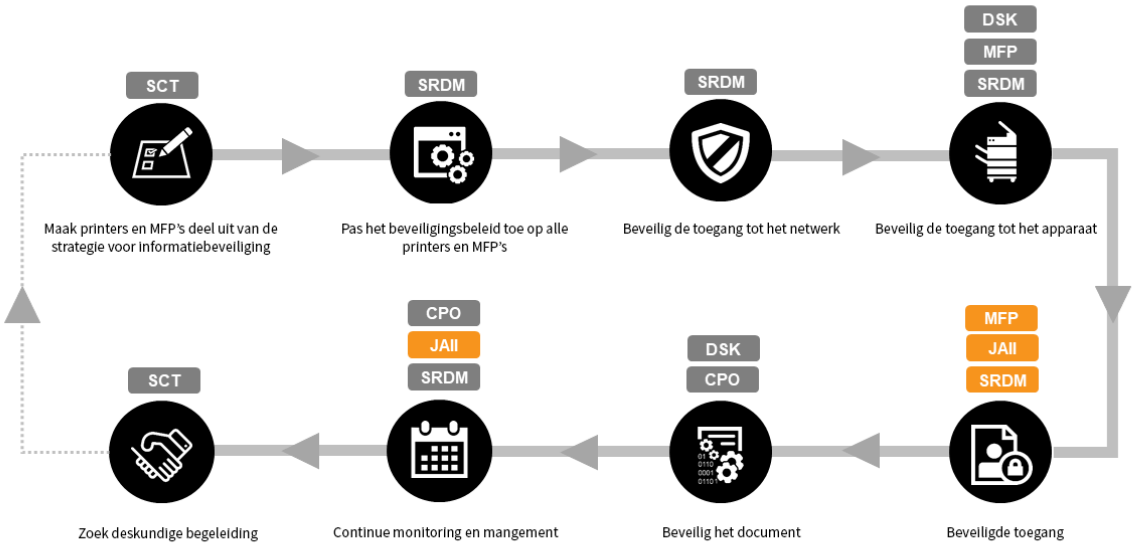
- Outputmanagementproducten uit het Optimised-portfolio van Sharp zijn zeer waardevol bij het opnemen van zo'n beleid, omdat ze zaken als 'toegang geven' en 'continue monitoring en beheer' verbeteren.

- Door meer producten uit ons portfolio toe te voegen, zoals Sharp-MFP's, Data Security Kit (DSK), Sharp Remote Device Manager (SRDM) en Cloud Portal Office (CPO) creëert u een uniek, robuust en consistent beveiligingssysteem dat aansluit op uw IT-team en de rest van uw bedrijf.

Om het sterkst mogelijke beveiligingsniveau te creëren, is het dus van belang dat bedrijven samenwerken met leveranciers die niet alleen voordelen opleveren op het gebied van outputmanagement, maar ook ervaren zijn op het gebied van integratie.

Sharp heeft jarenlange ervaring met het produceren van zeer veilige MFP's/printers, het ontwikkelen van outputmanagementapplicaties en het implementeren van complexe oplossingen. We bevinden ons daarom in de juiste positie om onze klanten advies te geven over alle aspecten van beveiliging, inclusief het print- en outputbeveiligingsbeleid.

Het opbouwen van een printbeveiligingsbeleid en Sharp-outputbeveiligingsoplossingen



SCT – Sharp Consulting Team, **SRDM** – Sharp Remote Device Manager, **DSK** – Data Security Kit, **MFP** – Multifunction Printer, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Conclusie

De nieuwe bedrijfsnorm is dat elke keer dat iemand print, kopieert, scant of faxt een document het risico loopt te worden gestolen of aangetast.

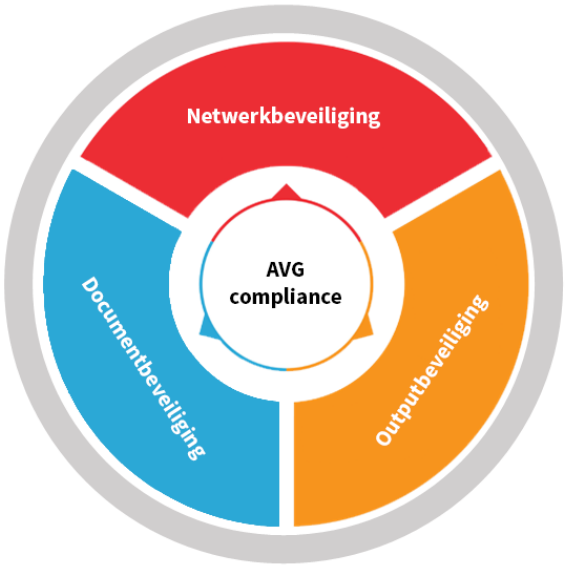
Bedrijven moeten beter op de hoogte zijn over de risico's van het niet beveiligen van fysieke of elektronische kopieën van gevoelige documenten en bestanden. De grootste issues zijn:

- Outputbeveiliging is essentieel voor elke moderne organisatie, ongeacht de omvang. Het groeiend aantal documenten dat door bedrijven wordt gegenereerd, brengt grote uitdagingen met zich mee omtrent het beheer van de IT-omgeving. Hieronder vallen het beheer van het stijgende aantal gebruikers, grotere bestanden, de hoeveelheid informatie die wordt gedeeld, overbelasting van netwerken en de gehele printeromgeving.

- Een outputmanagementsysteem geeft u maximale configuratieflexibiliteit. IT-beheerders beperken hiermee de toegang tot gesloten groepen kantoorgebruikers, én registreren daarnaast al hun activiteiten op de MFP, inclusief kopiëren, printen, scannen en faxen.

- Sharp begrijpt hoe belangrijk beveiliging is voor het moderne kantoor, en biedt hiervoor een unieke 360-graden-aanpak. Van netwerkbeveiliging, een beveiligingsaspect dat alle bedrijfsnetwerken en verbonden omgevingen dekt, en outputbeveiliging zoals beschreven in deze whitepaper, tot en met documentbeveiliging, een onderdeel dat ingaat op alle aspecten van documentgerelateerde beveiliging

- Deze uitgebreide beveiligingsaanpak zorgt er daarnaast voor dat uw organisatie profiteert van het hoogste compliance niveau met de nieuwste beveiligingsregelgeving, inclusief de Algemene verordening gegevensbescherming (AVG)



Om andere kwetsbaarheden binnen uw bedrijf te voorkomen, adviseren we dat u verder leest over het introduceren van nog meer beveiligingsmaatregelen, gerelateerd aan:

- Netwerkbeveiliging.
- Documentbeveiliging.
- AVG-compliance.

U vindt deze informatie op de informatiebeveiligingssectie van onze website: www.sharp.nl/informatiebeveiliging.

Of neem contact op met het Sharp Solutions Conslting Team

Bronnen

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

`

SHARP

Be Original.

www.sharp.nl | www.sharp.be