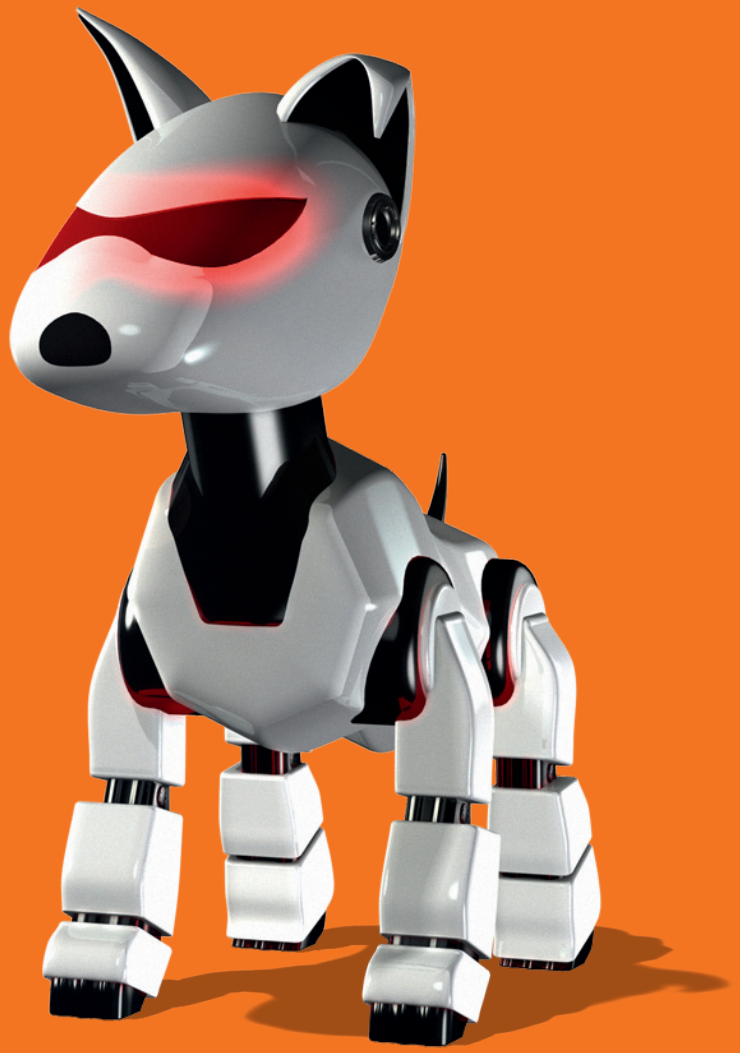
DE TOSHIBA GIDS OVER MFP-BEVEILIGING

SE SECURITY ENHANCED
Powerful Protection for Sensitive Data



TOSHIBA
Leading Innovation >>>

DE TOSHIBA'S GIDS OVER MFP-BEVEILIGING

www.toshibatec.nl

INLEIDING TOT MFP-BEVEILIGING

SE SECURITY ENHANCED
Powerful Protection for Sensitive Data

Is uw beveiligings-beleid wel com-pleet?

Hoewel de meeste organisaties hun IT-netwerken afdoende beveiligen, wordt relatief weinig aandacht besteed aan multifunctionele systemen (MFP's). Ten onrechte, want een onvoldoende beveiligde MFP levert vergelijkbare bedrijfsbrede risico's op. Via MFP's werken mensen immers ook met gevoelige informatie. Het onvoldoende beveiligen van deze gegevens kan bovendien juridische consequenties hebben.

Veilig printen… weet u het zeker?

Een MFP voor het scannen, printen, faxen en kopiëren van documenten is meer dan een krachtig hulpmiddel voor op kantoor. Het is een geavanceerd systeem, met vaak een harde schijf, een webserver en een eigen IP-adres. Bijna altijd is de MFP onderdeel van een bedrijfsmatig informatienetwerk.

Het is dan ook van groot belang om bewust te zijn van de veiligheidsrisico's van MFP's, waaronder misbruik door onbevoegden. Denk alleen maar aan het document met vertrouwelijke informatie dat na het printen blijft liggen, zodat iedereen het kan lezen of meenemen. Met andere woorden: als MFP's geen deel uitmaken van uw beveiligingsbeleid, kan gevoelige informatie gemakkelijk in verkeerde handen komen.

Wees bewust van de risico's van MFP's

Uit onderzoek van Forrester (Global IT Budgets, Priorities and Emerging Technology Tracking Survey) blijkt dat IT-beveiliging voor bedrijven een hoge zakelijke prioriteit heeft. Dat is op zichzelf toe te juichen. Toch blijkt dat de bewustwording over de risico's van MFP's nog vaak onvoldoende is. Veel organisaties lijken nog niet te beseffen dat de onschuldige kopieermachines van weleer zich hebben ontwikkeld tot veelzijdige en krachtige kantoorsystemen, die integraal deel uitmaken van geavanceerde informatienetwerken.

MOET U ZICH ZORGEN MAKEN?

SE SECURITY ENHANCED
Powerful Protection for Sensitive Data

Doet u alles wat mogelijk is?

Dagelijks worden ook in uw organisatie de meest uiteenlopende documenten gekopieerd, geprint, gefaxt of gescand: van persoonlijke informatie, vertrouwelijke rapporten, e-mails en memo's tot financiële overzichten, klantgegevens, personeelsdossiers en nog veel meer.

Misbruik en diefstal van informatie zijn ongewenste, maar steeds vaker voorkomende aspecten van de moderne maatschappij. Wie met gevoelige informatie werkt, moet daar alert op zijn. De overheid stelt er dan ook eisen aan, bijvoorbeeld via de Wet bescherming persoonsgegevens (Wbp). Organisaties moeten kunnen garanderen dat de vertrouwelijke informatie in hun systemen vertrouwelijk blijft. Daar hoort dus ook de beveiliging van MFP's bij.

Een onvoldoende beveiliging van persoonlijke en vertrouwelijke informatie kan sancties en materiële schade opleveren. Maar nog erger is vaak de reputatieschade die een organisatie oploopt, als blijkt dat onzorgvuldig wordt omgegaan met informatie.

Gevaren van binnen de organisatie

Gevaren die de MFP-integriteit bedreigen, komen niet alleen van buiten de organisatie. Een risico van binnenuit is het gemak waarmee vertrouwelijke informatie kan worden gekopieerd vanaf documenten die op de harde schijf van de MFP staan.

Een ander voorbeeld is de ontoereikende beveiliging van informatie op een desktopcomputer of op een computer die toegankelijk is via het lokale netwerk. Deze informatie is daardoor niet alleen eenvoudig te bekijken, maar ook op een aangesloten MFP af te drukken.

Informatie op de harde schijf

Een belangrijk aandachtspunt betreft de beveiliging van MFP's die retour gaan naar de leverancier. Hoe weet u zeker dat alle informatie op de harde schijf is verwijderd? Wees er altijd bedacht op dat uw oude MFP in handen kan vallen van hackers die oneigenlijk gebruik kunnen maken van de opgeslagen data op de harde schijf.

Hoe gemakkelijk dat is, bewijst een filmpje op YouTube. Een korte CBS-documentaire van vijf minuten laat zien hoe een verslaggever en een beveiligingsspecialist drie MFP's uit een magazijn halen. Met behulp van software die vrij via internet verkrijgbaar is, kunnen zij gevoelige informatie op de harde schijf inzien, waaronder medische dossiers en politierapporten.

Deze video bekijken? Ga naar http://www.youtube.com/watch?v=iC38D5am7go

ZAKELIJKE VOORDELEN

SE SECURITY ENHANCED
Powerful Protection for Sensitive Data

Vijf punten om snel te scoren

1. Implementeer een eenvoudige op rolgebaseerde procedure voor het gebruiken en printen van documenten, zodanig dat alleen de auteur printopdrachten kan inzien.
2. Ga alleen in zee met een leverancier die gestandaardiseerde procedures hanteert voor de beveiliging van ingenomen MFP's, waaronder het wissen van de harde schijf.
3. Wees bij aanschaf van nieuwe MFP's kritisch welk type harde schijf de MFP bevat en hoe de beveiliging van data is geregeld.
4. Maak waar mogelijk gebruik van processen die de data op de harde schijf van de MFP standaard overschrijven. Dit draagt bij aan een beter beleid voor gegevensbeveiliging, beperkt de risico's en voorkomt grote financiële schade.
5. Houd de huidige infrastructuur en het gebruik van technologieën als cloud computing tegen het licht. Raadpleeg een betrouwbare leverancier, omdat de beveiliging daar vaak verder gaat dan die van de eigen organisatie.

De noodzaak van een integrale aanpak

Het onderkennen en aanpakken van de risico's van MFP's is een belangrijk begin van uw beveiligingsbeleid. Maatregelen, zoals het automatisch overschrijven of versleutelen van data op de harde schijf, zijn daarvan vaak een onderdeel. Helaas kunnen daardoor, afhankelijk van de leverancier, de systeemprestaties afnemen. Een andere manier is het onbruikbaar maken van de data bij retour van het systeem naar de leverancier.

Hoe dan ook, het is van belang om de aspecten van gegevensbeveiliging niet afzonderlijk te bezien, maar in hun samenhang. Het implementeren van een integrale aanpak voor de gehele levensduur van een document is noodzakelijk: vanaf de documentaanmaak tot het gebruik en de vernietiging ervan.

Strategie voor documentbeveiliging

De implementatie van een gerichte strategie voor documentbeveiliging brengt dus vooral zakelijk voordeel met zich mee. Van de andere kant levert niets doen alleen maar risico's op.

Het is duidelijk dat u blootgesteld kunt worden aan grote zakelijke risico's als vertrouwelijke gegevens in verkeerde handen vallen. Maar denk ook aan de sancties van overheid en verzekeraars, of van consumenten- en brancheorganisaties, als blijkt dat u zich onvoldoende houdt aan het toenemend aantal wetten en regels die gelden voor de beveiliging van informatie.

EEN ALLESOMVATTENDE AANPAK

SE SECURITY ENHANCED
Powerful Protection for Sensitive Data

Kom in actie

De afgelopen tien jaar is de technologie van MFP's sterk doorontwikkeld. Toch bestaat er nog veel onbegrip en onwetendheid over. MFP's maken integraal deel uit van de IT-infrastructuur in elke kantooromgeving en verdienen daarom een prominente plaats in uw beveiligingsbeleid.

Wie niet de juiste beveiligingsmaatregelen implementeert en in de praktijk handhaaft, moet rekening houden met rampzalige gevolgen. Bereid u dus nu voor. Tegen de tijd dat u merkt dat uw bedrijfsdata in gevaar zijn gebracht, is het meestal al te laat.

Wij helpen u graag

Toshiba TEC heeft voor zijn MFP's een speciale harde schijf ontwikkeld met Wipe-technologie om data te versleutelen en onleesbaar te maken als de harde schijf wordt verwijderd. Daardoor zijn deze systemen bij uitstek geschikt voor organisaties die de beveiliging van vertrouwelijke informatie een hoge prioriteit geven.

De gegevens op deze beveiligde Toshiba harde schijf worden vrijwel in real time gecodeerd met een 256-bit-algoritme, waardoor authenticatie door de desbetreffende MFP nodig is om de gegevens van de harde schijf te gebruiken. Wordt de harde schijf verwijderd om op een ander systeem te worden aangesloten, dan worden de data automatisch versleuteld en onleesbaar gemaakt.

Gemoedsrust

Bij Toshiba TEC staat het thema beveiliging hoog op de agenda. Zo kan onze professionele service 'Toshiba Managed Document Services (MDS)' u vanuit elke invalshoek inzicht geven in uw documentverwerking en in de directe en indirecte kosten van alle printprocessen in uw organisatie. Onze MDS consultants brengen het huidige printerpark en de aanverwante informatiestructuren en processen in kaart en houden hierbij de meest uiteenlopende aspecten tegen het licht: afdrukgewoontes, papiergebruik en papierverspilling, workflowverbeteringen en kostenbesparingen, inclusief kwetsbare aspecten van de beveiliging en specifieke risico's.

We beginnen met het in kaart brengen van het huidige printerpark en de aanverwante informatiestructuren en processen. Vervolgens krijgt ieder systeem een fysieke inspectie en bepalen we in gesprekken met management en medewerkers hoe ze deze systemen gebruiken in hun dagelijkse werkzaamheden.

Op basis van deze kennis ontwikkelen wij samen met u een printstrategie om het documentbeheer te optimaliseren met procedures op basis van rechten en rollen en het beveiligd vrijgeven van printopdrachten, volledig afgestemd op uw organisatie.

EEN ALLESOMVATTENDE AANPAK

SE SECURITY ENHANCED
Powerful Protection for Sensitive Data

Toegang

Geautoriseerde gebruikers hebben toegang tot print-opdrachten en gescande documenten, waardoor mobiel werken en gezamenlijk documentgebruik mogelijk worden. De toegang tot documenten is met wachtwoorden geregeld.

Scannen

Fysieke documenten worden gescand op de MFP en opgeslagen in uw dagelijkse digitale werkomgeving. U scant uw documenten direct naar kantoor- en enterprise-toepassingen. Via bijvoorbeeld Google Docs, Microsoft SharePoint en Microsoft Exchange krijgen geautoriseerde gebruikers toegang tot hun documenten.

'Ctrl P'

Documenten worden als printopdracht verzonden, op een printserver opgeslagen en pas vrijgegeven nadat de gebruiker zich heeft geïdentificeerd. De gebruiker hoeft geen specifieke printer te kiezen – de printopdracht kan op elke printer in het netwerk worden afgedrukt.

Authenticatie

Een geautoriseerde gebruiker kan zich bij elk multifunctioneel systeem in het netwerk identificeren om de printopdracht vrij te geven. Door middel van bijvoorbeeld contactloze ID-kaarten of een pincode kunnen alleen geautoriseerde gebruikers printopdrachten vrijgeven. Dit gaat ook papierverspilling tegen doordat niet-vrijgegeven opdrachten worden gewist.

Beveiligd document management systeem

Alle fysieke documenten kunnen naar een beveiligd document management systeem worden gescand en vervolgens worden vernietigd. Indexering vindt plaats om alle data gemakkelijk te kunnen raadplegen. Er vindt een complete registratie plaats zodra iemand gegevens raadpleegt of aanpast.

Data overschrijven & beveiligde harde schijf

Door het overschrijven van data verdwijnen ook alle ghost images (kopieën van de informatie) op de harde schijf. De beveiligde harde schijf zorgt ervoor dat data niet meer toegankelijk zijn zodra de schijf van de MFP wordt losgekoppeld.

DE JUISTE MFP-BEVEILIGING

SE SECURITY ENHANCED
Powerful Protection for Sensitive Data

Een zorgvuldige afweging

De verschillende aspecten van gegevensbeveiliging moeten in hun onderlinge samenhang worden bezien. Het implementeren van een aanpak voor de totale levensduur is essentieel – vanaf de documentaanmaak en het gebruik tot aan de vernietiging ervan.

Helaas is er soms te weinig aandacht voor het onderwerp MFP-beveiliging – door een gebrek aan kennis of doordat tijd of middelen ontbreken. Een keuze voor nieuwe technologische oplossingen kan echter veel problemen voor IT-managers oplossen en bovendien zakelijk voordeel opleveren.

Ga bij de keuze van een MFP alleen in zee met leveranciers die zich houden aan de geldende richtlijnen, waaronder ISO 15408 en IEEE 2600. Deze industrienormen voor beveiliging, zowel fysiek als op systeemniveau, verzekeren u als gebruiker ervan dat de leverancier op transparante wijze aan informatiebeveiliging werkt. Als gebruiker kunt u daar rechten aan ontlenen, wat u als afnemer aanvullende bescherming biedt.

Er komen nieuwe technologische oplossingen om de herkomst van documenten beter te kunnen bepalen, vergelijkbaar met watermerken. Deze identificatiemiddelen maken duidelijk waar en wanneer een document voor het eerst werd geprint. Ook wordt gewerkt aan de beveiliging van papieren archieven met behulp van scantechnieken die fysieke documenten automatisch converteren naar beveiligde, maar gemakkelijk doorzoekbare digitale bestanden. Het bewaren van documenten in digitale vorm is niet alleen veiliger, maar ook veel efficiënter en goedkoper.

Woordenlijst

Cloud computing:
Voor klanten beschikbare software, hardware en opslag op een externe locatie, waarbij alleen voor het gebruik wordt betaald.

Ghost image:
Gegevens die als printopdracht naar een MFP worden gestuurd, blijven als leesbaar beeld achter op de harde schijf. Dit verdwijnt als gekozen wordt voor het overschrijven van data.

MFP:
Een multifunctioneel product voor printen, scannen, faxen en kopiëren in één apparaat.

MDS:
Managed Document Services: een allesomvattende dienstverlening om u te helpen bij het besparen op kosten, het stroomlijnen van uw werkzaamheden, het toezicht houden op uw output-omgeving, het beveiligen van uw documenten en het ontzien van het milieu.

Rolgebaseerd printen:
Methode om printfuncties al dan niet beschikbaar te stellen, afhankelijk van de gebruiker, de applicatie of de website.

Beveiligde harde schijf:
De beveiligde harde schijf is alleen toegankelijk voor systemen die zich kunnen authentificeren. Gebeurt dat niet, dan is de informatie op de harde schijf niet te lezen, te kopiëren of af te drukken.

Beveiligd printen:
Printopdrachten worden op de centrale printserver bewaard totdat de gebruiker zich identificeert. Dat kan onder andere met behulp van contactloze ID-kaarten of een pincode.

ISO 15408:
Deze industrienorm stelt algemene principes en criteria vast voor de evaluatie van veiligheidsaspecten van IT-producten.

IEEE 2600:
Industrienorm (Institute of Electrical and Electronics Engineers) met een serie standaarden voor de beveiliging van printers en systemen.

256-bit-algoritme:
Deze wijze van encryptie wordt door overheden en militaire organisaties erkend als het hoogste niveau voor het versleutelen van gegevens.

TOSHIBA
Leading Innovation >>>

DE TOSHIBA GIDS OVER MFP-BEVEILIGING

Neem voor meer informatie contact op met Toshiba via:
info@toshibatec.nl
Of kijk op onze website:
www.toshibatec.nl