KYOCERA

kyoceradocumentsolutions.nl

Houd documenten veilig, van creatie tot archief.

Whitepaper

Veilig digitaal samenwerken.

De beveiliging van documenten is van cruciaal belang in onze hybride maar steeds digitalere wereld. Het beschermen van gevoelige informatie is cruciaal, of het nu gaat om persoonlijke informatie, financiële gegevens, bedrijfsgeheimen of intellectueel eigendom.

In deze whitepaper bespreken we hoe de beveiliging van documenten gedurende de hele levenscyclus, van creatie tot archivering, kan worden gegarandeerd.
Kom meer te weten over het belang van documentbeveiliging, best practices voor het maken van documenten, toegangscontrolemaatregelen, veilige opslag, versleuteling, samenwerking, het verwijderen van documenten, archiveringsstrategieën en niet onbelangrijk: hoe vertel je klanten over het belang van documentveiligheid.

Laten we beginnen met het kijken naar documentveiligheid en de stappen die je kunt nemen om de veiligheid en integriteit van je waardevolle gegevens te waarborgen.

Waarom documentveiligheid belangrijk is voor jouw organisatie.

In het huidige digitale tijdperk is informatie de levensader van elke organisatie. Daarom is documentbeveiliging belangrijker dan ooit. Denk aan de gevolgen die een datalek of onbevoegde toegang tot gevoelige informatie kunnen hebben: reputatieschade, juridische kwesties, financiële schade en wantrouwen bij klanten en zakenpartners.

Documentbeveiliging is niet alleen een wettelijke of reglementaire vereiste; het is een fundamentele vereiste voor elke verantwoordelijk opererende organisatie.

Bescherming van persoonlijke informatie

Wanneer organisaties persoonlijke gegevens van klanten, werknemers en partners verzamelen en opslaan, is het hun ethische en wettelijke verantwoordelijkheid om deze informatie te beschermen tegen onbevoegde toegang, identiteitsdiefstal en fraude.

Bescherming van financiële informatie

Denk aan de gevolgen van onbevoegde toegang tot financiële gegevens, betalingsinformatie of intellectueel eigendom met betrekking tot financiële transacties. De vertrouwelijkheid en integriteit van financiële gegevens moeten gewaarborgd blijven om financiële fraude en potentiële financiële schade te voorkomen.

Vergeet ook niet het beschermen van handelsgeheimen en gegevens waarop eigendomsrecht rust. Organisaties investeren veel geld in R&D en ongeoorloofde openbaarmaking van vertrouwelijke informatie kan leiden tot verlies van concurrentievoordeel, verminderde innovatie en schade aan de eigen marktpositie.

De beveiliging van documenten en informatie bevordert het vertrouwen van klanten, zakenpartners en andere belanghebbenden. Ze zullen eerder geneigd zijn om zaken te doen en een langdurige relatie aan te gaan met een organisatie als ze weten dat hun informatie veilig is.

Door prioriteit te geven aan documentbeveiliging, laat je zien dat je organisatie zich inzet voor gegevensprivacy en naleving van wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). Dit voorkomt juridische sancties en geeft belanghebbenden het vertrouwen dat je hun privacyrechten serieus neemt.

Kortom, documentbeveiliging is geen optie, het is een vereiste. Het beschermt persoonlijke gegevens, financiële informatie, handelsgeheimen en bedrijfsinformatie. Het helpt organisaties te voldoen aan regelgeving, het vertrouwen van klanten te behouden en hun reputatie te beschermen.

Met deze informatie als basis gaan we nu verder met het onderzoeken van de verschillende stadia van documentbeheer, van het maken van documenten tot het archiveren ervan.

Documentveiligheid is geen optie, het is een vereiste.

Documenten maken

De beveiliging van documenten moeten vanaf het begin worden geïmplementeerd zodat gevoelige informatie wordt beschermd vanaf het moment dat het wordt gemaakt.

Zo maak en houd je documenten veilig.

Veilige omgeving

Allereerst is het natuurlijk belangrijk om in een veilige omgeving te werken. Dit betekent dat je alleen betrouwbare en veilige netwerken en apparaten moet gebruiken. Maak of open geen gevoelige documenten terwijl je gebruik maakt van openbare wifi of onbeveiligde apparaten, omdat deze kwetsbaar kunnen zijn voor onbevoegde toegang of het onderscheppen van gegevens.

Sterke authenticatie

Voeg een beveiligingslaag toe met een sterk wachtwoordbeleid en multifactorauthenticatie. Laat gebruikers werken met complexe wachtwoorden en laat ze deze regelmatig aanpassen. Meerfactorauthenticatie, zoals het gebruik van een combinatie van een wachtwoord, toegangspas, beveiligingstoken of een pincode, voegt een extra beschermingslaag toe tegen ongeautoriseerde toegang.

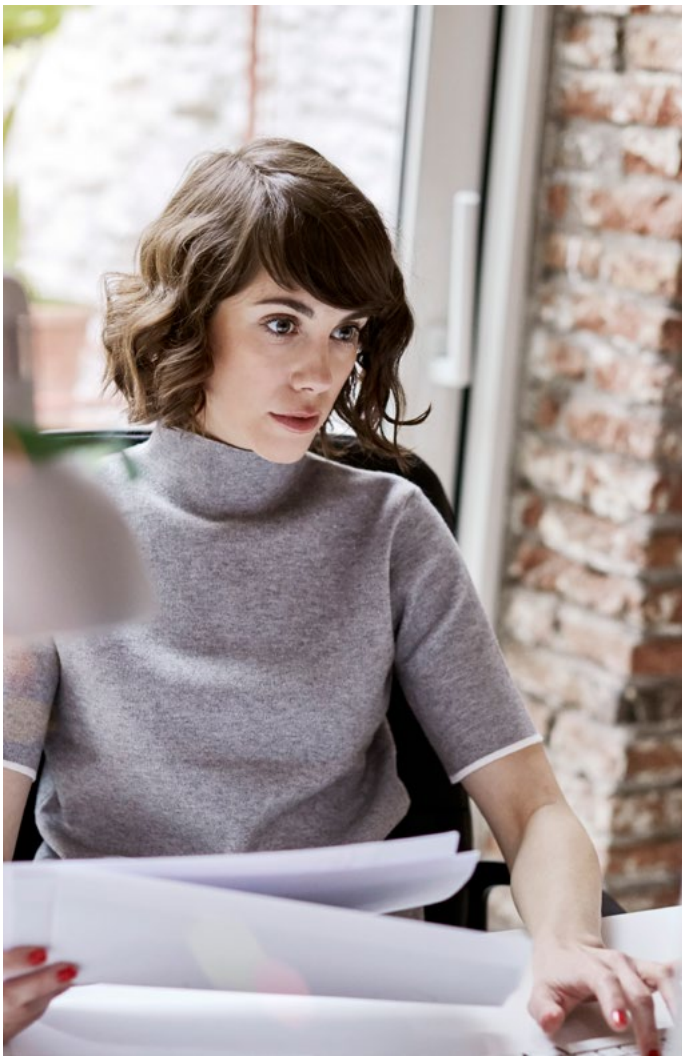
Versleutel gevoelige documenten

Versleutelen of encryptie is het proces van het coderen van de inhoud van een document, zodat alleen bevoegde personen met de juiste decryptiesleutel toegang hebben tot het document. Het gebruik van encryptietechnieken zoals Advanced Encryption Standard (AES) voegt een extra beveiligingslaag toe aan de inhoud van het document, zelfs als het in verkeerde handen valt.

Richtlijnen voor classificeren en labelen

Creëer tenslotte gedetailleerde richtlijnen voor het classificeren en labelen van documenten. Dit helpt bij het bepalen van het gevoeligheidsniveau van elk document en zorgt ervoor dat de juiste beveiligingsmaatregelen consequent worden toegepast. Informeer medewerkers goed over het belang van documentclassificatie en richtlijnen zodat ze gevoelige informatie op de juiste manier labelen en behandelen.

Door deze procedure vanaf het begin toe te passen, leg je een solide basis voor documentveiligheid. Onthoud dat hoe eerder je beveiligingsproblemen aanpakt, hoe beter je voorbereid bent om gevoelige informatie gedurende de hele levenscyclus te beschermen en hoe meer documentveiligheid de standaard wordt binnen je organisatie.



Opslag van documenten

Documenten worden over het algemeen gemaakt om informatie vast te leggen, te communiceren en te bewaren en zijn een essentiële onderdeel van ons persoonlijke en professionele leven. Met een document leggen we kennis, ideeën, feiten, instructies en andere vormen van informatie vast en dragen we die over.

De kans dat een document alleen voor eigen gebruik wordt gemaakt is relatief klein. Het is waarschijnlijker dat documenten en dus de informatie die daarin is opgenomen zullen worden gedeeld, bekeken, opgeslagen, aangepast, geprint en gedistribueerd.

De netwerkbeveiliging is bij de meeste organisaties redelijk op orde, dus je mag verwachten dat het veilig is om documenten hierin op te slaan. En wat is er dan makkelijker dan gebruik te maken van de bekende Windows-mappenstructuur.

Ondanks dat de opslag in Windows-mappen op zichzelf veilig kan zijn, zijn er een aantal overwegingen waarom deze beveiliging niet optimaal is.

Beperkte toegangscontrole

Windows-standaardmappen bieden beperkte opties voor toegangscontrole. Je kunt mappen beveiligen met wachtwoorden en machtigingen instellen. Niets meer en niets minder.

Voor alle andere wensen op het gebied van toegangscontrole kun je veel beter een document-managementoplossing gebruiken.

Hierbij kun je denken aan:

- Toegang tot bepaalde documenten, mappen of zelfs delen van documenten geven aan specifieke gebruikers of groepen
- Externe gebruikers veilig toegang geven tot specifieke documenten, zonder hen toegang te geven tot het volledige netwerk
- Integratie met bedrijfsapplicaties zoals CRM-systemen
- Veilige toegang tot informatie vanaf mobiele devices
- Het bijhouden van een audit trail, waarin wordt vastgelegd wie welke acties heeft uitgevoerd, zoals het bekijken, bewerken of verwijderen van specifieke documenten. Dit is van groot belang voor naleving van regelgeving.

Ontbrekende versleuteling

Windows-standaardmappen bieden geen automatische end-to-end-codering voor opgeslagen bestanden. Dit betekent dat als iemand toegang krijgt tot je computer of het netwerk waar het bestand is opgeslagen, deze persoon zonder al te veel moeite de inhoud van het bestand kan lezen.

Ontbrekende audit-trail

Het volgen van gebruikersactiviteit en het maken van gedetailleerde audittrails is nagenoeg niet aanwezig in de standaard Windows-mappen. Dit maakt het onmogelijk om bij te houden wie wanneer wat met een bepaald document heeft gedaan.

Nu lijkt het misschien niet zo belangrijk om te weten wie een document heeft opgeslagen of ingezien. Maar als het document persoonsgegevens bevat heeft de verwerker de plicht zich hiervoor te kunnen verantwoorden.

De Wet aanvullende bepalingen verwerking persoons-gegevens in de zorg (Wabvpz) bepaalt onder andere dat een patiënt bij een zorginstelling een overzicht kan opvragen, waarin is opgenomen wie wanneer bepaalde informatie beschikbaar heeft gemaakt en/of heeft ingezien. De zorginstelling is verplicht om gehoor te geven aan dit verzoek en zal dus geautomatiseerde registratie van gegevens, die bedoeld is om bij te houden welke gebeurtenissen/handelingen binnen een systeem hebben plaatsgevonden moeten toepassen.

Ongecontroleerd delen en samenwerken

Dit is een situatie die ontstaat als gebruikers documenten en bestanden delen zonder de nodige beveiligingsmaatregelen in acht te nemen. Dit kan gebeuren wanneer bestanden worden gekopieerd naar gedeelde netwerkmappen of cloudopslagdiensten zonder dat er duidelijke regels zijn voor wie toegang heeft tot welke bestanden en wat ze met die bestanden mogen doen.

7 belangrijkste aandachtspunten bij de opslag van documenten.

Ongeautoriseerde toegang
Als gebruikers documenten delen zonder toegangscontrole-mechanismen, kunnen ongeautoriseerde personen mogelijk toegang krijgen tot gevoelige informatie. Dit kan leiden tot datadiefstal, verlies van vertrouwelijkheid en juridische problemen.

Verlies van controle
Bij ongecontroleerde deling is het moeilijk om overzicht te houden over wie toegang heeft tot welke documenten en wat er met die documenten gebeurt. Dit kan leiden tot (onbedoelde) wijzigingen, verwijderingen of zelfs het verlies van belangrijke informatie.

Gebrek aan transparantie
Als documenten ongecontroleerd worden gedeeld, is het vaak moeilijk bij te houden wie welke acties heeft ondernomen. Dit maakt het lastig om verantwoordelijkheid toe te wijzen in het geval van problemen of fouten.

Beperkte samenwerkingsfuncties
Standaard Windows-mappen bieden mogelijk niet de uitgebreide samenwerkings-functies die nodig zijn om efficiënt en veilig met anderen samen te werken. Dit kan leiden tot versieconflicten, verwarring en inefficiëntie.

Nalevingsproblemen
Ongecontroleerde deling kan leiden tot het niet voldoen aan regelgeving voor gegevensbeheer en privacybescherming. Dit is in iedere sector een probleem maar weegt nog zwaarder in gereguleerde sectoren, zoals gezondheidszorg of financiële dienstverlening.

Opslaan en herstellen
Om na hardwarestoring, natuurramp, malwareaanval of andere calamiteit snel weer aan het werk te kunnen heb je reservekopieën van je documenten nodig. Werken met de Windows-mappenstructuur maakt het lastig om een efficiënte en betrouwbare back-upstrategie te implementeren.

Mobiele toegang
Er wordt tegenwoordig veel vaker op afstand gewerkt. Het is met Windows-mappen lastiger om vanaf mobiele apparaten toegang tot je digitale documenten en gegevens te krijgen, deze te bekijken, bewerken en beheren.

Hoe dan wel?

Documenten en informatie vormen de levensader van onze organisaties en maken het waarborgen van de veiligheid van onze documenten van cruciaal belang.

Het gebruik van een documentmanagementsysteem (DMS) is niet alleen een technologische keuze, maar ook een strategische investering in documentveiligheid, efficiëntie en naleving.

Een DMS is een complete softwareoplossing om informatie te beheren, bewaren en beschermen en biedt veel voordelen die rechtstreeks bijdragen aan het waarborgen van documentveiligheid en de bescherming van gevoelige en vertrouwelijke informatie. Daarnaast vereenvoudigt een DMS het samenwerken, ongeachte de locatie van je medewerkers.

De vijf belangrijkste voordelen van het gebruik van een DMS

Toegangscontrole en autorisatie

Uitgebreide toegangscontrole- en autorisatiemogelijkheden, waardoor je kunt bepalen wie welke documenten mag bekijken, bewerken en delen. Dit stelt beheerders in staat om specifieke gebruikersrechten toe te wijzen op basis van rollen, functies of individuele vereisten. Gevoelige documenten kunnen worden beveiligd tegen ongeoorloofde toegang door strikt gedefinieerde toegangsrechten toe te passen. Dit minimaliseert het risico van interne datalekken en beperkt het bereik van potentieel schadelijke activiteiten.

Versiebeheer en revisiegeschiedenis

Met een DMS beheer je eenvoudig en nauwkeurig verschillende versies en revisiegeschiedenis van documenten. Dit betekent dat elke wijziging in een document wordt vastgelegd, inclusief wie de wijziging heeft doorgevoerd en wanneer. Hierdoor kunnen eerdere versies worden hersteld, de integriteit van documenten worden behouden en onbedoelde wijzigingen kunnen worden teruggedraaid. Doordat er volledige transparantie in het wijzigingsproces is, verbetert een DMS de documentcontrole en vermindert het de kans op frauduleuze activiteiten.

Beveiliging tegen externe bedreigingen

Een DMS bevat geavanceerde beveiligingsfuncties die bescherming bieden tegen externe bedreigingen zoals malware, ransomware en hackingpogingen. Een DMS implementeert end-to-end encryptie om ervoor te zorgen dat de inhoud van documenten wordt beschermd tegen onderschepping en ongeoorloofde toegang, zelfs wanneer documenten worden verzonden via onveilige netwerken.

Het monitoren van inkomend en uitgaand verkeer helpt bij het identificeren van verdachte activiteiten, waardoor je proactief kan reageren op potentiële bedreigingen.

Naleving van regelgeving

Voor organisaties in sectoren met strenge regelgeving zoals gezondheidszorg, financiële en juridische dienstverlening, biedt een DMS mogelijkheden om te voldoen aan regelgevende vereisten. Een DMS stelt je in staat om gedetailleerde audit trails te genereren. Dit betekent dat alle activiteiten van gebruikers worden vastgelegd en bewaard. Dit is van cruciaal belang voor het aantonen van naleving aan externe instanties en voor het beheren van mogelijke juridische kwesties. Door nalevingsprotocollen te ondersteunen, minimaliseert een DMS het risico van boetes en reputatieschade.

Efficiëntie en samenwerking

Met een DMS kan er soepel samengewerkt worden door real-time bewerkingen en gedeelde toegang tot documenten mogelijk te maken. Dit minimaliseert de noodzaak om documenten via onveilige kanalen te delen, wat de kans op ongeautoriseerde toegang verkleint. Bovendien kunnen je medewerkers efficiënter werken, waardoor de kans op fouten en onbedoelde beveiligingsinbreuken wordt verminderd.

Door uitgebreide toegangscontrole, versiebeheer, bescherming tegen externe bedreigingen, de naleving van regelgeving en eenvoudig (samen)werken borgt een DMS waardevolle informatie, bedrijfscontinuïteit en helpt het je het vertrouwen van klanten en partners te behouden.

Aanvullende mogelijkheden van een DMS

- Digitale handtekeningen
- Tweefactorauthenticatie (2FA)
- Geavanceerde auditing en rapportage
- Geautomatiseerd retentiebeheer
- Externe delen en gasttoegang
- Geautomatiseerde veiligheidsupdates

Hoe zit dat met cloud?

We horen nog regelmatig het argument dat documentopslag in de cloud niet veilig is en daarom ongewenst. Vaak is gevoel gebaseerd op misvattingen of onbekendheid met moderne cloudbeveiligingspraktijken. We hebben de meest voorkomende redenen om niet voor cloud te willen kiezen op een rij gezet.

Misvattingen over fysieke beveiliging

Vaak leeft het idee dat het opslaan van gegevens in een fysieke, lokale omgeving veiliger is dan in de cloud. Organisaties voelen zich ongemakkelijk bij het idee dat hun gegevens zich buiten hun directe controle bevinden.

Dit is een misvatting omdat cloudproviders technologisch vooruitstevende beveiliging bieden in hun datacenters, met fysieke beveiligingslagen die de meeste organisaties zelf niet kunnen evenaren.

Gebrek aan vertrouwen in derden

Men is sceptisch over de mate waarin cloudproviders hun gegevens veilig kunnen houden. Het is belangrijk om te begrijpen dat het bestaansrecht van cloudproviders hun uitgebreide beveiligingsmaatregelen en nalevings-certificeringen zijn om de veiligheid van gegevens te kunnen waarborgen.

Beïnvloeding door berichtgeving

Nieuwsberichten over incidenten met gegevenslekken of beveiligingsinbreuken kan bijdragen aan het gevoel dat documentmanagement in de cloud onveilig is. Hoewel incidenten kunnen voorkomen, moeten deze worden gezien als uitzonderingen en niet als de norm. Het is belangrijk om te begrijpen dat juist traditionele on-premise systemen niet immuun zijn voor beveiligingsproblemen.

Onbekendheid met beveiligingspraktijken

De onbekendheid met moderne cloudbeveiliging kan leiden tot onzekerheid over de veiligheid van gegevens in de cloud. De toegevoegde waarde van encryptie, tweefactorauthenticatie, geavanceerde toegangscontrole en andere beveiligingsmaatregelen die cloudproviders implementeren zijn het bewijs dat de veiligheid gewaarborgd is.

Angst voor gegevensverlies

We maken ons zorgen over het verlies van gegevens of dat we geen toegang meer tot onze documenten kunnen krijgen als de cloudprovider een fout maakt. Deze zorgen zijn heel begrijpelijk dus het is goed om te weten dat cloudproviders redundantie en back-upmechanismen geïmplementeerd hebben om gegevensbehoud en beschikbaarheid te garanderen.

Onbekendheid met wet- en regelgeving

In sommige sectoren, zoals de gezondheidszorg of financiële dienstverlening, kunnen er specifieke zorgen zijn voor het gebruik van cloudoplossingen. Hierdoor kan een onterecht gevoel van onveiligheid ontstaan. Cloudproviders hebben hiervoor namelijk nalevingscertificeringen en moeten aan strenge beveiligingsnormen voldoen.

Behoefte aan eigen controle

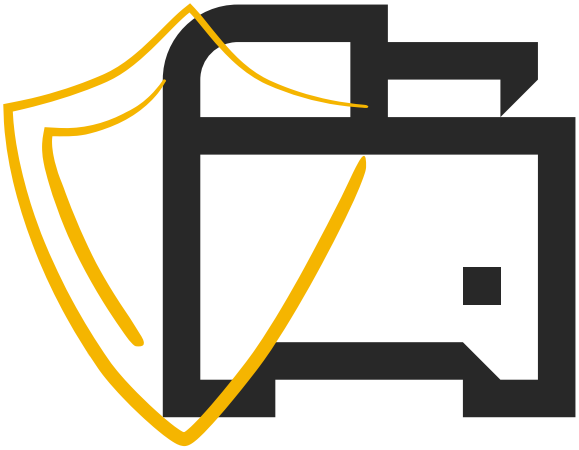
Vaak voelt een organisatie zich comfortabeler met het hebben van volledige controle over de eigen fysieke infrastructuur. Het uitbesteden van beveiliging aan een derde partij kan als ongemakkelijk worden ervaren, zelfs als deze partij beschikt over gespecialiseerde beveiligingsexpertise en -middelen.

Het is goed om deze zorgen serieus te nemen en tegelijkertijd te erkennen dat documentveiligheid in de cloud gewaarborgd wordt door fysieke beveiliging van datacenters, gegevensencryptie, toegangscontrole, tweefactorauthenticatie, regelmatige beveiligingsupdates, naleving van regelgeving, redundantie en back-ups, evenals beveiligingscertificeringen. Dit alles vormt een solide beveiliging die documenten tegen ongeautoriseerde toegang, gegevensverlies en andere bedreigingen beschermen.

Printen

Hoewel digitale technologieën en documentmanagementsystemen aanzienlijke vooruitgang hebben geboekt, blijft het printen van documenten voorlopig een normale activiteit in de meeste organisaties. Medewerkers hebben op bepaalde momenten nog steeds behoefte aan tastbare documenten. Je kan hierbij denken aan een papieren document zoals een contract, om het al dan niet te kunnen voorzien van een "natte" handtekening, het maken van notities tijdens controle- en goedkeuringsprocessen of het delen van informatie in een teambespreking.

Wanneer er geprint wordt zijn er potentiële risico's, in verband met informatiebeveiliging en privacy, die belangrijk genoeg zijn om aandacht aan te besteden.



Geprinte documenten in de uitvoerlade
Als een medewerker gevoelige informatie zoals financiële rapporten, juridische documenten of personeelsinformatie afdrukt en ze niet direct ophaalt bij de printer, kan de informatie gemakkelijk in verkeerde handen vallen en leiden tot gegevenslekken.

Verlies of vergeten documenten
Het wordt nog wel eens vergeten om geprinte documenten op te halen bij de printer. Dit verhoogt het risico dat onbevoegde personen toegang krijgen tot deze informatie. Dit is een onwenselijke situatie, vooral als het om vertrouwelijke documenten gaat.

Onbeheerde printopdrachten
Als er geen beheer en controle is over printopdrachten, kunnen medewerkers per ongeluk de verkeerde afdrukken meenemen.

Onbeveiligde toegang tot printers
Wanneer de fysieke toegang tot de printer niet wordt beperkt kan dit leiden tot ongeautoriseerde afdrukken en toegang tot documenten.

Onveilige opslag van printopdrachten
Printopdrachten worden soms op de printer opgeslagen voordat ze worden afgedrukt. Als deze opdrachten niet worden versleuteld of verwijderd, kunnen ze worden ingezien door onbevoegde personen.

Datalekken via geheugen van printer
Printers hebben vaak een intern geheugen waarin kopieën van afgedrukte documenten kunnen worden opgeslagen. Als deze gegevens niet regelmatig worden gewist, kan dit leiden tot onbedoelde gegevensblootstelling.

Ongeautoriseerde afdrukken
Medewerkers kunnen mogelijk gevoelige documenten afdrukken zonder de juiste toestemming of goedkeuring. Dit kan leiden tot het onbedoeld delen van vertrouwelijke informatie.

Met het ontwikkelen van beveiligingsfuncties blijven we werken aan een producten die meer veiligheid bieden bij het gebruik van Kyocera's MFP's en printers.

Malware en hacks
Printers zijn verbonden met netwerken en kunnen kwetsbaar zijn voor malware-aanvallen of hacks. Een onveilige printer kan worden misbruikt als toegangspunt tot bedrijfsnetwerken.

Onveilige verwijdering van geprinte documenten
Als afgedrukte documenten niet op een veilige manier worden vernietigd, kunnen ze uit de prullenbak worden opgepikt door onbevoegde personen.

Deze punten zijn zowel van technologische als organisatorische aard en dus zal om de veiligheid rond printers te waarborgen op beide vlakken een veilige situatie moeten worden gecreëerd.

Op het gebied van de print hardware zelf wordt al vele jaren gewerkt aan het creëren van veilige printers en multifunctionals. Zo kunnen we onze hardware rekenen tot de veiligste in de markt.

Met uiteraard de standaard beveiligingen als vertrouwelijk printen, encryptie en verwijdering van verwerkte data op de machine, ondersteuning van alle gangbare veiligheidsprotocollen.

Maar daarnaast wordt veel aandacht gegeven aan het bereiken van de zo veilig mogelijke machine.

7 beveiligingskenmerken van printers en MFP's

Vertrouwelijkheid
Informatie die wordt verwerkt door de MFP mag niet bij derden terechtkomen.

Integriteit
Informatie mag niet worden gewijzigd, deze moet accuraat en correct zijn.

Beschikbaarheid
Informatie moet onmiddellijk toegankelijk zijn voor geautoriseerde gebruikers, met behoud van vertrouwelijkheid en integriteit.

Authenticiteit
De juistheid van de auteur of de eigenaar van de informatie kan worden gevalideerd.

Verantwoording
De geschiedenis van gebruikers- en beheerdersbewerkingen en de geschiedenis van het gedrag van de MFP kunnen worden gevolgd.

Onweerlegbaarheid
Door de afzender te verifiëren (authenticatie) en ervoor te zorgen dat de gegevens tijdens de overdracht niet zijn onderschept of gewijzigd (integriteit) kan de legitimiteit van de gegevens worden bevestigd.

Betrouwbaarheid
De MFP is op het gebied van document-veiligheid altijd beschikbaar in de meest veilige staat.

Veiligheidsmaatregelen

S/MIME
Secure/Multipurpose Internet Mail Extensions

Wanneer multifunctionals e-mails als platte tekst verzenden, kunnen ze door iedereen worden gelezen. Met Secure/Multipurpose Internet Mail Extensions (S/MIME) kunnen gebruikers hun e-mails versleutelen en digitaal ondertekenen. Bij versleuteling wordt de openbare sleutel van de ontvanger gebruikt en is de privésleutel van de ontvanger nodig om het bericht te ontsleutelen en te lezen. Digitale handtekeningen verifiëren de authenticiteit en integriteit van het bericht.

Het gebruik van S/MIME werkt als het plaatsen van tekst in een ondoordringbare virtuele envelop. Elke poging om deze envelop te verwisselen met een envelop met een andere inhoud is detecteerbaar. Bij integratie in multifunctionele apparaten versleutelt S/MIME berichten met de openbare sleutel van de ontvanger van een Public Key Infrastructure (PKI), zodat alleen de ontvanger de berichten kan ontsleutelen en lezen.

Bovendien maakt S/MIME het mogelijk om berichten digitaal te ondertekenen met je privésleutel, waardoor je identiteit als afzender en de ongewijzigde status van het bericht worden bevestigd. Met technologie kunnen apparaten e-mails versleutelen en ondertekenen binnen een PKI-raamwerk, waardoor de communicatiebeveiliging van klanten wordt verbeterd.

Resultaat
Het gebruik van S/MIME resulteert in een verhoogde gegevensbeveiliging door het verzenden van versleutelde berichten te vergemakkelijken.

Voordelen
Deze aanpak minimaliseert het risico op gegevens-blootstelling en mogelijke boetes door de kans op ongeautoriseerde toegang tot gevoelige informatie te verkleinen.

SCEP
Simple Certificate Enrolment Protocol

Een belangrijke verbetering die multifunctionele printers (MFP's) in staat stelt automatisch certificaten te verkrijgen van een certificeringsinstantie (CA). Voorheen was het bijwerken van certificaten voor elk apparaat een arbeidsintensief proces waarbij handmatig moest worden ingegrepen wanneer certificaten verliepen of nieuwe apparaten werden geïnstalleerd. SCEP revolutioneert dit proces echter.

Het nieuwe SCEP-gestuurde proces stroomlijnt de inspanning die van beheerders wordt gevraagd drastisch. Na initiatie en bevestiging verloopt de hele taak zelfstandig, waarbij alle communicatie automatisch en zonder interactie van de beheerder plaatsvindt. Zelfs het initiëren van het proces kan geautomatiseerd worden indien gewenst.

Resultaat
De implementatie van SCEP leidt tot het automatisch ophalen van officiële certificaten. Dankzij deze automatisering kan IT-personeel zich richten op andere essentiële IT-beveiligingstaken.

Voordelen
De invoering van SCEP leidt tot tijdsbesparing en lagere IT-kosten. De automatisering van het ophalen en installeren van certificaten draagt bij aan een efficiëntere bedrijfsvoering, waardoor organisaties hun middelen effectiever kunnen inzetten.

OCSP/CRL

Online Certificate Status Protocol/Certificate Revocation

De OCSP/CRL-instellingen bieden een mechanisme om de geldigheid te controleren van certificaten die worden gebruikt in cryptografische communicatie. Net als een identiteitskaart met een bepaalde geldigheidsperiode, kunnen certificaten ook ongeldig worden door intrekking. CRL's (Certificate Revocation Lists) dienen om deze ingetrokken certificaten op te sommen. Het handmatig controleren van certificaten aan de hand van CRL's is echter tijdrovend en arbeidsintensief. Het regelmatig plannen en uitvoeren van dergelijke controles voor alle beschikbare certificaten is onpraktisch en CRL's kunnen vaak verouderd zijn, wat leidt tot onzekerheid over de geldigheid van certificaten.

Wanneer een MFP verbinding maakt met internetdiensten zoals bijvoorbeeld HTTPS, wordt meestal de geldigheidsperiode van certificaten gevalideerd. De machine voert meestal geen controles uit aan de hand van CRL's vanwege hun onbetrouwbare nauwkeurigheid.

De introductie van OCSP (Online Certificate Status Protocol) en CRL-instellingen verandert dit. Deze beveiligingsfunctie doet rechtstreeks navraag bij de certificeringsinstantie om de status van het certificaat te bepalen. OCSP-servers antwoorden met 'Goed', 'Ingetrokken' of 'Onbekend' voor de gevraagde certificaatstatus. Dit stelt gebruikers in staat om geïnformeerde beslissingen te nemen over het vertrouwen van gepresenteerde certificaten zonder onduidelijkheid.

Resultaat

De toepassing van OCSP/CRL-instellingen leidt tot geautomatiseerde controles van de geldigheid van certificaten. Hierdoor kunnen IT-teams hun inspanningen richten op andere cruciale IT-beveiligingstaken.

Voordelen

Deze implementatie bespaart tijd en verlaagt de IT-kosten door het proces van het controleren van certificaten te automatiseren. De betrouwbaarheid van certificaatstatuscontroles wordt verbeterd, waardoor de onzekerheid, veroorzaakt door verouderde CRL's, wordt weggenomen en de betrouwbaarheid van certificaten die worden gebruikt in cryptografische bewerkingen wordt gegarandeerd.

TLS version 1.3 ondersteuning

Encryptie is van vitaal belang om internetcommunicatie te beveiligen, net als wanneer je een website opent via HTTPS, dat HTTP binnen TLS gebruikt. Hoewel deze technologie al een tijdje bestaat, is er veel vooruitgang geboekt. In tegenstelling tot andere aanbieders, die nog steeds vertrouwen op TLS 1.2, bieden wij de nieuwste en veiligste communicatieprotocollen

De belangrijkste verbeteringen van TLS 1.3 zijn:

- Verwijdering van de zwakke functies in TLS 1.2
- Verplichte digitale handtekeningen, zelfs voor bekende configuraties
- Introductie van Perfect Forward Security, waardoor de beveiliging wordt verbeterd
- Verwijdering van onveilige of verouderde functies
- SSL of RC4 onderhandeling niet toestaan om compatibiliteitsredenen
- Introductie van een sessie hash voor extra beveiliging
- Ondersteuning voor meerdere OCSP-antwoorden
- Encryptie van de handshake tijdens het opstarten van de encryptie
- Toevoeging van moderne, veilige sleuteluitwisselingsprotocollen die niet beschikbaar waren in versie 1.2
- Nieuwe digitale handtekening algoritmen

Resultaat

Onze ondersteuning voor het nieuwste coderings-netwerkprotocol leidt tot een betere beveiliging van de communicatie.

Voordelen

Deze vooruitgang minimaliseert het risico op gegevensblootstelling en boetes in verband met inbreuken op de beveiliging. De nieuwste encryptietechnologie zorgt voor een betere bescherming van gevoelige informatie.

Security Information and Event Management (SIEM) Support

Het systeem voor het bijhouden van auditlogs, dat gebruik maakt van het Syslog-protocol, verbetert de beveiligingsmonitoring door het eenvoudig opsporen van onbevoegde handelingen mogelijk te maken. Deze mogelijkheid is uitgebreid door de implementatie van SIEM (Security Information and Event Management), die de bestaande audit logfunctie uitbreidt.

Door deze opzet worden details zoals aanmeldtijden, gebruikers en uitgevoerde acties op multifunctionele printers (MFP's) vastgelegd en doorgestuurd naar een externe server. Hierdoor kunnen klanten security event logs centraal beheren vanuit het perspectief van de server.

SIEM is een beveiligingsconcept, dit houdt in dat gegevens van netwerkapparaten worden verzameld voor gecentraliseerde evaluatie. Ongebruikelijke activiteiten, die kunnen wijzen op potentiële aanvallen of bedreigingen, worden gevisualiseerd en gecommuniceerd naar beheerders. Dit proces maakt vaak gebruik van machine learning en kunstmatige intelligentie voor geavanceerde analyse.

In tegenstelling tot handmatige beoordeling, voert SIEM-software, aangeboden door gespecialiseerde beveiligingsbedrijven (niet Kyocera), real-time analyses uit. Bekende voorbeelden zijn IBM QRadar, Splunk en HPE ArcSight. Gegevens van verschillende netwerkapparaten worden verzameld, wat tijd en moeite bespaart doordat de analyse wordt geautomatiseerd in plaats van handmatig moet worden beoordeeld.

Resultaat

Het systeem levert realtime analyse van beveiligings-waarschuwingen, waardoor ongeoorloofde activiteiten op de juiste manier kunnen worden geregistreerd en gemonitord.

Voordelen

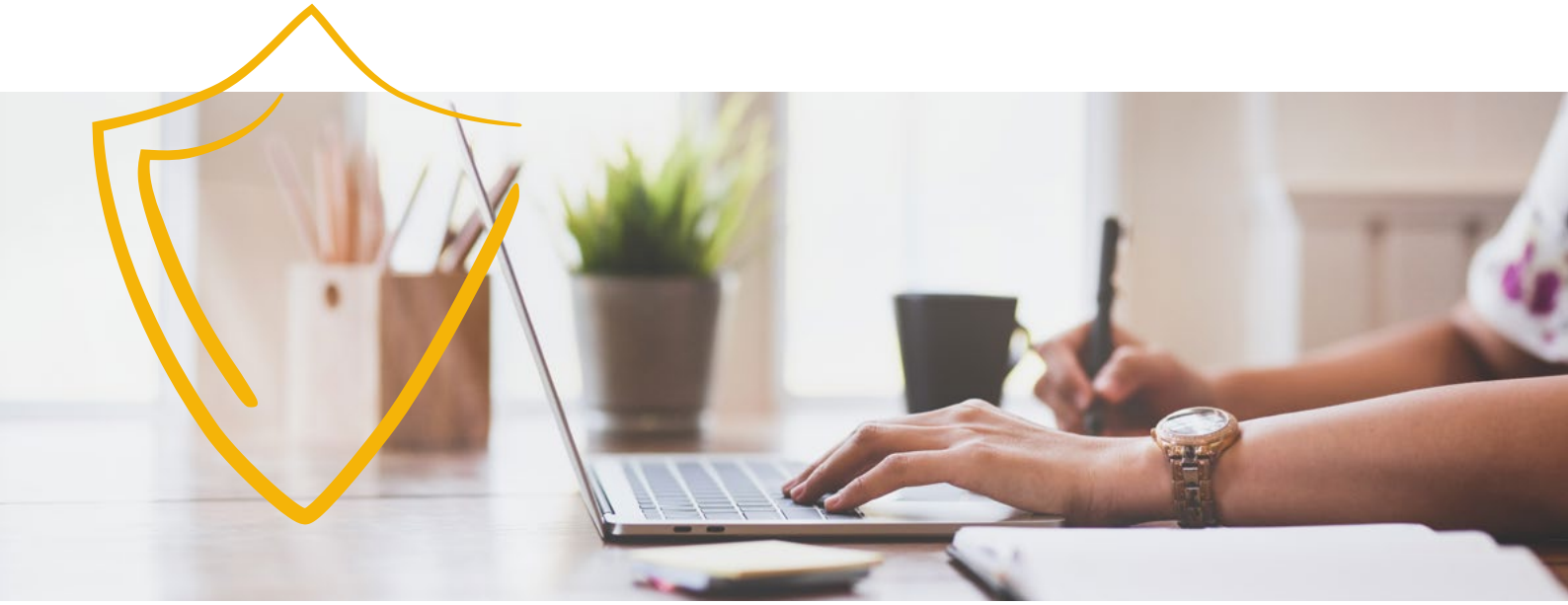
SIEM zorgt voor effectieve monitoring, beheer van gebruikersrechten, log auditing, reactie op incidenten en potentiële risicovermindering. Door de analyse en reactie te automatiseren, wordt de kans op gegevensblootstelling en boetes als gevolg van beveiligingslekken geminimaliseerd.

De gebruiker

Aan de hardware zal het niet liggen en als er iets fout gaat zal het hoogstwaarschijnlijk een typisch geval zijn van “The butler did it”. Het is daarom van belang om een duidelijk beleid af te spreken van wat en hoe er wordt geprint. Wie er toegang heeft tot welke machines en welke documenten, hoe er wordt geprint en gescand.

De standaardmogelijkheden van hardware leveren op zichzelf voldoende veiligheid maar zijn vaak omslachtig in beheer en gebruiksvriendelijkheid. Daarnaast leveren ze de gebruiker vaak voor de organisatie ongewenste vrijheden en blijft de foutkans aanzienlijk. Het gebruik van een printmanagementsysteem helpt je deze beleidsafspraken te stroomlijnen en af te dwingen.

Op de juiste manier geïmplementeerd, verbetert printmanagementsoftware het vermogen van je bedrijf om de nieuwe technologische functionaliteiten van de MFP te beheren. Je kunt op een kosteneffectieve manier de beveiliging van de workflow verbeteren vanaf een individueel werkstation tot aan de afgedrukte documenten die buiten de bedrijfsmuren komen.



Beveiliging is touwtrekken in drie richtingen

Er is niet één enkele "one-size fits all" beveiligingsinstelling. Als een organisatie haar beveiligings- en privacybeleid opstelt, is er altijd een strijd in drie richtingen over hoe deze instellingen gedaan kunnen worden.

De drie primaire gebruikersgroepen en perspectieven:

- De eindgebruikers/landelijke wetgeving zoals AVG/GDPR, die een hoog niveau van individuele privacy van gegevens vereisen
- De beheerder die de afdrukomgeving moet beveiligen tegen externe bedreigingen
- De organisatie die de afdrukomgeving wil kunnen controleren om misbruik te voorkomen

Privacy van gebruikers beveiligen

Drie basismaatregelen zijn essentieel in elke printomgeving, ongeacht of men de beveiliging bekijkt vanuit het perspectief van het individu, de beheerder of het bedrijf.

1. De beveiligde printfunctie zorgt ervoor dat de gebruiker volledige controle heeft over wanneer en waar zijn documenten worden geprint.

2. Gesloten gebruikerssessies moeten zowel gebruikers-authenticatie als automatisch afmelden omvatten.

3. Printbestanden moeten worden opgeslagen op een beveiligde plaats op de printserver.

Naast deze basisbeveiligingsopties zijn er aanvullende functies die de privacy van de gebruiker kunnen verhogen. Om de toegang tot geprinte documenten te voorkomen, kunnen privéwachtrijen worden gecreëerd waaruit opdrachten direct worden verwijderd nadat ze zijn geprint. Zo wordt voorkomen dat iemand anders dan de gebruiker de inhoud en naam van het afgedrukte bestand kan inzien.

AVG-compliant

Printmanagement draagt bij aan een AVG-compliant printomgeving en heeft de nodige stappen geïmplementeerd om ervoor te zorgen dat alle rechten van gebruikers die door de verordening worden gegeven zijn beveiligd. Denk hierbij aan de optie om gebruikers te voorzien van al hun gegevens, de optie om gebruikersaccounts te anonimiseren en informatie die gebruikers informeert over hun rechten.

Beveiligd printen

Het belang van een centraal printmanagementsysteem is toegenomen met de verschuiving van kleine desktopprinters naar gecentraliseerde multifunctionele printapparaten.

Het beheren van de toegang tot documenten op het moment dat ze uit de printer komen is een essentieel en basiselement in de beveiliging van de workflow.

De Secure Print-functie geeft verzonden taken pas vrij nadat de gebruiker bij de MFP is aangekomen en zich heeft geautoriseerd met een ID-kaart, PIN-code of gebruikersnaam en wachtwoord. Dit betekent dat de printopdracht alleen wordt geproduceerd met volledige fysieke controle van de geautoriseerde persoon, waardoor wordt voorkomen dat materiaal per ongeluk of express wordt opgehaald of ingezien door onbevoegden.

Aanmelden/afmelden

Het vereisen van gebruikersautorisatie op de MFP verbetert, naast het mogelijk maken van het vrijgeven van printopdrachten, de beveiliging van kopiëren en scannen.

Dit is van belang wanneer een gebruiker bijvoorbeeld een gevoelig document kopieert en de MFP zonder papier komt te zitten of een storing krijgt.
Een deel van het document bevindt zich nog in het geheugen van de MFP en zal worden geprint zodra iemand papier bijvult of de storing oplost.
Dit kan eenvoudig worden verholpen als de gebruiker uitlogt, het geheugen zal dan ook automatisch worden gewist.

Automatisch uitloggen op de MFP is op sowieso een belangrijke beveiligingsfunctie. Onderzoek toont aan dat de menselijke factor vaak de zwakste schakel in de beveiligingsketen is. Hoewel gebruikers worden geïnstrueerd om altijd uit te loggen, is de kans aanwezig dat ze dit niet doen en de MFP ingelogd achterlaten. Met alle risico's van dien.

Documentbeveiliging

Alle printbestanden die worden opgeslagen op de printserver moeten versleuteld worden opgeslagen. Daarnaast moet worden ingesteld hoe lang opdrachten op de server bewaard moeten blijven als de gebruiker ze niet ophaalt. Na het verstrijken van deze termijn worden de bestanden automatisch verwijderd en wordt het risico op ongeautoriseerde toegang nog verder geminimaliseerd.

Scannen

Ervoor zorgen dat gebruikers alleen kunnen scannen naar hun eigen mailadres en persoonlijke folder voorkomt het per ongeluk of moedwillig verzenden van informatie naar buiten de organisatie direct vanaf de MFP.

Zodra documenten naar buiten zijn verzonden ben je de controle en het inzicht kwijt. Dit kan leiden tot verlies van gevoelige informatie of zelfs juridische problemen als documenten onbedoeld worden verspreid.

Conclusie

Deze whitepaper heeft laten zien hoe belangrijk documentbeveiliging is in de hedendaagse digitale wereld. We hebben stap voor stap bekeken hoe we onze digitale informatie kunnen beschermen, vanaf het allereerste moment van documentcreatie tot het moment waarop we ze in het archief plaatsen.

Het is niet langer een keuze, maar een absolute noodzaak om documentbeveiliging serieus te nemen. Onze documenten bevatten vaak gevoelige en waardevolle informatie, van persoonlijke gegevens tot bedrijfskritische data. Deze moeten worden beschermd tegen ongeoorloofde toegang en mogelijke bedreigingen.

We hebben besproken dat het creëren van een veilige werkomgeving, het implementeren van sterke authenticatie- en wachtwoordbeleidsregels, het versleutelen van gevoelige documenten en het volgen van heldere classificatie- en labelingrichtlijnen essentieel zijn voor een solide documentbeveiligingsprogramma.

Daarnaast hebben we benadrukt dat documentbeveiliging niet alleen een technische aangelegenheid is, maar ook draait om het opbouwen van vertrouwen. Door verantwoord om te gaan met onze eigen documenten en die van anderen, winnen we het vertrouwen van klanten, zakenpartners en medewerkers.

Het is aan ons allemaal om deze kennis en inzichten toe te passen. We moeten digitale documenten gedurende hun hele levenscyclus actief beschermen. Hierdoor kunnen we profiteren van de voordelen van digitale samenwerking en informatie-uitwisseling, zonder dat dit ten koste gaat van de veiligheid.

Onthoud dat documentbeveiliging niet alleen een verplichting is, maar ook een kans om te laten zien dat je als organisatie maatregelen neemt om waardevolle informatie te beschermen. Het is een investering in het verdienen en bestendigen van vertrouwen en het waarborgen van veiligheid in de digitale wereld.

KYOCERA Document Solutions is sinds 1934 pionier op het gebied van innovatieve technologie. We helpen onze klanten om informatie om te zetten in kennis en daarmee concurrentievoordeel te behalen.

KYOCERA Document Solutions Nederland B.V.
Beechavenue 25, 1119 RA Schiphol-Rijk
Tel 020 587 72 00

KYOCERA

kyoceradocumentsolutions.nl