Whitepaper Informatiebeveiliging

Netwerkbeveiliging

Bescherming van de netwerkapparatuur in de kantooromgeving

www.sharp.nl | www.sharp.be

SHARP
Be Original.

Inhoud

Introductie

In de moderne verbonden wereld is effectieve informatiebeveiliging voor het volledige bedrijfsnetwerk essentiëler dan ooit.

Elke dag vinden talloze pogingen plaats om vertrouwelijke documenten te stelen, zonder autorisatie aan te passen, te onderscheppen of openbaar te maken. Daarnaast wordt keer op keer geprobeerd ongeautoriseerde toegang te verkrijgen tot privé- en bedrijfsnetwerken. Dit whitepaper onderzoekt de belangrijkste uitdagingen die bedrijven tegenkomen in de bescherming van hun IT-infrastructuur op het gebied van met het netwerk verbonden kantoorapparatuur, zoals multifunctionele printers (MFP's) en printers.

In dit whitepaper onderzoeken we:

- **De achtergrond**
  Elke dag komen bedrijven voor uitdagingen te staan op het gebied van netwerkbeveiliging, maar de kwetsbaarheden die verband houden met moderne, met het netwerk verbonden MFP's en printers worden vaak over het hoofd gezien. Hackers en cybercriminelen gebruiken die kwetsbaarheden om toegang te krijgen tot organisaties en zo vertrouwelijke informatie te stelen die staat opgeslagen op harde schijven en andere netwerkapparatuur. Of ze veroorzaken grote schade of verstoren de bedrijfsvoering. De impact hiervan op de productiviteit en winstgevendheid is soms enorm groot.

- **Het probleem**
  Het risico van niet-beveiligde MFP's en printers wordt vaak onderschat of genegeerd. Of bedrijven beschikken simpelweg niet over de juiste kennis en mogelijkheden om dit probleem te tackelen. Daarnaast wakkert een gebrek aan bewustzijn onder gebruikers het probleem verder aan, aangezien slechte gewoonten de veiligheid van documenten en data onnodig beïnvloeden. Bedrijven weten wel welke stappen ze moeten nemen om een printbeveiligingsbeleid te creëren, maar het is vaak een complex en tijdrovend proces.

- **De aanbevelingen**
  Wij adviseren een set hardware- en softwareoplossingen en verschillende best practices die u kunnen helpen een beveiligde printomgeving te creëren. Daarmee voorkomt u ongeautoriseerde toegang tot en aanvallen op apparatuur die met het bedrijfsnetwerk verbonden is. Deze sectie biedt specifieke oplossingen voor verschillende grote beveiligingsuitdagingen.

- Zes stappen om printbeveiligingsstandaarden in te voeren en in stand te houden, met een combinatie van Sharp-technologie en Sharp Optimised Software Solutions.
- 'Out-of-the-box'-functies en -instellingen beschikbaar op elk Sharp-netwerkapparaat uit de huidige productlijn, zoals wachtwoordbescherming, data overschrijven, encryptie et cetera.
- Optionele oplossingen die u helpen een consistent printbeveiligingsbeleidte creëren en printerparken eenvoudig en effectief te beheren, zoals Sharp Remote Device Manager (SRDM).
- Optionele geavanceerde functies en features voor MFP's en printers, zoals Data Security Kit (DSK).
- Optionele diensten van Sharp, zoals beveiligingsaudit, beveiliging-as-a-service, het vernietigen van data na de leaseperiode et cetera.

- **De conclusie**
  We bieden een samenvatting van het volgende:

- De consequenties van kwetsbaarheden voor elke, met het bedrijfsnetwerk verbonden, MFP en printer.
- Onze aanbevelingen gebaseerd op de Sharp-geïntegreerde features en aanvullende Sharp-beveiligingsoplossingen.
- Volgende stappen voor het creëren van een printbeveiligingsbeleid – met een interne aanpak óf met de hulp en expertise van het Sharp Professional Services-team.

Achtergrond

In de afgelopen jaren is de behoefte aan effectieve IT-beveiliging flink toegenomen – maar één gebied wordt nog over het hoofd gezien.

De meeste beveiligingsbewuste organisaties hebben ervoor gezorgd dat hun netwerk en computingmiddelen zijn beschermd met de nieuwste technologie. Zo installeren ze firewalls, stellen ze specifieke wachtwoordregels in, vragen ze om gebruikersauthenticatie en beschermen ze versleutelde en elektronisch ondertekende data, en nog veel meer.

Nieuwe technologieën, zoals cloud en mobile, brachten nieuwe uitdagingen met zich mee voor IT-beheerders en security-officers. Maar ook moderne, slimme MFP's en printers zijn doorontwikkeld en beschikken over verschillende geavanceerde mogelijkheden op het gebied van netwerkcommunicatie en dataopslag. In feite zijn het krachtige computers geworden met slimme functies. Volgens IDC zijn er bijna 53 miljoen printers en multifunctionele apparaten aanwezig in kantoren en huizen in West- en Oost-Europa1. De meeste daarvan zijn verbonden met een netwerk. Dit houdt in dat ze een toegangspunt zijn met een IP-adres, en dus net zo ontvankelijk voor malware en hackeraanvallen zijn als pc's of andere met het netwerk verbonden endpoints. Daarom vragen ze om dezelfde data-, communicatie en informatiebeveiligings-functies. toegang tot andere apparaten op het netwerk of gevoelige informatie. Communicatie en data die zijn opgeslagen op de harde schijf of in het geheugen van een MFP kunnen dan worden onderschept en zonder toestemming worden verstuurd naar elke mogelijke locatie ter wereld. De netwerkapparatuur zou daarnaast vatbaar zijn voor Denial Of Service-aanvallen (DOS). Dit soort aanvallen is ontworpen om het netwerk ontoegankelijk te maken voor eindgebruikers, en heeft een vergaande impact op de productiviteit van het bedrijf. Daarnaast kunnen slecht beveiligde apparaten toegang bieden tot phishing-aanvallen die als doel hebben vertrouwelijke informatie te bemachtigen of virussen te introduceren in het netwerk.

Bij 25% van de IT-beveiligingslekken die opgelost moesten worden, was print betrokken (1).

Bovenstaande is niet zomaar een hype – het is een serieuze bedreiging. Uit een recent IDC-onderzoek blijkt dat meer dan een kwart van de respondenten te maken heeft gehad met een groot IT-beveiligingslek. Bij meer dan 25 procent van deze incidenten betrof het de printomgeving (2).

Het niet beschermen van MFP's en printers kan grote gevolgen hebben voor een bedrijf, én voor de reputatie en het klantvertrouwen van het bedrijf. De negatieve effecten van een datalek zijn:

- Omzetverlies
- Productiviteitsverlies zonder toegang tot data en het netwerk.
- Verslechterde concurrentiepositie door gestolen informatie.
- Boetes vanwege niet naleven regelgeving;
- Rechtzaken.
- Ongeoorloofd gebruik van apparatuur en netwerkmiddeln

Probleem

Activiteiten van hackers en cyberaanvallen zijn inmiddels de norm. De malwaredreiging en impact hiervan op uw bedrijfsvoering is dichterbij dan u denkt – ongeacht uw bedrijfstype en -grootte.

Volgens onderzoeksbureau Quocirca geeft 63 procent van de ondervraagde bedrijven aan een of meer datalekken te hebben ervaren (3).

Dus waarom doen bedrijven dan niet meer om de bedreiging te bestrijden?

Het potentiële risico wordt helaas vaak over het hoofd gezien vanwege een gebrek aan inzicht in de kwetsbaarheden die ontstaan als apparaten zoals MFP's en printers worden verbonden met het bedrijfsnetwerk. Veel bedrijven hebben dus geen of ontoereikende printbeveiligingssystemen en -middelen, zoals getrainde mensen, best practices en beveiligingsprocedures voor het gebruik van netwerkapparaten binnen het bedrijf. Of ze gebruiken apparaten voor zakelijke doeleinden, terwijl deze apparaten juist ontworpen zijn voor privégebruik en dus over beperkte beveiligingsfuncties beschikken.

Met name mkb-bedrijven hebben vaak geen printbeveiligingsmaatregelen doorgevoerd en/of nog nooit een printbeveiligingsaudit ondergaan. Grotere organisaties hebben eerder een tekort aan de juiste mensen of kwaliteitstools om cyberaanvallen op netwerkapparatuur en verbonden technologieën te detecteren, beheren en voorkomen.

Daarnaast vormen slechte gebruikers-gewoonten vaak een serieuze uitdaging voor IT-beheerders, omdat ze kunnen leiden tot grote beveiligingsproblemen. Voorbeelden van zulke gewoonten zijn niet-beveiligd printen, documenten onbeheerd op de MFP of uitvoer laten liggen, printen vanaf niet-beveiligde USB-sticks, printen zonder endpoint-to-endpoint-versleuteling of gevoelige documenten opslaan op de harde schijf van de MFP of printer.

Bijna twee derde van de bedrijven heeft een print-gerelateerd datalek ervaren.

Voor veel organisaties kan ook het verwijderen van informatie aan het eind van de contractperiode een groot probleem zijn. Het printproces zorgt er soms voor dat er een kopie van de geprinte data achterblijft op de harde schijf van een MFP of printer. Wat gebeurt er dan met die data als het contract afloopt?

Het opzetten van een consistent netwerk-beveiligingssysteem of het introduceren van een printbeveiligingsbeleid voor het detecteren en voorkomen van ongeautoriseerde toegang tot een groep MFP's en/ of printers die zijn aangesloten op het netwerk, kan een zeer complexe en tijdrovende taak zijn. U moet in elk geval rekening houden met de volgende fasen:

- Voorspellen en beoordelen van de mogelijke consequenties van het ontbreken van een netwerkbeveiligingssysteem.
- Erkennen van het bestaan van mogelijke kwetsbaarheden en begrijpen hoe ze de netwerk-infrastructuur kunnen aantasten.
- Begrijpen van de complexiteit van de uitdaging, die van bedrijf tot bedrijf verschilt.
- Vinden van een intern of extern hulpmiddel dat helpt de uitdaging te tackelen.
- Tools identificeren die de MFP- en het printerpark kunnen monitoren, ongeautoriseerde toegang tot netwerkapparatuur kunnen voorkomen en u waarschuwen in het geval van afwijkende activiteiten.
- Opzetten en beheren van een betrouwbaar netwerkbeveiligings-systeem dat rekening houdt met alle unieke uitdagingen van uw bedrijf.

Aanbevelingen

Heeft bovenstaande u wakker geschud voor wat betreft uw eigen netwerkbeveiliging? Dat was precies de bedoeling. Het risico voor uw bedrijf moet niet worden onderschat. Maar wees niet bang.

Het is ons doel om u kennis te laten maken met een eenvoudige manier om printbeveiligingsmaatregelen in te voeren in uw bedrijf. Ook willen we laten zien hoe Sharp kan helpen inzicht te bieden in uw netwerkbeveiligingsniveau en hoe u dit eenvoudig kunt verbeteren

Maak gebruik van directe bescherming

Onderzoek door IDC laat zien dat "technologieleveranciers van hardcopy managed print- en document-services zich richten op printapparaat-beveiliging die voorkomt dat hackers het bedrijfsnetwerk binnendringen via print-apparatuur"4. Veel bedrijven vergeten echter de beveiligingsinstellingen, of stellen ze niet goed in, waardoor ze vatbaar zijn voor aanvallen.

De lijst met beveiligingsfeatures- en instellingen die volgt, is 'out-of-the-box' beschikbaar voor alle Sharp-MFP's en -printers. Ze zijn allemaal snel aan of uit te schakelen of aan te passen door de IT-beheerder om de standaard beveiligingsniveaus te veranderen. Daarnaast bieden ze een effectiever beschermingsniveau dat aansluit op uw specifieke bedrijfsbehoeften.

- Lokale beheerdersinstellingen zijn: wachtwoord wijzigen door de beheerder, webpaginatoegang op het apparaat, beveiliging voor gebruik op afstand.
- Standaard beveiligingsmodus: Poort Controle, Protocol instellingen, SNMP MIB instellingen, toegangsfilters, SSL, S/MIME, IPSEC, IEEE802.1X, Toestaan of weigeren van Mobiele Print Protocollen , Externe Service instellingen, Publieke mappen - Netwerkadres server, Tracking ID (Traceren van printinformatie), Gebruikersinstellingen, Toestaan/ weigeren gebruikersbeveiliging alternatieven, automatisch verwijderen van opgeslagen bestanden, verwijderen van de gehele printwachtrij in het geval van een fout.
- Ook zijn verschillende geavanceerde optionele instellingen beschikbaar. Deze instellingen geven IT-beheerders toegang tot Sharp-beveiligingsinstellingen voor organisaties die vragen om het hoogste beveiligingsniveau, zoals militaire of overheidsinstanties, of bedrijven die hun beveiliging naar het hoogste niveau willen tillen.
    - Data Security Kit (DSK) omvat: Data Security Kit-installatie, databeveiligingsverbeteringen, printbeveiligingsverbeteringen, Firmware-validatie.
    - Advanced Data Security Kit (Advanced DSK) omvat: HCD-PP gecertificeerde Advanced Security-modus (inclusief Data Security Kit), Opslag Encryptie-verbetering, Geavanceerde wachtwoordeis, Firmware beveiligingscontroles.

Zes eenvoudige stappen

Op de lange termijn bieden de volgende zes beveiligingsstappen een gestructureerde aanpak voor het ontwikkelen en introduceren van uw eigen, consistente netwerkbeveiligingsframework.

1. Beveilig de toegang tot het netwerk

Vertrouwelijke documenten zouden alleen geprint moeten worden met een beveiligde procedure die ongeautoriseerde toegang en ongeoorloofd kopiëren voorkomt. Doorgaans wordt een printopdracht opgeslagen op de HDD van het apparaat en pas daadwerkelijk geprint als de gebruiker een pincode invoert. Zodra het document is geprint, wordt alle data automatisch verwijderd van de HDD.

Technieken voor het garanderen van veilige communicatie tussen apparaten en het netwerk zijn:

- Maak gebruik van IP-filtering om toegang tot specifieke IP-adressen te beperken en MAC-filtering (Media Access Control). Dit helpt uw netwerk en communicatiekanalen te beschermen door alleen toegang te geven via gespecificeerde IP-adressen of -reeksen.
- Stel ongebruikte poorten buiten werking. Dit zorgt voor een extra beveiligingslaag en geeft u meer controle over uw netwerk door ongeautoriseerde toegang tot alle verbonden apparaten te voorkomen.
- Zorg ervoor dat IPSec (Internet Protocol Security voor veilige en versleutelde data-uitwisseling), TLS (Transport Layer Security voor versleutelde datatransmissie) en HTTPS (HyperText Transfer Protocol Secure voor beveiligde netwerk-communicatie) zijn geconfigureerd voor het hoogste beschermings-niveau.

2. Beveilig het apparaat (en bescherm uw data)
Er zijn twee manieren om ervoor te zorgen dat data opgeslagen op harde schijven (HDD) of MFP's en printers beveiligd blijft:

- Data-encryptie is de procedure of functie die documenten versleutelt met behulp van een complex 256-bits algoritme.
- Data Overwrite is de wisoptie voor de HDD van een apparaat. De optie zorgt ervoor dat alle data die op de harde schijf staat opgeslagen en alle elektronische afbeeldingen van geprinte documenten permanent worden verwijderd door ze tot tien keer te overschrijven.

Voor extra gemoedsrust biedt Sharp daarnaast een end-of-lease-/serviceoptie die ervoor zorgt dat alle digitale data die op een apparaat overblijft, wordt verwijderd, en dat de fysieke HDD wordt vernietigd.

3. Beveilig de gebruikerstoegang (via gebruikersidentificatie en -autorisatie)

Een van de belangrijkste stappen in het proces is controle krijgen over alle gebruikers door gebruikersbeheer en -autorisatie te introduceren. De belangrijkste activiteiten in deze categorie:

- Gebruikersidentificatie is het proces waarmee beheerders alleen geregistreerde gebruikers toegangsrechten geven tot MFP's en printers. Ze moeten gebruikers identificeren met lokale authenticatie, gebaseerd op de lokale gebruikerslijst, of met netwerkauthenticatie via de authenticatieserver.
- Gebruikersautorisatie wordt gebruikt om toegang te verlenen tot de netwerkapparatuur van de organisatie en om het gebruik ervan te beheren. Op basis van de gebruikers-bevoegdheden kunnen ze toegang voor bepaalde mensen beperken, toegang tot apparaat-functies begrenzen en toegang volledig blokkeren. De beheerder kan toegang tot het apparaat ook configureren met ID-kaarten, waarop de identificatie-gegevens van de gebruiker staan.

4. Print vertrouwelijke informatie op beveiligde wijze
Vertrouwelijke documenten zouden alleen geprint moeten worden met een beveiligde procedure die ongeautoriseerde toegang en ongeoorloofd kopiëren voorkomt. Doorgaans wordt een printopdracht opgeslagen op de HDD van het apparaat en pas daadwerkelijk geprint als de gebruiker een pincode invoert. Zodra het document is geprint, wordt alle data automatisch verwijderd van de HDD.

5. Beheer de netwerkactiviteit
Mits op de juiste manier geïnstalleerd, geven netwerkbeveiligingstools IT-beheerders rechtstreeks vanaf hun pc's de volledige controle over alle netwerkapparatuur. Op die manier beheren ze alle MFP's en printers en kunnen ze op afstand de meeste mogelijke beveiligingsrisico's ontdekken, apparaten instellen en beheren. De mogelijkheid om apparaten te klonen, stroomlijnt daarnaast hun werk en biedt extra gemoedsrust, omdat alle wijzigingen aan de apparaatinstellingen eenvoudig zijn toe te passen voor de gehele vloot.

6. Kies de juiste partner
Er zijn veel bedrijven die professionele printbeveiligingsdiensten bieden. Het deskundigheidsniveau loopt echter ver uiteen. Sharp neemt netwerkbeveiliging zeer serieus en is nauw betrokken bij elke nieuwe productontwikkeling. Als fabrikant wordt onze apparatuur beoordeeld op basis van richtlijnen die gespecificeerd zijn voor een Common Criteria-certificatie. Dat houdt in dat onze netwerk-MFP's met een geïntegreerde databeveiligingsoptie onafhankelijk zijn onderzocht door het internationaal erkende Japan's IT Security Evaluation and Certification-systeem (JISEC).

De apparaten voldoen volgens de certificering aan de nieuwste Protection Profile for Hardcopy Devices v1.0-standaard (HCD-PP v1.0) van de Common Criteria. Dat betekent dat we ondersteuning kunnen bieden aan klanten die omgaan met de gevoeligste data.

Schakel een expert in

Het bovenstaande lijkt misschien nogal overweldigend, maar onthoud dat u er niet alleen voor staat. U kunt altijd een expert inschakelen.

Sharp biedt verschillende oplossingen, tools en diensten om uw netwerkkwetsbaarheden de controleren en meten, maar ook om een verbeteringsplan te creëren en verschillende scenario's te ontwerpen die aansluiten op uw bedrijf.

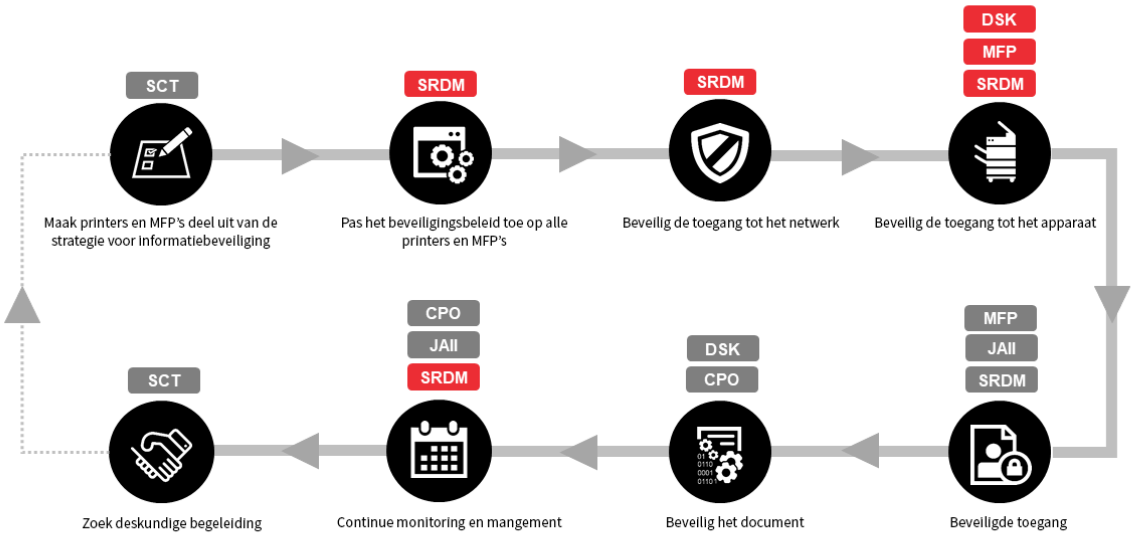
- **Workshop printbeveiliging**
  We kunnen verschillende tools en technieken inzetten die uw organisatie helpen inzicht te krijgen in de beveiligingsbedreigingen. Hieruit trekken we verschillende conclusies, en vervolgens creëren we een op maat gemaakt verbeteringsplan.

  De audit richt zich op alle netwerkperiferieën en hun beveiligingsniveau. We brengen alle standaard en geavanceerde features die beschikbaar zijn voor deze apparaten in kaart, alsook de tools voor effectieve bedreigingsdetectie en -preventie. Bovendien controleren we of uw bedrijfsapparatuur naar behoren werkt en maximale beveiliging kan leveren voor uw bedrijf en gebruikers. Daarnaast zet de printbeveiligingsaudit de 'volgende stappen' uiteen voor het introduceren van een consistent printbeveiligingsbeleiden gaan we in op alle beveiligingsaspecten van uw bedrijf, inclusief:

  - Netwerkbeveiliging – zoals beschreven in dit document.
  - Outputbeveiliging – omvat alle activiteiten gerelateerd aan document-output, zoals printen, scannen, faxen en e-mailen.
  - Documentbeveiliging – gaat in op het beheer van elektronische en papieren documenten binnen uw kantooromgeving.
  - AVG-compliance – garanderen van compliance met de meest recente EU-regelgeving omtrent beveiliging en de bescherming van persoonlijke gegevens.

- **Beveiligingspakket**
  Dit pakket combineert een klantenworkshop en Sharp Remote Device Manager-installatie en optionele Output Management-systeemconfiguratie en -implementatie om zo een bredere kantoorbeveiliging te garanderen – netwerkbeveiliging & outputbeveiliging.

- **Sharp Remote Device Manager (SRDM)**
  Deze Sharp-tool helpt u binnen enkele seconden kritische beveiligings-instellingen te implementeren. De implementatie wordt geleverd als een service van een getraind Sharp-team. Op basis van uw behoeften en eisen worden alle relevante beveiligingsinstellingen in uw IT-omgeving opgenomen en heeft u alle Sharp-MFP's en -printers onder controle.



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

Wat hebben we geleerd? Het goede nieuws is dat er ook goed nieuws is!

Hoewel MFP's en printers absoluut een serieuze (en momenteel nog onderschatte) bedreiging kunnen vormen voor uw bedrijf, zijn er verschillende stappen die u kunt nemen om het risico te verkleinen.

- **U bent niet de enige – bedreigingen zijn overal te vinden.** Elke dag worden we geconfronteerd met nieuws over datalekken, cyberaanvallen, virussen en andere kwaadwillende activiteiten bij bedrijven van alle grootten. Hierbij is het allerbelangrijkst om te realiseren wat de impact op uw bedrijf zou zijn als het zou worden getroffen door een aanval. Vraagt u zich eens af: 'Is mijn bedrijf goed genoeg voorbereid om zichzelf te verdedigen?'

- **De oplossing is niet altijd eenvoudig.** Het kan lang duren om te ontdekken wat de juiste beveiligingsmaatregelen en -functies zijn, en om deze te configureren en toe te passen. Bovendien brengt dit vaak implementatie-moeilijkheden met zich mee. Elke organisatie is anders, dus is het zaak dat u andere tools toepast en unieke strategieën introduceert die de specifieke bedreiging op uw bedrijf tackelen. Maar wat uw behoeften ook zijn, Sharp kan u helpen een effectieve beveiligingsoplossing te creëren voor de bescherming van uw MFP's en printers.

- **Is uw bedrijf niet voorbereid? Probeer erachter te komen wat het probleem is.** Waarom is uw bedrijf kwetsbaar? Beschikt het over voldoende tools en middelen om uw netwerk- en printbeveiligingsbeleid te creëren of verbeteren? Of moet u de hulp inschakelen van Sharp-specialisten om uw netwerken en netwerkperiferieën te beoordelen en relevante beveiligingstools in gebruik te nemen?

- **Creëer uw eigen beveiligingsdoelstellingen.** Om erachter te komen wat uw mogelijke kwetsbaarheden zijn en waar u behoefte aan heeft om voldoende bescherming te bieden, moet u antwoord geven op vragen als 'Waar moet mijn organisatie over een paar jaar staan?' en 'Hoe kan ik mijn bedrijf voorbereiden om de juiste maatregelen en tools te introduceren om in de toekomst cyberaanvallen, malware etc. te voorkomen?'.

- **Zorg ervoor dat u de juiste expertise hebt.** Als u intern over de benodigde middelen beschikt, kunt u uw eigen printbeveiligingsbeleid bouwen. Of u schakelt het Sharp Professional Services team in om u te helpen een effectief beveiligingssysteem te creëren en tools te introduceren die relevant zijn voor uw bedrijfstype en -behoeften, zoals:

    - Beveiligde netwerkapparatuur van Sharp die compatibel is met de meest recente beveiligingscertificaten.
    - Beveiligingssoftware, -oplossingen en -diensten van Sharp, die bijdragen aan een printbeveiligingsbeleid: DSK, SRDM, printbeveiligingsaudit etc.

- **Wij helpen graag.** Wij kunnen ervoor zorgen dat u geen onverwachte vertragingen oploopt bij de beoordeling en implementatie van uw printbeveiligingsbeleid. Medewerkers van Sharp staan klaar om u inzicht te bieden in uw huidige bedrijfsbeveiligingsniveau, dit te beoordelen, en een strategie voor te stellen die een consistent printbeveiligingsbeleid oplevert – afgestemd op de behoeften van uw organisatie. Onze specialisten helpen u de relevante tools en diensten uit de volgende lijst te kiezen:

    - Sharp- standaardbeveiligingsfuncties.
    - Optionele tools, zoals SRDM.
    - Optionele verbeteringen, zoals DSK.
    - Sharp-netwerkbeveiligingspakket.
    - Sharp-beveiligingsaudit.
    - Printbeveiligingsbeleid.

- **Kijk altijd naar het grote geheel.** Om mogelijke kwetsbaarheden in andere onderdelen van uw bedrijf te voorkomen,

kunnen we u helpen nog meer beveiligingsmaatregelen uit het Sharp-portfolio in uw organisatie op te nemen. Zo levert u 360-graden-beveiliging voor elk onderdeel van uw bedrijf:

- Netwerkbeveiliging.
- Outputbeveiliging.
- Documentbeveiliging.
- AVG-compliance.

Meer weten over onze beveiligingsoplossingen? Bekijk onze whitepaper-bibliotheek of ga naar de informatiebeveiligingssectie op onze website: www.sharp.nl/informatiebeveiliging

Of neem contact op met uw Sharp Solutions Consulting Team.

Bronnen

1. “Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years” report, IDC, Q4 2018
2. “IT and Print Security Survey 2015” IDC, September 2015
3. “Printing: a false sense of security”, Quocirca, 2013
4. “Transformative Technology in Document Security”, IDC, May 2015

`

SHARP

Be Original.