SHARP

Whitepaper

Waarom u een ‘op de mens gerichte’ aanpak van beveiliging nodig heeft

MEER DAN 21% VAN DE EUROPESE WERKNEMERS OP KANTOOR GEBRUIKT ONVEILIGE PUBLIEKE CLOUD OPLOSSINGEN VOOR HET DELEN VAN VERTROUWELIJKE BESTANDEN

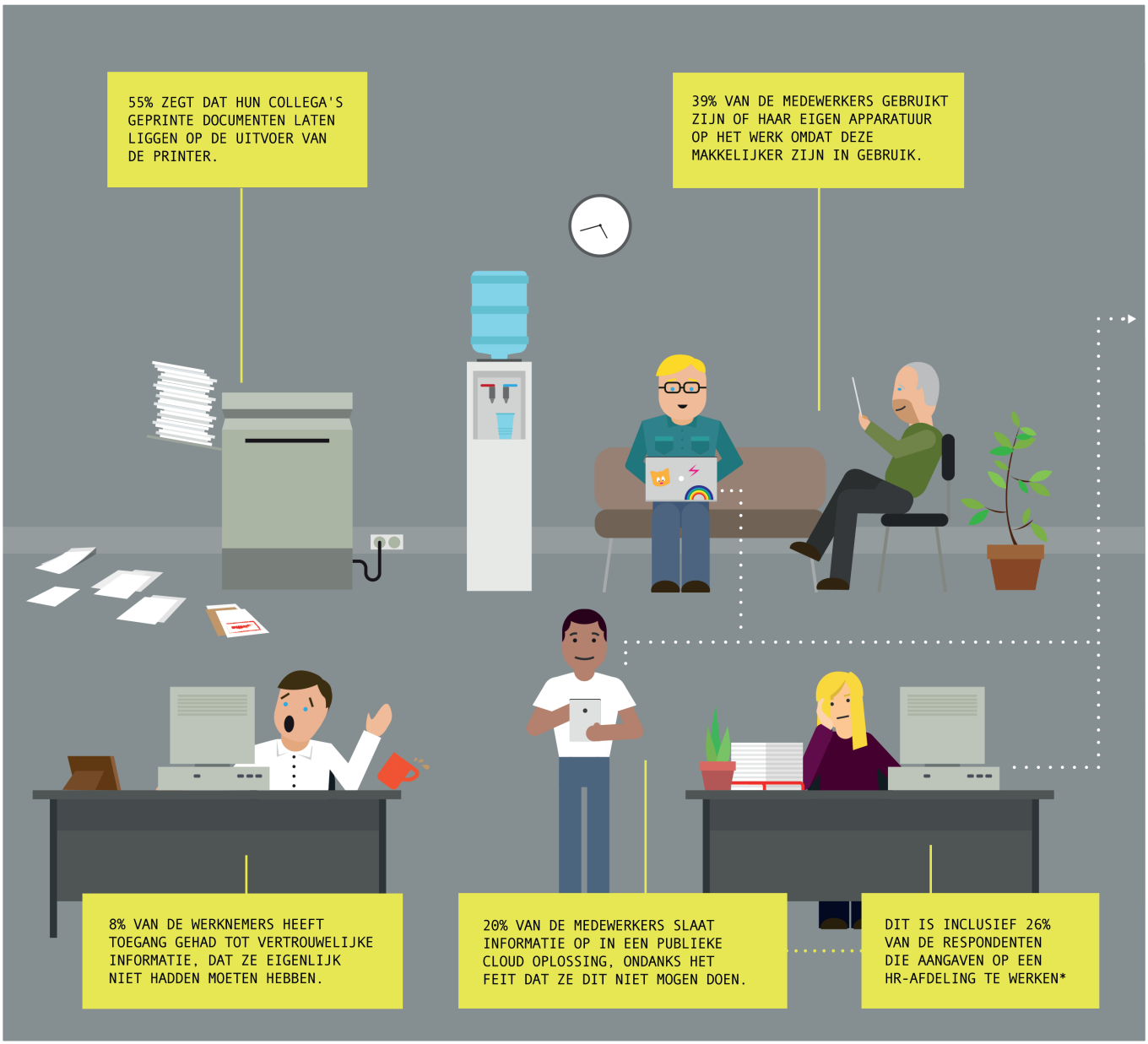
Volgens een onderzoek dat Sharp heeft uitgevoerd onder 6.045 kantoormedewerkers in Europa nemen werknemers databeveiliging niet serieus. Hierdoor lopen bedrijven vermijdbare veiligheidsrisico’s, die kunnen leiden tot hoge boetes, verlies van intellectueel eigendom en dat er een tekort aan medewerkers ontstaat.

We vroegen aan beveiligings- en privacy expert Dr. Karen Renaud om uit te leggen waarom databeveiliging voor kantoormedewerkers zo'n lage prioriteit heeft en hoe bedrijven dit kunnen veranderen om te zorgen voor een effectieve bescherming tegen externe en interne bedreigingen.

*Het onderzoek is uitgevoerd in april 2016 door Censuswide in opdracht van Sharp Europa.

Een ‘op de mens gerichte’ aanpak van beveiliging

Volgens een onderzoek dat Sharp heeft uitgevoerd onder 6.045 kantoormedewerkers in Europa, nemen mensen databeveiliging niet serieus. Hierdoor lopen bedrijven vermijdbare veiligheidsrisico’s, die kunnen leiden tot boetes, verlies van intellectueel eigendom en dat er een tekort aan medewerkers ontstaat.



Het onderzoek is uitgevoerd onder 6.045 medewerkers op kantoor in negen landen uit de Europese Unie (Frankrijk, Duitsland, Verenigd Koninkrijk, Italië, Zweden, Polen, Nederland, Tsjechische Republiek en Hongarije).

*457 respondenten gaven aan werkzaam te zijn op een HR-afdeling

Een ‘op de mens gerichte’ aanpak van beveiliging

- Bijna één op de tien (8%) ondervraagden gaf aan onterecht toegang te hebben gehad tot vertrouwelijke informatie.
- 21% van de mensen gaf desgevraagd aan dat zij publieke cloud oplossingen gebruiken voor het delen van bestanden zonder toestemming van het bedrijf waar ze voor werken.

- Bijna één derde van de respondenten (29%) gaf toe het kantoorprotocol te negeren en werk mee naar huis te nemen om af te kunnen maken.
- Het niet opvolgen van bedrijfsbeleid kwam veel voor: een vijfde van de medewerkers in het onderzoek (20%) gaf toe werk op te slaan in publieke cloud oplossingen zonder daar toestemming voor te hebben.
- Hierbij horen ook 26% van de ondervraagden die op HR afdelingen werken, en dus mogelijk persoonlijke gegevens in gevaar brengen*.

* 457 ondervraagde kantoormedewerkers gaven aan op een HR afdeling te werken.

Een ‘op de mens gerichte’ aanpak van beveiliging

We vroegen aan beveiligings- en privacy expert Dr. Karen Renaud om uit te leggen waarom databeveiliging voor kantoormedewerkers zo'n lage prioriteit heeft. Hierna legt Karen uit hoe bedrijven dit kunnen veranderen om te zorgen voor een effectieve bescherming tegen externe en interne bedreigingen.

Analyse en advies van Dr. Renaud

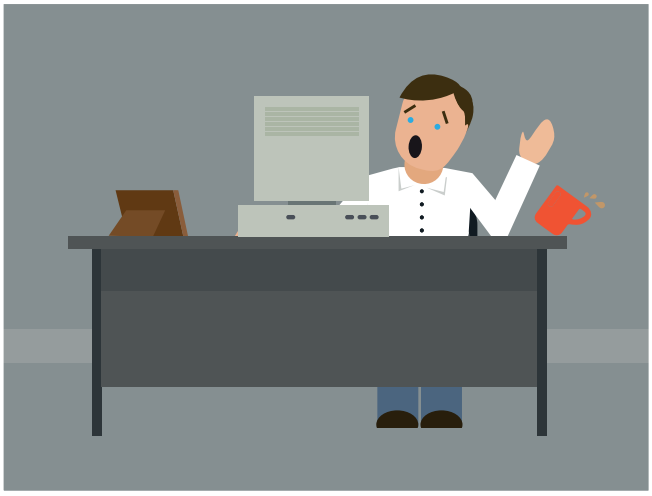
De bevindingen van het Sharp onderzoek verbaasden me niet. Het ondersteunt eigenlijk ander onderzoek dat is uitgevoerd door het Pew Research Centre in de VS naar houdingen ten opzichte van beveiliging en persoonlijke informatie.

Medewerkers dragen weliswaar de verantwoordelijkheid zich bewust te zijn van databeveiliging, maar ik denk niet dat werkgevers hun deel van de last voldoende op zich nemen.

Veel kleine bedrijven denken hun beveiliging te regelen door hun medewerkers simpelweg een beveiligingsbeleid te laten ondertekenen. Deze bedrijven zijn niet realistisch als ze denken dat het voldoende is om mensen gewoon een lijst instructies te geven.

In plaats daarvan zou je een mensgerichte aanpak moeten hanteren. Dit betekent het respecteren van het feit dat we mensen zijn, dat we op sommige gebieden feilbaar zijn en dat een willekeurige hoeveelheid instructies alleen er niet voor gaat zorgen dat we altijd veilig gedrag vertonen.

We hebben een oplossing nodig die zowel uit technologie als uit opleiding/ training bestaat.



8% VAN DE MEDEWERKERS HEEFT TOEGANG GEHAD TOT VERTROUWELIJKE INFORMATIE TERWIJL ZE DAT NIET HADDEN MOETEN HEBBEN

Waarom we beveiliging niet serieus nemen

Veel bedrijven denken dat ze het beveiligingsprobleem kunnen oplossen met vastomschreven beleid. Ik denk echter dat we iets realistischer moeten zijn, want het beheersen van menselijk gedrag is een van de moeilijkste dingen die er zijn.

We dienen te begrijpen dat het echt ingewikkeld is om mensen te managen en hen dingen op een bepaalde manier te laten doen, vooral als die activiteit een gewoonte is geworden.

Wij mensen leren steeds nieuwe vaardigheden en iedere keer dat we het geleerde herhalen wordt het automatischer. Alles wat je regelmatig doet wordt naar het automatische deel van de hersenen geduwd. Het is dus onrealistisch om van je mensen te vragen iedere mail zorgvuldig te controleren op de mogelijkheid dat het bijvoorbeeld een phishing mail is. Dat is niet de manier waarop het menselijk brein werkt. We gaan ervan uit dat dingen goed zijn als ze normaal gesproken goed zijn, en zo’n zeldzaam phishing bericht overvalt ons dus op een onbewaakt ogenblik.

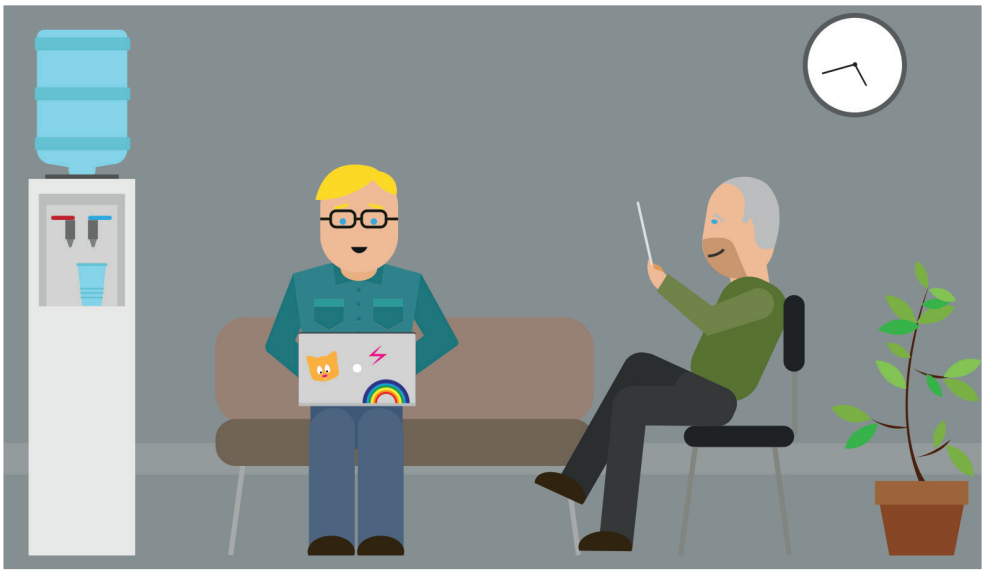
Een ander probleem is dat, hoewel we medewerkers instrueren te handelen en te reageren op bepaalde manieren, organisaties vaak hun medewerkers overladen met gemengde (en verwarrende) boodschappen.

Neem bijvoorbeeld e-mail. Een bedrijf vraagt zijn mensen om alert te zijn op links, maar stuurt frequent interne mails waarin links staan, waarop de medewerkers geacht worden te klikken en er kennis van te nemen.

Mensen denken vaak dat zij niet te maken zullen krijgen met een schending van de beveiliging, omdat het menselijk brein zich nou eenmaal niet zo snel ontwikkelt als de technologie. We zijn gewend te reageren op dingen die ons direct raken. Daarom is het lastig voor mensen om de gevolgen van slechte beveiliging te onderkennen als dit geen directe consequenties heeft.

Als je bijvoorbeeld een zwak wachtwoord gekozen hebt en er gebeurt niets, dan blijf je zwakke wachtwoorden gebruiken en blijft deze manier van denken hangen. Je gaat er niet van uit dat de beveiliging een gevaar kan lopen als een consequentie van jouw handelen. Vervolgens gebeurt er jaren later iets vervelends en dan is dat een nare verrassing.

39% VAN DE MEDEWERKERS GEBRUIKT ZIJN OF HAAR EIGEN APPARATUUR OP HET WERK OMDAT DEZE MAKKELIJKER ZIJN IN GEBRUIK



Bouwen aan een veiligheidscultuur

Mensen leren door te kijken hoe andere mensen binnen een organisatie zich gedragen, dus waar bedrijven zich op zouden moeten richten is op het opbouwen van een veiligheidscultuur.

Dit kan heel eenvoudig beginnen met de juiste training. Je moet er echter wel voor zorgen dat de training niet alleen relevant is, maar ook interessant en gevarieerd. Je kan mensen niet even vragen een webinar te volgen en dan verwachten dat dat het verschil maakt.

Organisaties zien training nog wel eens als een vaccin, in de zin van ‘we hebben iedereen ingeënt, dus nu kan ons niets meer overkomen’. We weten echter uit ervaring dat als mensen een training volgen zij direct daarna wel veilig gedrag vertonen, maar na verloop van tijd nemen de effecten af en begint veilig gedrag lastig te worden. Je kan bewustzijn niet in één keer tot stand brengen, je moet steeds blijven trainen en bewustzijnsacties uitvoeren.

Medewerkers moeten de problemen die met beveiliging te maken hebben onderkennen en het belang ervan begrijpen, omdat zij voortdurend de balans zullen zoeken tussen beveiliging en het afkrijgen van hun werk.

Organisaties moeten een dunne scheidslijn bewandelen tussen overmatig veilig handelen en onveilig handelen. Organisaties dienen een balans te vinden tussen veilig werken en mensen niet beperken in hun mogelijkheden hun werk effectief uit te voeren. Zodra beveiliging teveel een obstakel wordt gaan mensen op zoek naar manieren om dit te omzeilen. Er is een open cultuur nodig waardoor bedrijven weten dat dit gebeurt, zodat zij de lijn opnieuw kunnen trekken en betere manieren vinden om veilig te blijven werken.

21% ZEGT PUBLIEKE CLOUD SERVICES TE GEBRUIKEN VOOR HET DELEN VAN DOCUMENTEN ZONDER GOEDKEURING VAN HET BEDRIJF WAAR ZE VOOR WERKEN

Veiligheid opnemen in het ontwerp van de systemen

Als organisaties aan de slag gaan met het creëren van een beveiligingsbeleid dienen ze te bedenken hoe zij hun systemen zo kunnen ontwerpen dat onveilige situaties worden voorkomen. Op deze manier legt de organisatie de last alleen bij de gebruiker als er geen andere keus is.

Printers zijn hier een duidelijk voorbeeld van, omdat zij eenvoudig zo kunnen worden ingesteld dat data privé blijft. Normaal gesproken drukken mensen op een klein kantoor de afdrukknop in en, behalve als het dringend is, halen ze de pagina’s op een later moment wel een keer op. De afgedrukte informatie, die vertrouwelijk zou kunnen zijn, ligt daar dus al die tijd en er is een risico dat anderen het kunnen inzien.

Echter kan je bij veel printers een beveiligingsniveau toevoegen, bijvoorbeeld een code of een ID paslezer bij de printer, die gebruikt moet worden voordat de printopdracht verwerkt wordt. Op deze manier kan de gebruiker de printopdracht pas uitvoeren en meenemen als hij of zij voor de printer staat. Dit maakt onveilig gedrag onmogelijk, zonder dat de gebruiker er meer moeite voor hoeft te doen. De gebruiker moet de afgedrukte pagina’s sowieso op gaan halen, dus er komt geen extra last bij.

Er zijn veel meer beveiligingsmaatregelen zoals dit, die in de kantooromgeving kunnen worden ingebouwd. Je moet echter op vele gebieden over expertise beschikken, dus voor kleine bedrijven is het vaak raadzaam om dit aan de juiste leveranciers uit te besteden. Je kan niet verwachten van mensen die op andere gebieden gespecialiseerd zijn, dat ze ook zelf van alles weten over cyberbeveiliging.

55% VAN DE MEDEWERKERS GEEFT AAN DAT COLLEGA’S HUN GEPRINTE DOCUMENTEN LATEN LIGGEN OP DE UITVOERTRAY

Openbare versus eigen systemen

In toenemende mate worden publieke cloud tools om bestanden te delen een alledaags fenomeen binnen bedrijven, met alle potentiële risico’s van dien voor de informatie.

Als bedrijf moet je, in plaats van het gebruik ervan te verbieden, uitzoeken waarom mensen zulke tools en diensten gebruiken en welke informatie zij daar opslaan. De meeste mensen gebruiken zulke tools voor het delen van bestanden omdat het de makkelijkste manier is om data te delen met collega’s die op andere locaties werkzaam zijn.

Als je deze redenen steekhoudend vindt dien je hen een veiliger alternatief te bieden. Als je dat niet doet zullen ze de publieke sites voor het delen van bestanden blijven gebruiken en als ze weten dat jij dat niet wil, zal het heimelijk gebeuren. Sharp ontdekte dat 20% van de mensen werkinformatie in de cloud opslaan ook al weten ze dat ze daar geen toestemming voor hebben; het zou mij niet verbazen als dat percentage in werkelijkheid hoger ligt.

Er kunnen regels worden opgesteld die de zaken makkelijker en duidelijker maken. Bijvoorbeeld door het instellen van parameters waardoor gevoelige data niet kan worden verplaatst of overgezet en wordt opgeslagen op één locatie, terwijl niet gevoelige data elders wordt opgeslagen en vrijuit gedeeld kan worden.

Conclusie

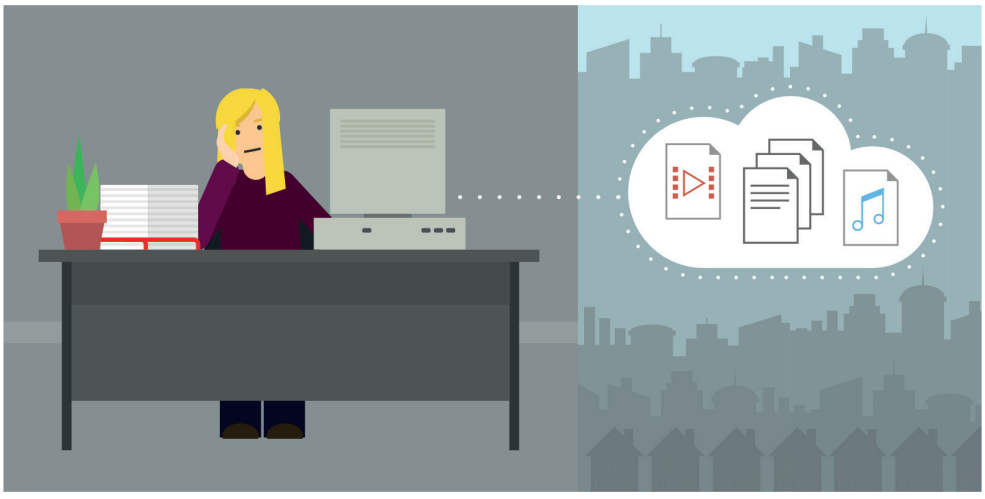
Mensen zijn geen computers en kunnen niet worden geprogrammeerd. Een mensgerichte aanpak is van essentieel belang voor de beveiliging; ontwerp dus voor mensen, niet voor robots.

Organisaties dienen zoveel mogelijk de technologie in te zetten om van de veiligste optie ook de automatische optie te maken. Maar bedrijven moeten ook de juiste balans vinden tussen beveiliging en mensen hun werk zo efficiënt mogelijk kunnen laten uitvoeren. Als het beveiligingsbeleid maakt dat mensen hun werk niet goed kunnen uitvoeren is het tijd om nog eens goed naar de gebruikte technologie te kijken.

Alleen door technologie, training en een mensgerichte aanpak met betrekking tot beveiliging te combineren kan een bedrijf naar veiligheid streven. Voortdurende instructie en training is ook een essentieel onderdeel van de beveiliging.

Maar onthoud dat er geen perfect vaccin is, het is een reis die we allemaal moeten blijven maken.

20% VAN DE MEDEWERKERS SLAAT INFORMATIE OP IN EEN PUBLIEKE CLOUD OPLOSSING, ONDANKS HET FEIT DAT ZE DIT NIET MOGEN DOEN



Sharp biedt een uitgebreide reeks aan beveiligingsoplossingen voor uw organisatie. Van beveiligingskenmerken die in Sharp's MFP hardware zijn ingebouwd, tot veilige printmanagement oplossingen en een cloud-based oplossing voor het opslaan en delen van elektronische bestanden. Onafhankelijk van de grootte van uw bedrijf kunnen we u helpen uw informatie te beschermen zonder uw team extra te belasten.

Beveiliging is standaard in de Sharp MFP ingebouwd

De intelligente MFP's en printers van tegenwoordig, die op bedrijfsnetwerken zijn aangesloten, bezitten veel van dezelfde soort datacommunicatie- en informatieopslagmogelijkheden zoals die ook op PC's worden aangetroffen. Daarom is het nodig net zoveel aandacht aan de beveiliging van de MFP's te besteden, als aan de beveiliging van computerapparatuur. De MFP's van Sharp hebben vele standaard ingebouwde beveiligingsfuncties die beschermen tegen mogelijke bedreigingen:

- **Gebruikersverificatie**
  Gebruikersverificatie en afdrukretentie houden in dat afgedrukte documenten niet worden verzameld op de uitvoertray van een MFP en zo het risico lopen door anderen binnen het kantoor opgehaald te worden.

- **Toegang**
  Hackers kunnen proberen om toegang te krijgen tot gevoelige gebruikersinformatie en adresgegevens die opgeslagen zijn op de harde schijf van een MFP. Sharp MFP's helpen deze dreiging aan te pakken met veilige wachtwoorden, filtering van IP en MAC adressen, port control en verschillende manieren van gebruikers-verificatie. Sharp's Data Security Kit (DSK) bevat versleutelingstechnieken (encryptie) die het praktisch onmogelijk maken om gegevens die achtergebleven zijn op een Sharp MFP te onderscheppen of te herstellen.

- **Veilig Scannen**
  Bepaalde Sharp MFP's bieden ook een scan-to-home functie die helpt om gescande afbeeldingen op de juiste manier op te slaan. Dit betekent dat gevoelige informatie niet per ongeluk wordt gescand en opgeslagen in de verkeerde netwerkmap. Beveiliging van gevoelige documenten kan ook worden geregeld via Sharp-versleutelde Adobe® PDF bestanden voor scannen en afdrukken.

- **Mobiele toegang**
  Tegenwoordig gebruiken veel mensen mobiel afdrukken. Sharp biedt een veilige manier voor mobiele gebruikers om te verbinden met het bedrijfsnetwerk via de MFP met gebruikersverificatie, een veilig op internet gebaseerd protocol en het vasthouden van het te printen document totdat de gebruiker bij het apparaat aanwezig is.

- **Audit Trail**
  Als bescherming tegen bedreigingen moet je in staat zijn verdachte activiteiten op te pikken. De zorgvuldige audit trail en job log functies van Sharp zorgen voor een uitgebreide controle op alle gebruikers- en apparatuur-activiteiten.

- **Veilig verwijderen**
  Als uw apparaat moet worden vervangen bieden de meeste Sharp MFP's standaard End-of-Lease functies die ervoor zorgen dat alle vertrouwelijke data en instellingen worden gewist en overschreven.

Optimised Software Solutions: Output Management

Sharp biedt printmanagement oplossingen voor alle soorten organisaties, klein of groot, om afdrukkosten te beheren en kosten toe te kunnen wijzen. Naast een ingebouwde facturatiecode en afdrukvrijgavefuncties zijn Sharp MFP's en printers compatibel met verschillende output management applicaties, die vereenvoudigde toegangscontrole en kostendoorbelastingsfuncties bieden. De voordelen zijn onder andere:

- **Toegang**
  Eenvoudige verificatie via netwerk gebruikersnaam en wachtwoord of ID kaart

- **Toestemming**
  Het beheren van MFP functies en toegang per gebruiker of per afdeling om de beveiliging te verbeteren

- **Zichtbaarheid**
  Het monitoren van alle activiteiten. Het beheren en monitoren van alle afdruk-/kopieer-/ en scanactiviteiten om de kosten te monitoren en bedrijfsmiddelen te optimaliseren.

- **Kosten doorbelasten**
  De mogelijkheid om gemaakte kosten in rekening te brengen per klant of project voor het werk dat je voor hen gedaan hebt.

Document Management en Workflow: Cloud Portal Office

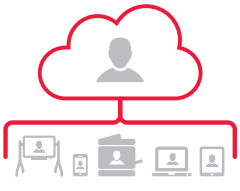
Cloud Portal Office van Sharp is onze bekroonde document management software en samenwerkingsoplossing voor het veilig opslaan en delen van elektronische bestanden en gescande documenten. Cloud Portal Office is volledig geïntegreerd met de MFP's en de BIG PAD interactieve schermen van Sharp, het helpt u efficiënter te werken en is een veiliger alternatief voor het gebruik van publieke cloud services door de medewerkers.

- **Toegang**
  Cloud Portal Office biedt veiligheidsfuncties die voldoen aan de industriestandaarden voor SaaS (Software as a Service) toepassingen, waarbij firewalls geïnstalleerd zijn aan de binnen- en buitengrenzen van het netwerk als bescherming tegen onveilige verbindingen en verkeer. Klanten worden voorzien van een eigen Cloud Portal Office-omgeving, waarbij het beveiligingsbeleid door het bedrijf kan worden bepaald en ingesteld, en dat maximale beveiliging voor aanvallen van buitenaf en voor onbevoegde toegang wordt geboden .

- **Zichtbaarheid**
  Uw IT beheerder houdt het overzicht over alle data binnen Cloud Portal Office. Ieder bedrijfsaccount krijgt een login voor een of meer Business Administrators. Deze admin logins worden normaal gesproken gebruikt door de IT medewerkers voor het monitoren en beheren van gebruikers binnen hun bedrijfsaccounts.

- **Bestanden delen**
  Cloud Portal Office biedt u strikte controle over wie toegang heeft tot uw bestanden, en deze kan wijzigen en delen. Wanneer u een bestand of een map met een collega deelt kunt u verschillende toestemmingsniveaus instellen, van alleen lezen, naar lezen, schrijven, wissen en delen. Het is ook mogelijk bestanden te sturen naar mensen die geen gebruik maken van Cloud Portal Office via een tijdelijke link, waarbij zij toegang krijgen om hun werk te kunnen doen, maar waarbij veiligheidsrisico's tot een minimum beperkt zijn.

- **Mobiele toegang**
  In de balans tussen beveiliging en toegankelijkheid biedt Cloud Portal Office eenvoudig "On-the-go" toegang tot opgeslagen content. Gebruikers die de Cloud Portal Office app op hun mobiele apparaat hebben geïnstalleerd kunnen documenten ophalen via een veilige SSL verbinding. Voor extra veiligheid dienen gebruikers zich aan te melden voordat zij toegang krijgen tot data. Hun gegevens zijn versleuteld op hun apparaat en ook alle systeemtoegang is versleuteld. Mocht een mobiel apparaat gestolen worden, dan kunt u uw wachtwoord resetten via een web browser.



Welkom bij Sharp

Bij Sharp werken we voortdurend aan innovatie om nog meer uit een bedrijf te kunnen halen. Onze vooruitstrevende kantoortechnologieën hebben een revolutie teweeggebracht in de manier waarop bedrijven met informatie, technologie en elkaar omgaan. Dit willen wij ook voor u realiseren. Ontdek hoe we vandaag nog verborgen potentieel in uw bedrijf kunnen losmaken.

SHARP

Inspiring ideas from technology

www.sharp.nl **www.sharp.be**