Whitepaper Informatiebeveiliging

Documentbeveiliging

Bescherming van bedrijfsinformatie

www.sharp.nl | www.sharp.be

SHARP
Be Original.

Inhoud

Introductie 3
Achtergrond 4
Probleem..... 5
Aanbevelingen 8
Conclusie 11
Bronnen 12

Introductie

Elke dag verwerken organisaties duizenden documenten in allerlei formats. Documenten die kunnen kwijtraken, gestolen of aangetast worden. Het is daarom essentieel om ze te beveiligen.

Sharp definieert documentbeveiliging als de beveiliging van informatie die afkomstig is van gescande papieren documenten of digitale documenten die staan opgeslagen in bedrijfsarchieven, zoals Microsoft Office-bestanden, e-mails, etc. Sharp-documentbeveiliging omvat:

- Documentgerelateerde bedrijfsprocessen;
- Documentopslag (fysieke, papieren documenten en elektronische archieven);
- Documentlifecycle (vastleggen → opslaan → beheren → bewaren → delen → integreren).

Dit whitepaper beschrijft de documentbeveiligingsuitdagingen waar elk bedrijf mee te maken heeft. De belangrijkste punten hierin zijn:

- **De achtergrond**
  Onderzoekt de complexiteit van documentbeveiliging. Van het identificeren van alle kantoordocumenten en -informatie in de meest voorkomende bedrijfsprocessen tot en met het onderscheiden van papieren (fysieke) en elektronische (digitale) documenttypen, en een omschrijving van het documentlifecycleproces.

- **Het probleem**
  Omschrijft de uitdagingen waar IT-beheerders, eindgebruikers en het bedrijfsmanagement mee te maken hebben vanuit een documentbeveiligingsperspectief. Met name op het gebied van het vastleggen, opslaan en toegang krijgen tot bedrijfsgevoelige documenten en informatie. De focusgebieden zijn:

  - Ongestructureerde data;
  - Handmatige taken gerelateerd aan kantoordocumenten;
  - Documentbeveiliging in het algemeen.

- **De aanbevelingen**
  Bespreekt hoe de Optimised Solutions, diensten en best practices van Sharp, kunnen helpen bij het creëren van een beveiligde documentomgeving. Zo'n omgeving voorkomt documentbeveiligingsbedreigingen die datalekken of verstoringen van documentverwerking kunnen veroorzaken. Daarnaast gaat deze sectie in op hoe Sharp u kan helpen complexe bedrijfsproblemen op te lossen omtrent:

  - Het inzien van het belang en de rol van documentprocessen.
  - Het optimaliseren van op papier gebaseerde archieven en elektronische bestandsarchieven.
  - Het identificeren van alle benodigde stappen voor het optimaliseren van de documentlifecycle of het creëren van uw eigen documentbeveiligingsbeleid en best practices.

- **De conclusie**
  Geeft een samenvatting van het onderwerp en focust op het volgende:

  - De belangrijkste bedrijfsuitdagingen gerelateerd aan zakelijke documenten.
  - De voornaamste aanbevelingen op basis van de expertise van Sharp en Sharp Optimised Products.
  - De benodigde stappen voor het creëren van een consistent documentbeveiligingsbeleid.
  - Het koppelen van documentbeveiliging aan andere beveiligingsaspecten in de kantooromgeving, inclusief netwerkbeveiliging en outputbeveiliging.

Achtergrond

De snelheid waarmee we werken en de hoeveelheid data die we creëren en consumeren, groeit exponentieel.

Industrieanalist IDC voorspelt dat de wereldwijde datacreatie in 2025 groeit tot een enorme hoeveelheid van 163 zettabytes (ZB). Dat is tien keer zoveel als de hoeveelheid data die werd geproduceerd in 2017.

Elke dag creëren bedrijven contracten, facturen, voorstellen en allerlei andere documenten, in talloze formaten. Al die documenten spelen een essentiële rol in hun bedrijfsvoering.

Zo definiëren contracten de handelsrelatie tussen de organisatie en hun klanten, terwijl facturen inkomsten opleveren als ze worden voldaan. Het beheren, bewaren en beschikbaar maken van deze informatie voor de juiste medewerkers is van grote invloed op het succes van een bedrijf.

90 procent van alle huidige data is de afgelopen twee jaar gecreëerd – dat is 2,5 quintiljoen bytes aan data per dag (2)

De omvang, de complexiteit en de diversiteit van de informatie die wordt gecreëerd en gebruikt door een bedrijf leidt tot uitdagingen op het gebied van beheer en controle. Om deze uitdagingen te tackelen, moeten bedrijven documenttypen begrijpen en in kaart brengen. Het is belangrijk dat ze inzicht krijgen hoe de documenten worden gebruikt, welke rol ze spelen in de bedrijfsprocessen en hoe ze worden opgeslagen, beheerd, gedeeld en bewaard.

Het grootste deel van deze uitdagingen staat direct in verbinding met drie hoofdissues.

- **Ongestructureerde data**

Ongestructureerde data is informatie die óf niet beschikt over een vooraf gedefinieerd datamodel, óf niet georganiseerd is op een vooraf gedefinieerde wijze. Vaak worden transactionele documenten zoals e-mails of kantoordocumenten door gebruikers opgeslagen in mappenstructuren die ze zelf aanmaken, zonder standaard conventies voor bestandsnamen of omschrijvende metadata.

Om die reden is het erg lastig om één overzicht te krijgen, en zijn de volgende vragen moeilijk te beantwoorden:

- Hoe worden documenten opgeslagen, beheerd en gecontroleerd?
- Hoe eenvoudig zijn documenten te vinden, auditen en delen?
- Hoe worden toegangsrechten en bestandsmachtigingen toegepast?

- **Handmatige processen**

Handmatige processen komen in bijna elk bedrijf voor, of het nu gaat om het verwerken van facturen, onkosten of beheren van HR-documenten. Technologie kan deze processen veel beter automatiseren, voor verhoogde efficiëntie, nauwkeurigheid en een betere volgbaarheid. Maar ook zeker voor betere beveiliging.

- **Inzicht in de documentlifecycle van uw bedrijf**

Elk document of documenttype heeft zijn eigen lifecycle, van vastleggen tot en met vernietigen. Het begrijpen, in kaart brengen en optimaliseren van de documentlifecycles voor verschillende documenttypen speelt een grote rol in de toepassing van de juiste beveiligingsmaatregelen voor het voldoen aan de regelgeving. Daarnaast leidt dit tot de benodigde flexibiliteit om efficiënt te werken.

Dit zijn belangrijke elementen die elk bedrijf moet overwegen bij het introduceren van een documentbeveiligingsbeleid voor de organisatie.

Probleem

Moderne bedrijven verwerken veel informatie, maar hebben vaak onvoldoende inzicht in hoe die informatie wordt geproduceerd, opgeslagen en hoe de toegang is geregeld. Dit leidt tot mogelijke beveiligingsproblemen.

De meeste organisaties omarmen digitale-contentcreatie en-opslag, maar de documenten worden vaak in twee formats opgeslagen: elektronisch (digitaal) en op papier (hardcopy).

- **Papieren bestanden/archieven**

Hardcopydocumenten in papier- of andere format vormen een groot beveiligingsrisico. Het is lastig om hun herkomst aan te tonen of een duidelijk auditspoor te identificeren, wat leidt tot een gebrek aan volgbaarheid. Daarnaast wordt de fysieke beveiliging vaak vergeten en worden vertrouwelijke documenten bijvoorbeeld vaak verkeerd gearchiveerd, raken ze kwijt of worden ze opgeslagen op niet-beveiligde locaties.

- **Elektronische bestanden/archieven**

Elektronische archieven die zijn opgeslagen in verspreide en soms geïsoleerde opslagsystemen brengen hun eigen beveiligingsuitdagingen met zich mee door hun grote volume en het aantal opslagsystemen/-locaties. Inzicht in de lifecycle van documenten is de enige manier om bedrijfsbrede processen en beveiligingspolicy's te introduceren.

Documentbeveiliging garanderen

De definitie van documentbeveiliging (of het gebrek daaraan) is breed en moet worden bekeken vanuit het perspectief van de documentlifecycle. Met name in relatie tot datalekken, ongestructureerde data, onbeveiligde bestanden, menselijke fouten, ongeautoriseerde toegang tot de opslag, etc.

De documentlifecycle bestaat uit zes hoofdfasen – vastleggen, opslaan, beheren, bewaren, delen en integreren.

- **Fase 1: vastleggen**

Vastleggen is de procesfase die de 'onboarding' van informatie omvat, of het nu gaat om het scannen van hardcopydocumenten, actief monitoren van een e-mailbox of het creëren en opslaan van documenten via een applicatie.

- **Scannen** is de meest voorkomende manier van het omzetten van hardcopycontent naar elektronische formaten. Hoewel scannen makkelijk is, kan het leiden tot uitdagingen op het gebied van beveiliging en wettelijke toelaatbaarheid. Zonder controle is het proces niet volgbaar, en behalen documenten mogelijk niet de test van bewijskracht en wettelijke toelaatbaarheid.

- **Indexeren** verwijst naar de methode die documenten omschrijft met behulp van metatags of full content (tekst). Indexeren maakt het mogelijk om bestanden snel te doorzoeken en faciliteert data discovery – tools die handig zijn bij het beoordelen van content voor wat betreft beveiliging of naleving.

- **Routing** is het proces dat wordt gebruikt om documenten naar de juiste opslaglocatie te sturen. Zonder documentrouting kunnen documenten per ongeluk worden opgeslagen op verkeerde of onbeveiligde locaties.

- **Fase 2: opslaan**
  Veilige opslag is mogelijk in papiervorm of een elektronisch bestandsformaat, maar veel bedrijven zien het opslagtype, de opslaglocatie en de benodigde beveiliging over het hoofd.

- Papieropslagsystemen komen nog steeds veel voor, maar de beveiliging hiervan is vaak onvoldoende. Daarnaast is het moeilijk om de juiste auditinformatie aan te tonen.

- Elektronische opslag wordt vaak geïmplementeerd met de gedachte dat het de betere methode is. Zonder duidelijk ontwerp en beheer zorgt deze vorm van opslag echter voor verschillende moeilijkheden. Hoe moeten zulke systemen bijvoorbeeld worden beveiligd in het bedrijfsnetwerk? Hoe worden de toegangsrechten ingesteld? En hoe monitor en beperk je het gebruik?

- **Fase 3: beheren**
  Documentmanagement omvat toestemming, versiebeheer en auditsporen.

- Machtigingen worden gebruikt om de toegangsrechten van gebruikers tot documenten te beheren. Ze spelen dus een belangrijke sleutelrol in een goed beveiligde documentomgeving. Hoewel machtigingen op zich niet ingewikkeld zijn, zijn ze zonder de juiste systemen moeilijk te introduceren en beheren. Om ze effectief te introduceren, moeten bedrijven eerst inzicht krijgen in hoe de gebruikersactiviteiten zich verhouden tot de informatie waar gebruikers toegang toe moeten hebben en de processen waarbij ze betrokken zijn.

- Versiebeheer zorgt ervoor dat gebruikers met de meest recente documenten werken terwijl eerdere versies (indien nodig) bewaard blijven. Dit is met name handig in strategische of juridische situaties waarin de herkomst van een document kan worden aangetoond door eerdere versies na te lopen. Versiebeheer is van groot belang bij het creëren van een goed beveiligd en wettelijk toelaatbaar archief voor digitale documenten.

- Een auditspoor slaat informatie op over elke activiteit en transactie van een document, inclusief informatie over wie het document heeft gecreëerd, aangepast, bekeken of er een nieuwe versie van heeft gemaakt. Auditsporen maken de activiteiten van alle opgeslagen documenten inzichtelijk en spelen een belangrijke rol in het garanderen van een goede beveiliging, met name als er een datalek plaatsvindt.

- **Fase 4: bewaren**

Het bewaren van documenten en informatie is een andere belangrijke factor in de beveiliging van een documentomgeving. Maar documenten die zijn opgeslagen in traditionele of elektronische archieven vragen om continu onderhoud, omdat de beschikbare opslagruimte beperkt is. De volgende procedures zijn dan ook essentieel.

- **Documentretentie**

Sommige documenten moeten (volgens de wet) een specifiek aantal jaren bewaard worden. De uitdagingen hierin bestaan uit:

  - Het bijhouden van een overzicht om ervoor te zorgen dat alleen documenten die buiten de bewaarperiode vallen, worden verwijderd.
  - Ervoor zorgen dat alle versies van de documenten die onder de bewaarpolicy vallen compleet en aanwezig zijn.
  - bepalen hoe documenten moeten worden beheerd – centraal of lokaal.

- **Documentvernietiging**

Bedrijven moeten policy's opstellen om zich op veilige wijze te ontdoen van alle papieren informatie, elektronische bestanden of elektronische bibliotheken zodra deze zijn verlopen of de bewaarperiode voorbij is.

  - Fysieke documentvernietiging is de traditionele manier om je van papierwerk te ontdoen op basis van een van de DIN Shredding Security-niveaus. Dit kan kostbaar en tijdrovend zijn.
  - Elektronische vernietiging verwijst naar het veilig en verifieerbaar wissen van elektronische documenten van harddrives of andere gegevensdragers.

- **Stage 5: delen**
  Deze fase definieert de manieren waarop een elektronisch document kan worden gedeeld met andere gebruikers of zakelijke partners.

  - Bestandsdeling vindt vaak plaats via gedeelde mappen of schijven, maar als deze niet juist worden beheerd kan dit ertoe leiden dat de bestanden worden gevonden en gebruikt door ongeautoriseerde gebruikers of gebruikersgroepen.
  - Toegang krijgen tot documenten via mobiele apparaten kan ook onderdeel zijn van de deelfase. Dit zorgt voor complexe problemen op het gebied van beveiligde toegang.

- **Fase 6: integreren**
  Integratie is het proces dat wordt gebruikt om informatie uit te wisselen met andere applicaties binnen het bedrijf, zoals een accounting- of ERP-systeem.

  Om integratie te laten slagen en consistente en juiste gegevens te bieden, is het essentieel dat de voorgaande fasen correct en compleet zijn. Problemen op het gebied van één van de eerder genoemde punten hebben een directe impact op het bedrijfsproces.

Aanbevelingen

Sharp biedt verschillende oplossingen en applicaties die organisaties kunnen helpen een databeveiligingsbeleid te creëren.

Documentbeveiliging is zeer complex, maar wordt duidelijker en gemakkelijker te begrijpen door de structuur van de documentlifecycle te definiëren, en vervolgens aan te passen of te verbeteren.

- Het van de basis af aan verbeteren van processen of definiëren van documentbeveiliging kan ingewikkeld en tijdrovend zijn, met name bij het in kaart brengen van processen en vastleggen van alle relevante informatie over processen en bedrijfsrollen. Sharp Professional Services maakt gebruik van zowel ervaring in documentoplossingen als van geavanceerde tools voor documentinformatie-discovery en workflow-mapping.

- Sharp gebruikt een stapsgewijs proces om bedrijven te helpen inzicht te krijgen in hun huidige documentlifecycle en gerelateerde uitdagingen. Vervolgens gebruiken we deze informatie om de processen en procedures te ontwerpen om in te spelen op de twee hoofddoelen van het optimaliseren van documentbeveiliging:

    - Structuur aanbrengen in ongestructureerde data.
    - Veel voorkomende taken versnellen en stroomlijnen.

Snel en veilig starten

- Sharp helpt klanten robuuste beveiligingspolicy's en documentomgevingen te creëren. De combinatie van onze Sharp-MFP's voor verzameling en ons Optimised Software-portfolio voor documentopslag- en beheer geeft klanten het vertrouwen dat hun documentinfrastructuur goed beveiligd en volgbaar is.

- Om te beginnen kan dit kleine procesveranderingen betekenen voor papier-intensieve afdelingen (HR, Finance of de juridische afdeling) waarna de processen en procedures stapsgewijs zijn uit te breiden naar andere delen van het bedrijf.

Vastleggen en opslaan van documenten vereenvoudigen

- Om ervoor te zorgen dat scannen veilig is, adviseert Sharp klanten om alleen te scannen naar beveiligde, interne systemen en geselecteerde e-mailgroepen of gebruikers. Deze zijn allemaal op Sharp-MFP's in te stellen door IT-beheerders. Dit is met name belangrijk met het oog op de AVG.

- Als er meer geavanceerde mogelijkheden nodig zijn, is hierin te voorzien met het Optimised-portfolio van Sharp-producten. Sharp biedt verschillende oplossingen die processen versnellen voor kleine, middelgrote en grote bedrijven. Ook zijn ze direct te integreren met veelgebruikte bedrijfsapplicaties.

- Sharp Optimised Solutions bieden de mogelijkheid om alle verzamelde documenten te indexeren:
    - Voeg rechtstreeks vanaf de MFP metadata toe.
    - Voeg metadata toe in de applicatie-interface, voorafgaand aan het opslaan en verwerken van de documenten.

- Sharp Optimised Solutions voorzien in routing-opties om ervoor te zorgen dat alle gebruikers op dezelfde gestructureerde wijze scannen en verzamelen. De documenten worden vervolgens doorgestuurd naar de juiste, relevante locaties en vaste applicaties.

Gebruikersrollen en -machtigingen

Bij het creëren van een documentbeveiligingsbeleid spelen gebruikersmachtigingen en -rollen een belangrijke rol in het bewaken van vertrouwen en controle.

- Sharp adviseert het gebruik van één centraal documentmanagementsysteem met gebruikersrollen die gekoppeld zijn aan de behoeften van een medewerker. Zoals:

    - Alleen directieleden hebben toegang tot alle bedrijfsdocumenten.
    - Alleen HR heeft toegang tot personeelsdocumenten.
    - Alleen projectmanagers hebben toegang tot project gerelateerde documenten.
    - Salesvertegenwoordigers hebben toegang tot salesgerelateerde bestanden, zoals brochures, formulieren, etc.

- Machtigingen worden gedefinieerd op basis van een rol of groep om controle te houden over wat gebruikers met documenten kunnen doen – creëren, bekijken, aanpassen, verwijderen. Het is ook mogelijk om in te stellen dat gebruikers documenten alleen kunnen bekijken en verder geen machtigingen hebben.

- Versiebeheer is essentieel. Met de Sharp Optimised Solutions kunt u bekijken aan welke versie van het document u werkt en eerdere versies nalopen of herstellen.

- Gezamenlijk, op hetzelfde moment werken wordt ondersteund door documentmanagement. Dit houdt in dat wanneer de ene medewerker in het document werkt, de andere het alleen kan lezen.

- Om ervoor te zorgen dat er wordt voldaan aan de beveiligingsregelgeving kunnen IT-beheerders gebruikmaken van een geavanceerde tool voor auditsporen dat alle documentactiviteiten bijhoudt. Inclusief wanneer een document is aangepast, wie het document heeft aangepast en hoelang een specifieke gebruiker aan het document heeft gewerkt.

Bewaar de juiste informatie voor het juiste moment

- Ontwerp een policy voor documentretentie (het al dan niet bewaren van documenten in het archief, en de (wettelijk bepaalde) bewaartijd van die documenten), gebaseerd op het type document en de afdelingen die de informatie verwerken.

    - Documentvernietiging is het eindpunt van het documentbewaarbeleid. Afhankelijk van het archief zijn er verschillende opties voor het verwijderen van alle data uit uw systemen.

        - Voor papieren documenten adviseert Sharp het gebruik van een professionele vernietigingsservice met tenminste een 5 DIN-beoordeling.
        - Voor elektronische documenten adviseert Sharp het gebruik van een elektronische-datawisservice.
        - Voor data die staat opgeslagen op HDD's (die gebruikmaken van on-premise documentmanagement en interne archieven) adviseert Sharp een tweeledig proces – datawissen en vervolgens fysieke vernietiging om ervoor te zorgen dat er geen toegang meer mogelijk is tot de harde schijven.

Probleemloze informatietoegang en -deling

Elk documentbeveiligingsbeleid dat in het bedrijf wordt ontwikkeld, moet beschrijven hoe gebruikers/medewerkers toegang krijgen tot documenten en hoe ze de gegevens kunnen delen met anderen.

Sharp Optimised Solutions bieden verschillende methoden om documenten te delen via documentmanagement-platformen.

- De eerste optie is om via e-mail een link naar het bestand te delen, waarbij de link na een bepaalde tijd verloopt. Details van de deelactiviteit worden vastgelegd en de link kan op verzoek door een vooraf ingestelde time-outperiode buiten werking worden gesteld.

- De tweede optie is om mappen binnen het systeem te delen met geregistreerde gebruikers van dezelfde organisatie. U bepaalt de rechten van de ontvangers – ‘lezen’, ‘lezen, bewerken’ of ‘lezen, bewerken, verwijderen’ – omtrent het werken aan de documenten uit de map. Deze rechten zijn ook in te stellen bij het ontwerpen van de overkoepelende regels voor het documentmanagementsysteem en het documentbeveiligingsbeleid.

- De meeste functies van het systeem zijn ook beschikbaar te maken voor mobiele werknemers, op zowel Android als iOS. Sharp adviseert dat bedrijven de voordelen van veilig mobiel werken goed in overweging nemen.

Het meeste uit uw data halen

Sharp heeft verschillende integraties ontwikkeld, zodat de gegevens die zijn verzameld met Sharp-MFP’s, hot folders of verbonden applicaties, zijn te integreren met bedrijfssystemen als Exact, Afas, OneDrive, SharePoint, etc.

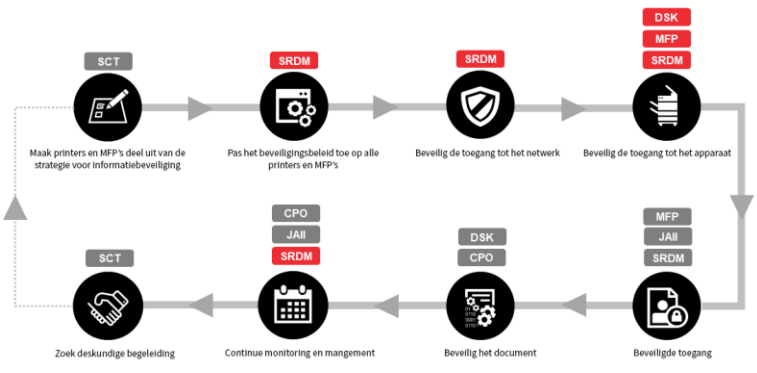
Sharp focust zich onder meer op:

- **Geoptimaliseerde workflow-software voor factuurverwerking**
  De oplossing maakt gebruik van Optical Character Recognition (OCR) om gegevens van facturen te halen en automatiseert de validatie- en goedkeuringsprocessen. Dit maakt het voor de crediteurenadministratie mogelijk om sneller, nauwkeuriger en efficiënter te werken

- **Geoptimaliseerde workflow-software voor digitale postverwerking**
  De oplossing verzamelt binnenkomende papieren en digitale post en verstuurt deze post elektronisch naar de juiste medewerkers of hun vervanger in het geval van een out of office-melding. De oplossing helpt bedrijven snel en efficiënt grote hoeveelheden post te sorteren en verdelen, en maximaliseert zo de personeelsproductiviteit.

- **Geoptimaliseerde workflow-software voor human resources**
  Deze oplossing introduceert een zeer veilig en beheerd archief voor vertrouwelijke personeelsdocumenten. Bedrijven kunne

Het bouwen van een printbeveiligingsbeleid en Sharp-documentbeveiligingsoplossingen



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

Geen enkel bedrijf kan het zich veroorloven informatiebeveiliging te negeren, met name als er documenten bij betrokken zijn. Ze zijn het intellectuele goud van elke organisatie, en het verlies ervan heeft een grote impact.

Documentbeveiliging is één van de belangrijkste beveiligingsaspecten van elk bedrijf. Helaas kan het creëren van een documentbeveiligingsbeleid een tijdrovend en complex proces zijn. Daarbij kan Sharp helpen.

Sharp heeft jarenlange ervaring in de branche van documentoplossingen, waardoor we een uitgebreide databeveiligingsaanpak hebben kunnen ontwikkelen voor bedrijven – van netwerkbeveiliging en outputbeveiliging tot en met documentbeveiliging.

We streven ernaar klanten te helpen een robuuste beveiliging te creëren voor hun documentgerelateerde bedrijfsprocessen, die voldoet aan alle regelgevingen. Dit doen we met behulp van onze expertise en ons internationaal erkende leiderschap in kantoorbeveiliging.

Met een bewezen aanpak voor documentbeveiliging helpen we bedrijven unieke systemen en processen te creëren voor elke stap uit de documentlifecycle (vastleggen, opslaan, beheren, bewaren, delen en integreren). Ook helpen we bedrijven te voldoen aan de meest recente privacyregelgevingen, zoals de Europese Algemene Verordening Gegevensverwerking (AVG).

Sharp Optimised Solutions zijn ontworpen om maximale functionaliteit en beveiliging te leveren, maar ook een snelle ROI.

Belangrijke verticale markten voor Sharp zijn de overheid, het onderwijs, de juridische sector, de financiële dienstverlening, de gezondheidszorg, de horeca en het bedrijfsleven. We leveren echter robuuste oplossingen voor elk type bedrijf.

Om mogelijk kwetsbaarheden in andere delen van uw bedrijf te voorkomen, kunnen we daarnaast helpen nog meer beveiligingsmaatregelen te introduceren. Met deze maatregelen uit het Sharp-portfolio levert u een 360-graden beveiliging voor elk onderdeel van uw bedrijf:

- Documentbeveiliging.
- Netwerkbeveiliging.
- Outputbeveiliging.
- AVG-naleving.

Meer informatie over de bovenstaande onderwerpen vindt u in onze whitepaper-bibliotheek of op de informatiebeveiligingssectie van onze website.

Of neem contact op met uw Sharp Solutions Consulting Team.

Bronnen

1. “Data Age 2025”, IDC, maart 2017
2. “Data Never Sleeps 5.0”, DOMO, 2018

`

www.sharp.nl | www.sharp.be

SHARP

Be Original.