SHARP

Be Original.

Eenvoudige printerbeveiliging voor kmo-bedrijven.

Inhoudsopgave

Introductie

Peter Plested,
Director, Information
Systems bij Sharp
Electronics Europe

Printers of multifunctionele printers (MFP's) zijn een bekend gezicht op de meeste werkplekken.

Elke dag worden ze gebruikt en vanaf de buitenkant zien ze er vaak niet uit alsof er de laatste tien – of zelfs twintig – jaar veel aan veranderd is. IT-beheerders weten echter wel beter: van binnen zijn MFP's inmiddels uitgegroeid tot geavanceerde computersystemen, die verbonden zijn met uw bedrijfsnetwerk en het internet.

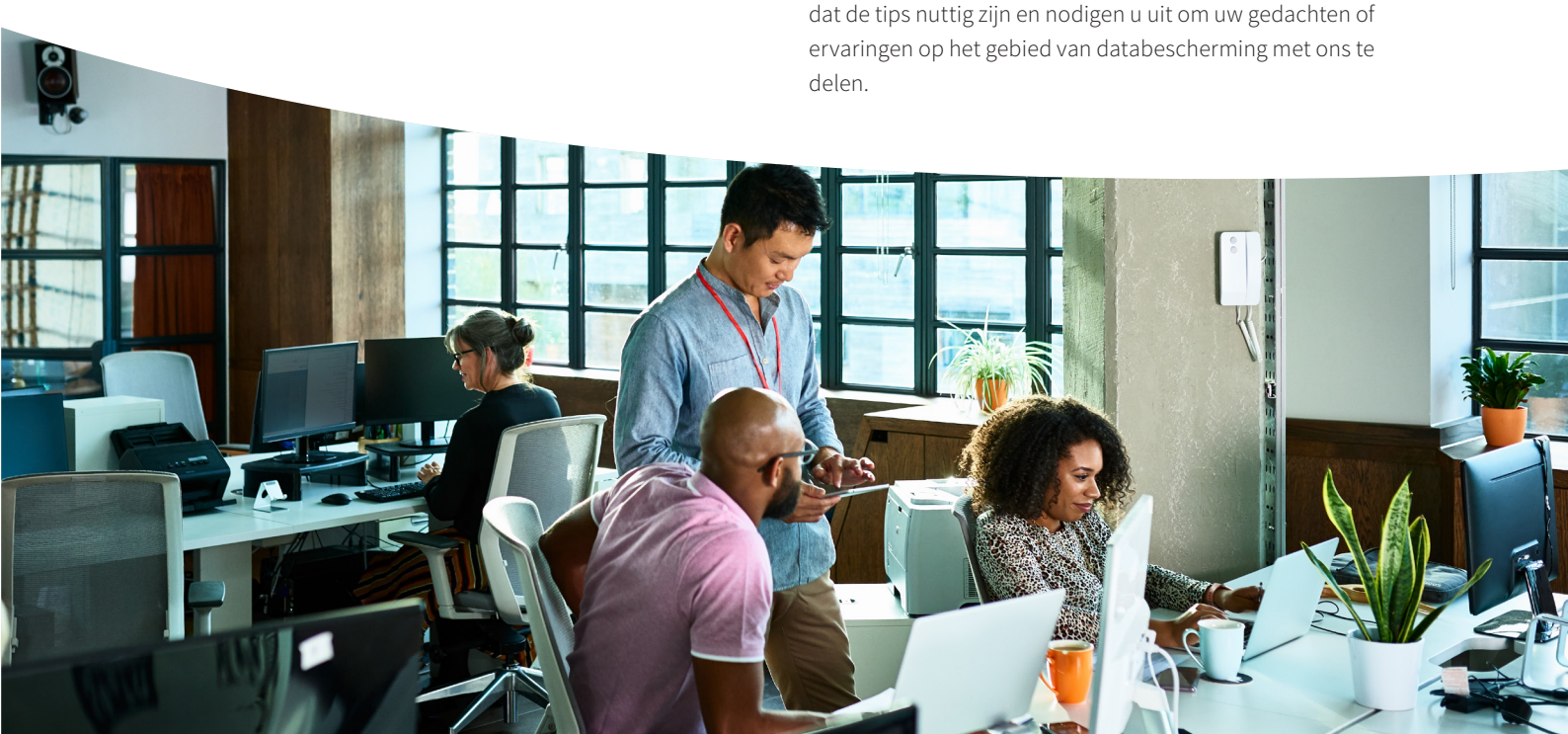
Hoewel negen van de tien Europese kantoormedewerkers niet inzien dat printers en MFP's een beveiligingsrisico vormen, zijn ze net zo vatbaar voor cyberaanvallen als een laptop of pc. Het is daarom belangrijk dat ze beveiligd worden en dat verantwoord gedrag bij gebruikers wordt gestimuleerd.

Als printerfabrikant staat beveiliging centraal in onze productontwikkeling. We willen ervoor zorgen dat onze producten en diensten het professionele leven van mensen vereenvoudigen en productiever maken – en tegelijkertijd de data beschermen.

We waren nieuwsgierig naar hoe mensen tegen printerbeveiliging aankijken. Zien zij, die niet in onze branche werken, printen als een probleem of risico? Om daarachter te komen, ondervraagden we meer dan 5.500 kantoormedewerkers in het Europese kmo. We ontdekten dat bijna de helft van de mensen niet eens wist dat het mogelijk is om een printer te hacken.

Ons onderzoek laat daarnaast zien dat er een overduidelijk tekort is aan formele training en advies op het vlak van printerbeveiliging. We streven ernaar deze kloof te helpen dichten met behulp van technisch advies en whitepapers die zijn te downloaden via onze website. Ook deze gids, die is gemaakt in samenwerking met ethische hacker Jens Müller, moet daarin ondersteunen.

De gids biedt een momentopname van het printgedrag op kantoor in Europa en biedt een aantal eenvoudige beveiligingstips voor de medewerkers die verantwoordelijk zijn voor de kantoortechnologie bij kmo-bedrijven. We hopen dat de tips nuttig zijn en nodigen u uit om uw gedachten of ervaringen op het gebied van databescherming met ons te delen.



Is uw bedrijfsnetwerk veilig?

Wist u dat kleinere bedrijven het minst vaak hun printerbeveiliging op orde hebben?

49% van de werknemers van de bedrijven in de Benelux met minder dan 49 medewerkers geeft aan dat iedereen hun printer of MFP kan gebruiken. Dit getal daalt naar 22% voor bedrijven met 151-250 werknemers.

De risico's van onbeheerde printertoegang lopen uiteen van malware die via de printer – per ongeluk of moedwillig – naar het netwerk wordt geüpload tot het uitlekken van vertrouwelijke gegevens die na het afdrukken op de uitvoerlade worden achtergelaten.

De belangrijkste resultaten van het onderzoek in de Benelux:

35%

Slechts 35 procent van de kantoormedewerkers is zich ervan bewust dat printers of MFP's een beveiligingsrisico vormen binnen hun bedrijf.

11%

11 procent van de kantoormedewerkers geeft aan dat er binnen hun bedrijf geen beveiligingsprotocollen zijn voor printers of MFP's.

21%

21 procent van de kantoormedewerkers geeft aan vertrouwelijke of persoonlijke informatie te hebben aangetroffen op de uitvoer van de MFP/printer; informatie die niet voor hen bedoeld was, wat een datalek is.

29%

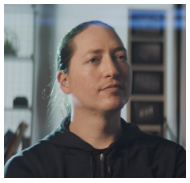
29 procent van de kantoormedewerkers heeft een kantoorprinter gebruikt om persoonlijke documenten af te drukken die ze thuis of buiten de beveiligingsomgeving van het bedrijf hadden gecreëerd

15%

15 procent van de kantoormedewerkers heeft de printers op kantoor gebruikt om een document af te drukken dat ze – ondanks een waarschuwing dat het document mogelijk onveilig was – hadden gedownload.

Het onderzoek is uitgevoerd voor Sharp door Censuswide. 5.514 medewerkers in bedrijven met 10-250 werknemers uit zeven Europese landen werden ondervraagd. Dit was inclusief het VK, Duitsland, Frankrijk, Italië, Benelux, Zweden en Polen.

Een expert aan het woord



Jens Müller
Ethische hacker

Jens Müller, ethische hacker, onderzocht de implicaties van de onderzoeksresultaten die uit het onderzoek van Sharp naar voren zijn gekomen, en de mogelijke risico's van printers en MFP's voor de data- en gegevensbeveiliging binnen kmo-bedrijven.

Het onderzoek van Sharp toont aan dat negen van de tien Europese kantoormedewerkers hun printer of MFP niet zien als mogelijk beveiligingsrisico voor hun organisatie. Waarom zou iemand immers de printer of MFP van een bedrijf willen hacken? Wat levert dat nu eigenlijk op?

Ten eerste zijn printers en MFP's overal te vinden. Elk bedrijf heeft er een; ze zijn verbonden met het netwerk en zijn daarom een eenvoudig doelwit voor hackers als ze niet over de juiste beveiliging beschikken.

Printers en MFP's bevatten waardevolle informatie. Daarom is er dus wel degelijk voldoende motivatie om een printer te hacken. Bedrijven moeten zich afvragen hoe waardevol de informatie is die ze printen en scannen. In een tijdperk waarin de Algemene verordening gegevensbescherming (AVG) bedrijven verplicht om de persoonlijk identificeerbare informatie van individuen – dus ook hun eigen medewerkers – die zij in hun bezit hebben te beschermen, vormt de printer of MFP een mogelijk kostbare zwakke schakel.

Er bestaan twee soorten hackers: kwajongens die er een lolletje aan beleven en hun hackvaardigheden uit nieuwsgierigheid willen testen, en kwaadwillende personen die bedrijfsspionage als doel hebben. Hoewel we niet precies weten hoe groot het probleem van beveiligingslekken via printers en MFP's momenteel is, weten we wel dat er tienduizenden printers zijn die eenvoudig gehackt kunnen worden, omdat ze niet over de juiste of een up-to-date beveiliging beschikken. Er liggen dus grote problemen op de loer.

Niet alleen de grote bedrijven lopen dit risico; het kmo is net zo kwetsbaar, met name als hun activiteiten interessant zijn voor criminelen die zouden kunnen profiteren van het stelen van data of verstoren van de bedrijfsvoering. Bijvoorbeeld als ze een toeleverancier zijn van een overheidsorganisatie. Het probleem wordt verergerd doordat, zoals het onderzoek laat zien, kleinere bedrijven over het algemeen over minder mogelijkheden en middelen beschikken om cybersecurity te tackelen dan grote organisaties.

Daarom is het zeer belangrijk om personeel goed te informeren. Net zoals kmo-bedrijven hun personeel trainen voor belangrijke beveiligingsbedreigingen als phishing, zo zouden ze hun personeel ook moeten informeren over de beveiligingsrisico's van printers en MFP's – voornamelijk over hoe ze deze risico's kunnen beperken. Maar de realiteit is dat 36 procent van de kantoormedewerkers in de Benelux nog nooit training of advies heeft gehad over hoe zij veilig moeten printen.

Wat de risico's zijn? Niet alleen kunnen printers en MFP's toegang bieden tot gevoelige geprinte, gekopieerde, gescande of gefaxte documenten, maar er bestaat ook het risico dat printers worden misbruikt om toegang te krijgen tot het bedrijfsnetwerk of om DDoS-aanvallen uit te voeren. Dit zagen we met de Mirai-botnet, die apparaten – inclusief printers en MFP's – wereldwijd aantastte, en de grootste DDoS-aanval uit de geschiedenis lanceerde. Hackers zijn altijd op zoek naar de zwakste schakel, en dat zou zomaar, ook binnen uw eigen organisatie, de printer kunnen zijn.

Krijgt de printer in de organisatie geen wachtwoord? Dan is dat een probleem. We weten dankzij het onderzoek dat in de Benelux bij ruim een derde van de bedrijven (36 procent) geen autorisatie nodig is om de printer of MFP te gebruiken. Oudere printers zijn mogelijk nog kwetsbaarder, doordat hun beveiliging niet up-to-date is. Vergelijk ze maar met oude Windows-computers die vaak een eenvoudig doelwit zijn voor cyberaanvallen of virussen. De kwetsbaarheden van achterhaalde software en door de WannaCry-aanval in 2017 duidelijk aan het licht. Diezelfde risico's zijn ook van toepassing op printers.

Hoe kan een kmo-bedrijf zich dan beschermen tegen een kwetsbaarheid op zijn printer of MFP? Vaak is verdedigen moeilijker dan aanvallen; een hacker hoeft alleen een opening te vinden, waardoor de IT-beheerder (of andere IT-verantwoordelijke) dus rekening moet houden met elke mogelijke zwakke schakel. Beveiliging van bedrijfsapparatuur is een terugkerende kostenpost voor elke organisatie. Dat verklaart mogelijk waarom beveiliging vaak onder aan de prioriteitenlijst komt te staan. Echter is elke besparing een mogelijke consequentie. Daarnaast is het lastig om te investeren in iets dat doet wat hij moet doen (in dit geval dus het printen of scannen van documenten).

Maar printen is niet de enige zwakke plek. Ook gescande documenten zijn door een hacker eenvoudig te lekken. Kmo-bedrijven doen er daarom goed aan om pdf-documenten te versleutelen en te controleren of de e-mailscans die vanaf de MFP zijn verzonden wel beveiligd zijn.

En hoewel de grootste focus op data ligt, is het belangrijk dat kmo-bedrijven de analoge bedreiging van informatie die op papier staat niet onderschatten. In het verleden konden hackers gevoelige informatie weleens zo uit de prullenbak vissen. Het kan eenvoudig zijn om toegang te krijgen tot de printer en afdrukken die in de papierlade achterblijven, omdat printers zich vaak op een vrij toegankelijke plek van de kantooromgeving bevinden en door meerdere afdelingen worden gedeeld.

De risico's lijken misschien overweldigd, maar het is gemakkelijker om printerbeveiliging te garanderen dan u denkt. Er zijn eenvoudige manieren om risico's te verlagen en de meeste vragen niet om een extra investering, behalve dan uw tijd. Bekijk de tips van Jens Müller voor IT-beheerders en andere IT-verantwoordelijken.

Tips voor een goede printerbeveiliging

Onderstaande tips zijn relevant voor printers en/of MFP's die zijn verbonden met uw bedrijfsnetwerk. Verschillende tips zijn van toepassing op instellingen die u zelf kunt veranderen, andere op instellingen waarvoor u de hulp nodig heeft van het bedrijf dat uw printer of onderhoudsdiensten heeft geleverd.

Pas standaard wachtwoorden aan

Geef hackers niet de controle over uw printer. Stel een sterk wachtwoord in voor het beheerderspaneel wanneer u het apparaat installeert. Printers worden vaak met een standaard wachtwoord geleverd. Dit wachtwoord is vaak ook bekend bij hackers. Daarom is het essentieel dat IT-beheerders het wachtwoord voor elke printer op het kantoor aanpassen. Deze handeling kan uw IT-beheerder vaak zelf uitvoeren.

Stel gebruikersauthenticatie in

Zorg ervoor dat uw MFP alleen printopdrachten accepteert van medewerkers met de juiste autorisatie. Stel de MFP zo in dat gebruikers zich eerst moeten authentiseren voordat ze documenten kunnen afdrukken. Gebruikersauthenticatie is te activeren vanuit het beheerderspaneel van de printer. Het beperken van de toegang tot gebruikers die op een whitelist staan, moet een essentieel onderdeel zijn van uw beveiligingsstrategie. Daarmee voorkomt u ongewenste afdrukken en aanvallen. Deze handeling kan uw IT-beheerder vaak zelf uitvoeren.

Voorkom dat de toegangscontrole wordt omzeild

Door ervoor te zorgen dat een gebruiker er in het beginscherm, na autorisatie, alleen voor kan kiezen om afdrukken, kopieën of scans te maken, hebben medewerkers geen toegang tot beheerdersinstellingen. Geef daarnaast bezoekers geen (tijdelijke) toegang tot uw apparaten, maar laat ze hun documenten afdrukken op een apart apparaat dat niet verbonden is met uw bedrijfsnetwerk. Zo voorkomt u dat onbevoegden toegang hebben tot uw bedrijfsnetwerk en gegevens

Schakel onnodige printdiensten uit

Maak alleen gebruik van dat wat u nodig heeft. Schakel alle andere netwerk- en lokale printdiensten uit om het aantal risico's te verkleinen. Als u erachter bent welke diensten, functionaliteiten en applicaties echt binnen uw bedrijf worden toegepast, kunt u andere, onnodige diensten uitschakelen. Als u bijvoorbeeld via IPP print, is het niet nodig om de RAW port 9100 voor printdienst open te houden. En als u bijvoorbeeld alleen via een netwerkkabel print, is het niet nodig dat uw printer als wifi-/Airprint-hotspot fungeert. Deze instellingen kan uw IT-beheerder vaak zelf aanpassen en uitvoeren.

Zorg voor een goede netwerkbeveiliging

Een bedrijfsnetwerk kan een groot risico zijn als het gaat om document- en gegevensbeveiliging. Door ervoor te zorgen dat uw printers niet rechtstreeks in verbinding staan met het internet, maar alleen het interne bedrijfsnetwerk, wordt het risico op ongevraagde afdrukken en een potentieel datalek verkleind. Dit klinkt misschien logisch, maar er zijn momenteel tienduizenden printers direct toegankelijk via openbare IP-adressen. U kunt uw, interne, netwerkbeveiliging verder vergroten met behulp van een IP- of MAC-adresfilter.

Vergeet de fysieke beveiliging niet

Voor ongeautoriseerde gebruikers kan het makkelijker zijn om fysieke toegang te krijgen tot printers en MFP's dan toegang via het netwerk. Het starten van een ongewenste printopdracht vanaf een USB-stick hoeft maar enkele seconden te duren. U kunt maatregelen nemen door gebruikersauthenticatie in te stellen of alle fysieke poorten uit te schakelen, zoals ongeautoriseerd printen via USB (voorzijde), parallel- of USB-kabel (achterzijde), NFC en bluetooth.

Plaats printers daarnaast niet onbeveiligd op openbare plekken, en zorg er daarnaast voor dat het onderhoud alleen wordt uitgevoerd door geautoriseerd personeel. Het is belangrijk dat uw medewerkers weten hoe ze om moeten gaan met verdachte of onbekende mensen die zichzelf wellicht toegang willen verlenen tot uw bedrijfsnetwerk of documenten.

Laat vertrouwelijke documenten niet achter op de uitvoerlade. Stel Secure Print Release (ook bekend als Pull Printing, Follow Me Secure Print of pick up protection) in op basis van pincodes of ID-kaarten om het te printen document vrij te geven. De nieuwste generatie printers geeft middels een knipperend lampje op de documenteninvoer aan als daar nog documenten liggen – om te voorkomen dat gebruikers weglopen zonder hun documenten mee te nemen.

Plan regelmatige firmware-updates

De laatste tien jaar zijn de kantoorprinters flink veranderd. Het zijn niet langer mechanische apparaten maar inmiddels complete computersystemen voorzien van verschillende softwarepakketten. Daarom is het essentieel om ze te behandelen zoals u ook de andere onderdelen uit uw IT-systeem behandelt. Zorg er dus altijd voor dat u de nieuwste beveiligingspatches en firmware-updates installeert.

De meest recente versie is het meest stabiel en veilig. Deze versie beschikt gegarandeerd over de nieuwste beveiligingsfuncties voor een optimale bescherming van uw bedrijfs- en persoonsgegevens. Plan een vaste, regelmatige afspraak in om firmware-updates te installeren of voer deze meteen uit als uw leverancier deze aan u beschikbaar heeft gesteld.

Monitor uw netwerk en printerpark

Wat gebeurt er als uw netwerk te maken krijgt met een datalek of verdachte activiteiten? Logbestanden kunnen informatie tonen over wat er precies is gebeurd en u kunt deze bewaren voor digitaal bewijs van inbraakpogingen, zoals ongewenste printopdrachten.

IT-beheerders kunnen e-mailnotificaties instellen om ervoor te zorgen dat ze op de hoogte blijven van kritische problemen en beveiligingsovertredingen. Zo is een IT-beheerder snel op de hoogte van beveiligingsproblemen of datalekken.

Voer uw oude apparatuur veilig af

Gooi oude of afgedankte apparaten niet zomaar weg. In het verleden hebben beveiligingslekken plaatsgevonden omdat hackers weggegooide printers in handen kregen en zo toegang kregen tot de harde schijven (HDD) of niet-vluchtig geheugen (NVRAM). Als het apparaat geïntegreerd was in het netwerk van de organisatie bestaat de kans dat er gevoelige data op staat. Zorg er daarom altijd voor dat het geheugen of de HDD is gewist, voordat u het apparaat weggooit of laat afvoeren. Stuurt u het apparaat terug naar het bedrijf waar u het vandaan heeft? Maak gebruik van de end-of-lease-functie, die ervoor zorgt dat alle data wordt overschreven, voordat het apparaat het gebouw verlaat.

Versleutel de data

In onze ogen nutteloos document kan voor een ander veel waardevolle informatie bevatten. Het is daarom zeer belangrijk om data op de printer of MFP te versleutelen. Als die data niet versleuteld is, dan wordt elk document dat wordt afgedrukt via een netwerkprinter als platte, leesbare tekst verstuurd. Iedereen die hier tussenkomt heeft toegang tot de afgedrukte of verstuurde printopdrachten. Wat in-transit versleuteling betreft - data die zich verplaatst over het internet of besloten netwerk - kunnen IT-beheerders kiezen uit twee verschillende encryptiemogelijkheden: Transport Layer Security (TLS/SSL) en IPsec, dat het complete netwerkverkeer versleutelt.

Wilt u vertrouwelijke bestanden, zoals gescande documenten, versturen? Maak dan gebruik van S/MIME end-to-end versleuteling op basis van certificaten of gebruik een pdf-versleuteling met een sterk wachtwoord. Om te garanderen dat documenten veilig zijn opgeslagen op de printer of MFP, kunt u de harddiskversleutelingsfunctie inschakelen.

Begrippenlijst

Authenticatie
Bij een unieke identificatie wordt er gecontroleerd of de identiteit overeenkomt met in een systeem geregistreerde gegevens. Om de authenticatie en identificatie te verifiëren wordt er vaak gebruikgemaakt van een gebruikersnaam en wachtwoord.

Poorten
Poorten worden gebruikt door netwerkapparaten (pc's, servers, printers, etc.) voor communicatie onderling (bijvoorbeeld een werkplek die verbinding maakt met een printer). Onbeschermde poorten en diensten kunnen worden gebruikt als aanvalsoppervlak, bijvoorbeeld om malware te uploaden.

Protocollen
Een protocol wordt gedefinieerd als een set van regels en formats die informatiesystemen toestaat informatie uit te wisselen. In een netwerkcontext zijn dat bijvoorbeeld IP- en TLS/SSL-protocollen.

Transport Layer Security (TLS/SSL)
Technologie die data versleutelt wanneer deze wordt verstuurd tussen het ene apparaat en het andere om te voorkomen dat derden er tussenkomen. TLS/SSL wordt vaak gebruikt voor websites, maar kan ook worden gebruikt om andere diensten te beschermen.

Internet Printing Protocol (IPP)
Een netwerk printing protocol dat in staat is tot authenticatie en het beheer van de printwachtrij. IPP wordt ondersteund door de meeste moderne printers en MFP's

IP-adressen
Elk apparaat dat verbonden is met het internet moet over een uniek nummer (IP-adres) beschikken om verbinding te maken met andere apparaten. Er zijn momenteel twee soorten IP-adressen: IPv4 en een nieuwere, geüpgradede versie: IPv6

IPsec (Internet Protocol Security)
Een verzameling protocollen voor het beveiligen van Internet Protocol-communicaties (IP) op de netwerklaag. IPsec bevat ook protocollen voor het aanmaken van cryptografische sleutels.

S/MIME (Secure/Multipurpose Internet Mail Extensions)
Een serie specificaties voor het beveiligen van e-mail. S/MIME is gebaseerd op de veelgebruikte MIME-standaard en beschrijft een protocol voor het toevoegen van beveiliging via digitale handtekeningen en versleuteling.

MAC-adressen
Een media access control-adres (MAC-adres) van een apparaat is een uniek identificatiemiddel dat is toegewezen aan een network interface controller (NIC). Dit betekent dat een apparaat dat verbonden is met een netwerk is te identificeren aan de hand van zijn MAC-adres.

IP- of MAC-adresfilters
IP- en MAC-adressen zijn unieke nummers voor het identificeren van apparaten op het internet (IP) of een lokaal netwerk (MAC). Filters zorgen ervoor dat IP- en MAC-adressen worden vergeleken met een 'whitelist' voordat apparaten verbinding kunnen maken met het netwerk.

Netwerkdiensten
server (die een of meerdere diensten draait), op basis van netwerkprotocollen. Een aantal voorbeelden: domain name system (DNS), dynamic host configuration protocol (DHCP), voice over internet protocol (VoIP).

Whitelist
Een whitelist is een exclusieve lijst met mensen, entiteiten, applicaties en processen die speciale goedkeuring, rechten of toegang krijgen. Vanuit zakelijk oogpunt zou dit het personeel van een organisatie kunnen zijn en hun rechten voor toegang tot het gebouw, het netwerk en de computers. In het geval van een netwerk of computer definieert een whitelist de applicaties en processen die het recht hebben op toegang tot dataopslag in beveiligde onderdelen.

DoS/DDoS
Een Denial of Service (DoS) is een soort disruptieve aanval waarbij de normale werking of dienst waarin het netwerk of apparaat voorziet, wordt geblokkeerd of verstoord. Een Distributed Denial of Service (DDoS) is een soort DoS-aanval die gebruikmaakt van meerdere (talloze) aanvalssystemen om de hoeveelheid netwerkverkeer te vergroten. Hierdoor raken de systemen of netwerken overbelast

Phishingaanval
Phishing is het versturen van e-mails die afkomstig lijken te zijn van legitieme bedrijven om individuen zo ver te krijgen persoonlijke informatie te delen, zoals wachtwoorden of creditcardnummers.

Spoofing-aanval
In het geval van een spoofing-aanval doet een kwaadwillende partij zich voor als een ander apparaat of andere gebruiker op het netwerk om aanvallen te lanceren tegen netwerkhosts, data te stelen, malware te verspreiden of toegangscontroles te omzeilen.

Man-in-the-middle-aanval
In het geval van een man-in-the-middle-aanval (MITM) bevindt de aanvaller zich stiekem tussen twee partijen die geloven dat ze rechtstreeks verbonden zijn en met elkaar communiceren. De aanvaller tapt de communicatie af en brengt in sommige gevallen wijzigingen aan in de communicatie tussen de partijen.

Malware-aanval
Kwaadwillende software (malware) valt te omschrijven als ongewenste software die zonder toestemming op het systeem wordt geïnstalleerd. De malware is in staat zich te hechten aan legitieme code en zich zo te verspreiden; in sommige gevallen houdt malware zich schuil in nuttige applicaties of vermenigvuldigt de software zich op het internet.

De beveiligingsfuncties van Sharp

Sharp biedt een reeks geïntegreerde beveiligingsfuncties om bedrijfsinformatie en -documenten te beschermen tegen een groot aantal bedreigingen.

De nieuwste Sharp-productlijnen van A3 MFP's en A4 MFP's beschikken over de modernste beveiligingsfuncties. Sharp biedt een unieke beveiligingsaanpak en geeft het kmo daarmee de middelen om hun printbeleid te beheren. Bovendien helpt deze aanpak de bedrijven hun vertrouwelijke informatie te beschermen, of die nu via het netwerk wordt geprint, gekopieerd, gescand, gefaxt, opgeslagen of gedeeld.

Van netwerkbeveiliging, die alle zakelijke netwerken en verbonden randapparaten dekt, tot outputbeveiliging voor het beheren en monitoren van toegang, en documentbeveiliging, die zowel digitale als fysieke documenten beschermt – Sharp biedt u een eenvoudige oplossing.

Deze uitgebreide beveiligingsaanpak garandeert dat uw bedrijf ook voldoet aan de nieuwste beveiligingsregelgeving, waaronder de AVG (Algemene verordening gegevensbescherming).

Uw beveiligingsbehoeften bespreken? Neem contact met ons op via dit formulier of via +32 15 21 53 11. Sharp zorgt voor de beveiliging, zodat u zich op uw bedrijf kunt richten.

* A3 modellen: MX-6071, MX-6051, MX-5071, MX-5051, MX-4071, MX-4061, MX-4051, MX-3571, MX-3561, MX-3551, MX-3071, MX-3061, MX-3051, MX-2651.
** A4 modellen: MX-C304W, MX-C303W

www.sharp.be

SHARP

Be Original.