Xerox en informatiebeveiliging

Uw gegevens zijn uw zaken:
In samenwerking met partners de belangrijkste zaken beschermen

Inhoud

Overzicht

Informatie is het belangrijkste bedrijfsmiddel in elke organisatie en beveiliging is essentieel op kantoor - voor documenten en machines, inclusief printers en multifunctionele printers, die op het netwerk zijn aangesloten. En in de 21e eeuw is het netwerk de spil van vrijwel alle zakelijke activiteit.

Vrijwel elk bedrijf en elke persoon in het bedrijf is verbonden met het internet. Uw bedrijf – en elke organisatie waarmee u samenwerkt – maakt deel uit van een wereldwijd systeem van onderling verbonden computernetwerken en -servers. Ontelbare gebruikers voeren gelijktijdig taken uit, hebben toegang tot en delen informatie, kopen en verkopen goederen en diensten en communiceren via e-mail, chatberichten of Skype™, Twitter en vele andere internetdiensten.

De beveiligingsbedreiging is zeer reëel en de belangen nemen exponentieel toe. Een inbreuk in de beveiliging van de documenten van een organisatie kan tot ongeoorloofde acquisitie of gebruik van vertrouwelijke of eigendomsrechtelijke informatie leiden. Met als mogelijk gevolg schadelijke openbaarmaking, gestolen of gecompromitteerde intellectuele eigendoms- en handelsgeheimen. En voor vele organisaties kunnen deze beveiligingsschendingen resulteren in kostbare boetes en een rechtszaak die honderdduizenden tot miljoenen euro's kunnen kosten.

De toenemende beveiligingsrisico's komen tegenwoordig in verschillende vormen en met diverse mate van dreiging. De explosieve verspreiding van netwerkmachines betekent dat er een steeds groter aantal potentieel kwetsbare toegangspunten komt waarvan indringers misbruik kunnen maken. Er is continu dreiging van hackers, met programma's die 24/7 worden uitgevoerd en automatisch zoeken naar kwetsbaarheden in de netwerkbeveiliging om te exploiteren.

Beveiligingsrisico's verschillen van betrekkelijk onschuldige spamberichten tot aanhoudende bedreigingen die hele netwerken plat kunnen leggen.

Met de constante internetactiviteit moet u ervoor zorgen dat de vertrouwelijke informatie van uw bedrijf beveiligd blijft. Maar de eisen veranderen continu, en wel dagelijks.

Netwerkprinters en multifunctionele printers (MFP's), die kunnen printen, kopiëren, scannen naar netwerkbestemmingen, e-mailbijlagen verzenden en inkomende en uitgaande faxen verwerken, zijn met name kwetsbaar.

Voor diegenen die werkzaam zijn in informatiebeveiliging is het essentieel voor de beveiliging van het bedrijfsnetwerk dat er geen beveiligingsinbreuken plaatsvinden via de netwerkprinters en MFP's of op de printers zelf. Aanvallen kunnen tenslotte uit onverwachte hoek komen:

- De telefoonlijn die is aangesloten op een MFP kan gebruikt worden om toegang te krijgen tot het netwerk.
- De webserver die gebruikt wordt voor het beheren van de MFP's en printers kan kwetsbaar zijn voor een aanval.
- Er kan ongeautoriseerde toegang worden verkregen tot niet-beveiligde elektronische gegevens op de harde schijf of tijdens overdracht van/naar de machine.
- Vanaf een MFP kunnen kwaadaardige e-mails worden verzonden zonder audittrail.

Printers en multifunctionele printers zijn geavanceerde IT-platforms met verscheidene subsystemen en serieuze beveiligingsmaatregelen moeten elk element van het platform omvatten.

De printers en MFP's van tegenwoordig zijn beduidend anders dan PC's en servers.

- Printers en MFP's zijn gedeelde machines met meerdere gebruikers en meerdere beheerders.
- Printers en MFP's zijn iembedded machines:
  - Er kan een echt besturingssysteem in het systeem zijn ingebouwd.
  - Het besturingssysteem kan een directe externe interface hebben.
  - Het besturingssysteem is mogelijk van de eigen fabrikant.
  - Het besturingssyteem is mogelijk Microsoft® Windows®.

Overzicht

- Printers en MFP's beschikken over de volgende aspecten, die doorgaans geassocieerd worden met meer geavanceerde computernetwerken:
  - Netwerkprotocolstacks
  - Verificatie- en autorisatiefuncties
  - Versleuteling
  - Machinebeheer
  - Webservers

Uitdagingen vanwege de heterogeniteit van printer/MFP-implementaties:

- Veel grotere diversiteit dan bij traditionele PC's;
- Grote mate van diversiteit in de ondersteunende besturingssystemen tussen verschillende fabrikanten en zelfs tussen de productlijnen van een fabrikant.

De besturingsfuncties van traditionele PC's en servers zijn niet geoptimaliseerd voor printers en MFP's.

- Antivirusbenadering
  - Mogelijk geen antivirussoftware beschikbaar voor het gebruikte besturingssysteem in de printer en MFP
  - De strijd tegen malware verliest over het algemeen terrein
  - Het beheren van gegevensbestandupdates in een gedistribueerde omgeving is zeer complex
- Patches toepassen op printers en MFP's
  - Softwareversiebeheer van printers en MFP's is inconsistent
  - Configuratiebeheer zorgt voor aanvullende operationele werkzaamheden
- Security Information and Event Management (SIEM)
  - Waarschuwingen en machinestatusberichten van printers en MFP's zijn verschillend
  - Herstel van printers en MFP's is niet gestandaardiseerd

De situatie is tegenwoordig heel anders dan bij de printers en kopieermachines vroeger.

Vrijwel iedereen kan het netwerk en de informatiebronnen van een bedrijf aanvallen als de fysieke en elektronische toegang van een printer en MFP niet worden beveiligd en beschermd. Deze aanvallen variëren van een onbevoegde die documenten die in de opvangbak van de printer zijn blijven liggen simpelweg wegneemt, tot kwaadaardige wormen die vertrouwelijke documenten van het netwerk plukken.

Het hele systeem van een printer en MFP, inclusief alle machinebeheersoftware op het netwerk, moet worden geëvalueerd en gecertificeerd zodat de informatiebeveiliging is gewaarborgd en alle werknemers van een organisatie verzekerd zijn dat hun documenten en netwerk veilig en beschermd zijn tegen iedereen die uit is op het roven van de informatie – of zelfs tegen interne beveiligingsschendingen.

In dat opzicht zijn niet alle printers en MFP's gelijk. Daarom is een allesomvattende benadering, gebaseerd op fundamentele, functionele, geavanceerde en bruikbare beveiliging noodzakelijk voor de beveiliging van de informatiebronnen van hedendaagse bedrijven.

Gelukkig beschikt Xerox over de beveiligingsexpertise om te helpen. Xerox is de laatste 20 jaar toonaangevend geweest in het beschikbaar stellen van documentbeveiligingsoplossingen aan allerlei industriesectoren wereldwijd. Sterker nog, alle Xerox® - producten en – diensten die wij aanbieden zijn ontwikkeld met het oog op beveiliging en naadloze integratie in bestaande beveiligingsframeworks. Bovendien wordt beveiliging gedurende de hele levenscyclus van het product beheerd, vanaf de analyse van vereisten, ontwerp, ontwikkeling, productie, inbedrijfstelling tot de afvoer – wat u en uw klanten meer bescherming en geruststelling biedt.

Xerox helpt om uw gegevens te beschermen bij elke potentiële kwetsbaarheid. Wij zijn voortdurend geconcentreerd op de zaken waarin wij het beste zijn, zodat u zich kunt concentreren op uw zaken.

Beveiligingsdoelen van Xerox

In ons streven om elk van onze klanten beveiligingsoplossingen aan te bieden, hebben we vijf belangrijke beveiligingsdoelen geïdentificeerd:

Geheimhouding

- Geen ongeautoriseerde openbaarmaking van gegevens tijdens verwerking, overdracht of opslag.

Integriteit

- Geen ongeautoriseerde wijziging van gegevens
- Het systeem functioneert zoals bedoeld, zonder ongeautoriseerde manipulatie

Beschikbaarheid

- Het systeem functioneert goed
- Geautoriseerde gebruikers hebben toegang tot alle functies
- Bescherming tegen ongeautoriseerd gebruik van het systeem

Verantwoording

- Handelingen van een entiteit zijn rechtstreeks traceerbaar tot die entiteit

Onweerlegbaarheid

- Wederzijdse garantie dat de authenticiteit en integriteit van de netwerkcommunicatie behouden blijft

Kwetsbaarheden in de beveiliging: Risico's en kosten voor de industrie

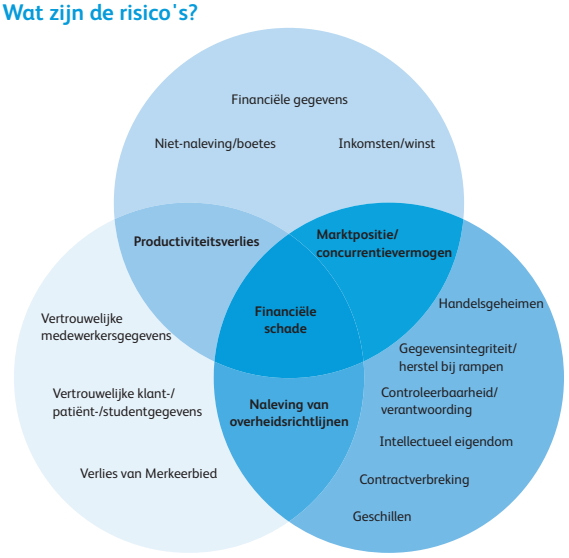
Bedrijven van alle omvang beschikken over vertrouwelijke informatie die waardevol is voor cybercriminelen en moet worden beveiligd. Het soort en de aard van de bedreigingen verandert voortdurend. Door de opkomst van Bring Your Own Devices (BYOD), wearables voor het tracken van gezondheidsdata, mobiele betaalsystemen, opslag in de cloud en het Internet of Things, is de dreiging reëel en neemt deze nog steeds toe.

Cybercriminelen richten zich in toenemende mate op het midden- en kleinbedrijf (MKB's), omdat ze een eenvoudiger doelwit vormen dan grote ondernemingen en omdat MKB's doorgaans niet over de middelen beschikken om zich tegen aanvallen te beschermen. Gegevensschendingen bij grote ondernemingen zijn voorpaginanieuws, maar we horen helaas niet veel over de cyberaanvallen op MKB's.

De belangen voor MKB's zijn zelfs nog groter dan voor grote ondernemingen. De klantinformatie in de administratie van MKB's is van steeds grotere waarde en de kosten van gegevensschendingen kunnen voor een MKB de genadeslag betekenen. Volgens een onderzoek uit 2015 van IBM en het Ponemon Institute waren de gemiddelde totale kosten van een gegevensschending voor de deelnemende bedrijven in twee jaar met 23 % toegenomen tot 3,79 miljoen US dollar.[1] De gemiddelde uitbetaalde kosten voor elk verloren of gestolen record met gevoelige en vertrouwelijke informatie nam toe van $145 in 2014 tot $154 in 2015.[1]

Dit laat nog buiten beschouwing de mogelijke boetes, het imagoverlies en verstoring van de bedrijfsvoering. Beveiliging is misschien niet altijd een topprioriteit in bedrijven, maar de beveiliging van informatie is van essentieel belang voor de gezondheid van de organisatie.

Wat zijn de risico's?



Gezondheidszorg

Verbeteringen in informatietechnologie – waaronder het gebruik van draagbare computers – hebben de behoefte geschept om belangrijke medische gegevens en patiëntgegevens elektronisch te delen, en hier met name wordt beveiliging een grote zorg.

De Amerikaanse Health Insurance Portability and Accountability Act (HIPAA) uit 1996 is door de federale overheid ingevoerd om alle organisaties in de gezondheidszorg te dwingen om bij gegevensbeheer uniforme praktijken te hanteren om de gegevens en privacy van patiënten te allen tijde te beschermen. HIPAA vereist dat een audittrail wordt bijgehouden van wie gegevens heeft bekeken, wanneer ze zijn zijn bekeken en of de personen de juiste autorisatie hadden om dit te doen.

Onder de Health Information Technology for Economic and Clinical Health (HITECH) Act werden de inspanningen van de Amerikaans overheid om een landelijk elektronisch administratiesysteem voor medische records voor de gezondheidszorg te realiseren aanzienlijk uitgebreid. HITECH werd aangenomen als deel van de American Recovery and Reinvestment Act van 2009 om de acceptatie en betekenisvol gebruik van informatietechnologie in de gezondheids-zorg te bevorderen.

Het niet voldoen aan HIPAA kan leiden tot civiele en strafrechtelijke straffen, zelfs als er geen schending heeft plaatsgevonden.

Overheid

De Amerikaanse overheid op lokaal, staat en federaal niveau legt tegenwoordig de nadruk op het vereenvoudigen van processen en het verbeteren van de onderlinge samenwerking tussen departementen ten behoeve van de burgers die ze van dienst zijn. Ze maken hierbij gebruik van diverse initiatieven om de nieuwste technologieën te benutten, terwijl ze tegelijkertijd strikte regelgeving implementeren die moet verzekeren dat de informatie die wordt gedeeld, goed is beveiligd. Een voorbeeld hiervan is de wet op gegevensschending van de staat Massachusetts, een van de meest stringente wetten in het land. De systemen, software en diensten van Xerox® voldoen aan deze strikte richtlijnen, en andere.

In 2014 nam het Amerikaanse ministerie van Defensie de National Institute of Standards and Technology (NIST) 800-53 normen aan, een publicatie waarin beveiligingsmaatregelen worden aanbevolen voor federale informatiesystemen en -organisaties en documentbeveiligingsfuncties voor alle federale informatiesystemen, met uitzondering van de systemen ontworpen voor de nationale beveiliging.

1. Onderzoek naar kosten van gegevensschending (2015): Globale analyse, IBM en Ponemon Institute, mei 2015.

Kwetsbaarheden in de beveiliging: Risico's en kosten voor de industrie

Het Amerikaanse Ministerie van Defensie heeft tevens aanvullende beveiligingsmaatregelen getroffen met de ingebruikname van ID-/toegangspassen: de Common Access Cards (CAC) en de tegenhanger voor de burgerlijke overheid, de Personal Identity Verification (PIV)-passen. Dergelijke passen vereisen een PKI-infrastructuur voor een beveiligde verificatie- en communicatieomgeving. Bovendien hebben de meeste federale overheidsinstanties de FIPS 140-2 standaard aangenomen voor certificering van de versleutelingsmodules die in printers en MFP's worden gebruikt. En ten slotte vereisen vele klanten van de federale overheid dat producten gecertificeerd zijn volgens de Common Criteria-norm.

Financiële dienstverlening

De financiële dienstverlening ondergaat een revolutie dankzij automatische stortingen, online bankieren, betaalpassen en andere innovaties in informatietechnologie. Hoewel dit zowel klanten als bedrijven meer gebruiksgemak biedt, komt dit intensieve gebruik van technologie met bijbehorende zorgen op het gebied van beveiliging.

Een veilige uitwisseling van creditcardgegevens is cruciaal en naleving van de gegevensbeveiligingsstandaard (DSS) van de betaalkaartenbranche (PCI) helpt bij het beperken van de kwetsbaarheden en het beschermen van de kaarthoudergegevens. PCI DSS is een branchespecifieke informatie-beveiligingsstandaard voor organisaties die met creditcards werken, waaronder Visa®, Mastercard®, American Express®, Discover® en JCB.

De Gramm-Leach-Bliley Financial Services Modernisation Act van 1999 (GLBA) werd aangenomen om ervoor te zorgen dat financiële instellingen die persoonlijke klantgegevens verzamelen of ontvangen een beveiligingsplan hebben om deze gegevens te beschermen. In naleving hiervan zijn organisaties verplicht om een risicoanalyse uit te voeren van hun huidige processen en firewalls te implementeren, gebruikerstoegang te beperken, het printen te bewaken, enzovoort.

Met de Dodd-Frank Wall Street Reform and Consumer Protection Act van 2010 is de noodzaak voor het nauwkeurig verzamelen en rapporteren van financiële gegevens nog aangescherpt. Door het Office of Financial Research (OFR) en aangesloten bureaus worden gegevens verzameld en geanalyseerd om nieuwe risico's voor de economie te identificeren en te monitoren en deze informatie openbaar te maken via periodieke rapporten en het afleggen van een jaarlijkse verklaring aan het Amerikaanse congres.

Onderwijs

In de huidige onderwijsinstellingen – van verplicht openbaar onderwijs tot het beroeps- en universitair onderwijs – kunnen alle transcriptie-aanvragen, aanvraagformulieren voor financiële steun en zelfs lesaantekeningen online worden gevonden. Omdat sommige scholen hun eigen medische afdeling hebben, moeten ze ook medische informatie elektronisch bewaren en delen. Deze interactieve omgeving biedt studenten een betere leerervaring en bevordert de productiviteit van het personeel, maar het maakt scholen ook kwetsbaar voor beveiligingsbedreigingen.

Aangezien deze instellingen informatie van diverse aard beheren, zijn vele regelgevingen op provinciaal en landelijk niveau van toepassing. In Amerika kent men de Computer Fraud and Abuse Act, USA Patriot Act, HIPAA en GLBA. De meest toepasselijke regelgeving voor het onderwijs is echter de Family Education Rights and Privacy Act (FERPA). Deze wet verbiedt de openbaarmaking van persoonlijk identificeerbare onderwijsinformatie zonder de schriftelijke toestemming van de student of diens ouder/verzorger.

Met zo veel regelgeving en nalevingsvoorschriften waarmee rekening moet worden gehouden, heeft Xerox de vereisten die door de federale overheid worden gesteld als richtlijn genomen. Door oplossingen te ontwikkelen die aan de meest stringente beveiligingsnormen voldoen, kunnen wij onze klanten in elke bedrijfssector zeer veilige oplossingen aanbieden.

Beveiligingsoverzicht

De ontwikkeling van producten, diensten en technologie bij Xerox wordt gestuurd door onze filosofie „Beveiliging = Veilig", met beveiliging op elk niveau.

Bij het ontwerpen van onze slimme MFP's staat beveiliging voorop en centraal. Als marktleider in de ontwikkeling van digitale technologie heeft Xerox aangetoond zich in te zetten voor de beveiliging van digitale informatie door potentiële kwetsbaarheden te identificeren en deze proactief aan te pakken om risico's te beperken. Klanten hebben in reactie daarop hun vertrouwen uitgesproken in Xerox als aanbieder van beveiligde oplossingen met een groot aantal standaard en optionele ultramoderne beveiligingsvoorzieningen.

Onze beveiligingsstrategie

De ontwikkeling van Xerox® - producten volgt het levenscyclusproces voor beveiligd ontwikkelen, waarbij rekening gehouden wordt met de richtlijnen van het Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM) en het SANS Institute. Dit omvat het opstellen van de beveiligingsvereisten, beoordelen van risico's, analyseren van kwetsbaarheden en het uitvoeren van penetratietests evenals het gebruik van informatie verkregen van OWASP en het Sans Institute. Deze strategie bestaat uit drie pijlers:

State-of-the-art beveiligingsvoorzieningen

Printers en multifunctionele machines zijn geavanceerde netwerkplatforms met meerdere subsystemen en Xerox biedt de grootste reeks beveiligingsfuncties op de markt, inclusief versleuteling, verificatie, autorisatie per gebruiker en auditcontrole.

Certificering

ISO 15408 Common Criteria voor het evalueren van beveiligingseigenschappen van IT-producten is de enige internationaal erkende norm voor beveiligingscertificering. Xerox was de eerste fabrikant die certificeringen heeft aangevraagd en verkregen voor MFP's in een „volledige" machine. Omdat elk element van het multifunctionele platform een potentieel toegangspunt vormt voor indringers, moet serieuze beveiligingscertificering alle elementen omvatten, waaronder de besturingssystemen, netwerkinterface, schijfstation(s), webserver, PDL-interpreter(s), MFP-gebruikersinterface, lokale hardwarepoorten
en het faxsysteem.

Onderhoud

Het up-to-date houden van de beveiliging van onze printers en multifunctionele machines gedurende hun hele levensduur vereist van Xerox een niet aflatende toewijding om continu beveiliging te bieden tegen de nieuwste aanvallen. Dit bewerkstelligen we als volgt:

- Zorgen dat software-updates doorlopend worden uitgegeven
- Kennisgeving van nieuwe beveiligingsbulletins via RSS-feeds
- Actie nemen tegen geïdentificeerde kwetsbaarheden
- Richtlijnen geven voor een veilige installatie en werking
- Informatie over Common Criteria verstrekken
- Patches beschikbaar stellen op www.xerox.com/security

Xerox garandeert middels het Xerox Security Model in combinatie met de Secure Development Life Cycle dat alle voorzieningen en functies van het systeem, niet slechts één of twee, veilig en beveiligd zijn.

Een alomvattende oplossing in beveiliging van printers en MFP's

Xerox heeft deze technologische verschuiving en de veranderende behoeften op de werkplek lang geleden al erkend en heeft hierop ingespeeld. Wij bieden allesomvattende beveiligingsvoorzieningen om uw printers/MFP's en uw gegevens veilig te houden. Xerox beveiligt elk onderdeel van het gegevensproces, waaronder printen, kopiëren, scannen, faxen, bestandsdownloads en de systeemsoftware. **Onze benadering op meerdere niveaus bestaat uit vier belangrijke aspecten.**

1. Bescherming tegen indringers

Het eerste en meest vanzelfsprekende kwetsbare punt is de gebruikersinterface – wie krijgt fysiek toegang tot uw printers en alle functies. Op basis van gebruikersverificatie wordt toegang verleend tot Xerox® - printers en multifunctionele machines aan geautoriseerde machine- en netwerkgebruikers. Eenmaal geverifieerd, kan de gebruiker het machine bedienen of klantgegevens bekijken, afhankelijk van de beperkingen op basis van de gebruikersrol. Xerox® printers en MFP's maken gebruik van verscheidene technologieën om geautoriseerde toegang tot de voorzieningen en functies van de machine door gebruikers en andere netwerkmachines te waarborgen. Daarna kijken we naar minder vanzelfsprekende kwetsbaarheden: wat wordt er naar de printer verzonden en hoe onderschept Xerox® ConnectKey® technologie aanvallen van beschadigde bestanden en kwaadaardige software. Onze systeemsoftware, inclusief DLM's en weblets, is digitaal ondertekend. Alle pogingen om geïnfecteerde, niet-ondertekende versies te installeren hebben tot gevolg dat het bestand automatisch wordt geweigerd. Printbestanden worden ook verwijderd als een deel ervan niet als legitiem wordt herkend.

Netwerkverificatie

Netwerkverificatie staat gebruikers toe zich bij de machinete verifiëren door het invoeren van een geldige gebruikersnaam en toegangscode voordat ze de machine mogen gebruiken. Via netwerkverificatie krijgt een gebruiker toegangsrecht tot één of een combinatie van de volgende functies: Printen, Kopiëren, Faxen, Serverfax, Opgeslagen opdrachten opnieuw printen, E-mail, Internetfax en Workflow scannen. Gebruikers kunnen daarnaast toegangsrechten krijgen tot één of een combinatie van de volgende systeempaden: Functies, Opdrachtstatus of Machinestatus.

1. Bescherming tegen indringers

Toegang tot machines met beperkte toegang regelen via gebruikerstoegang en interne firewall op de printer.

2. Machinedetectie

Waarschuwing bij het opstarten of op verzoek als er wijzigingen op uw printer zijn gedetecteerd die schadelijk voor de printer zijn.

3. Bescherming van documenten en gegevens

Houd persoonlijke en vertrouwelijke informatie veilig door versleuteling van de harde schijf (AES 256-bits, FIPS-gevalideerd voor veel producten) en beeldoverschijving van de harde schijf.

4. Externe partnerschappen

Bescherm uw data en machine tegen kwaadwillende binnendringers met McAfee whitelisting technologie, Cisco® Identity Services Engine (ISE) integratie, certificeringsinstanties en organisaties die testen op naleving van normen.

Microsoft® Active Directory® Services

Met behulp van Microsoft Active Directory Services (ADS) kan de machine gebruikersaccounts verifiëren aan de hand van een centrale database met gebruikersaccounts, in plaats van uitsluitend gebruik te maken van de gebruikersaccountdatabase die lokaal op de machine wordt bijgehouden.

LDAP-verificatie

LDAP-verificatie (BIND) wordt ondersteund voor verificatie bij de LDAP-servers voor het opzoeken van informatie en toegang. Wanneer een LDAP-client verbinding maakt met de server, wordt de verificatiestatus van de sessie standaard ingesteld op anoniem. Door de BIND-operatie wordt de verificatiestatus voor een sessie vastgelegd.

SMTP-verificatie

Deze functie controleert het e-mailaccount van de gebruiker en voorkomt dat onbevoegde gebruikers e-mails vanaf de machine kunnen verzenden. Systeembeheerders kunnen TLS inschakelen voor alle verzend- en ontvangstacties via SMTP.

POP3-verificatie voorafgaand aan SMTP

Systeembeheerders hebben de mogelijkheid om POP3-verificatie voorafgaand aan SMTP in of uit te schakelen als extra beveiligingslaag op Xerox® MFP's. Met POP3-verificatie voorafgaand aan SMTP moet eerst succesvol ingelogd worden op een POP3-server voordat men in staat is e-mail te verzenden via SMTP.

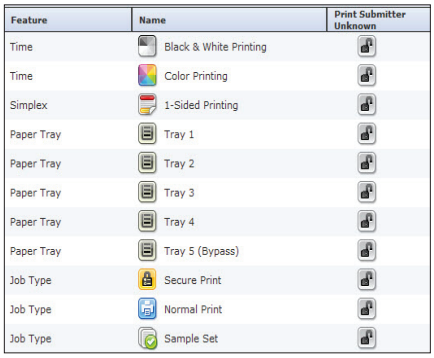
Op rollen gebaseerd toegangsbeheer (RBAC)

De RBAC-functie zorgt ervoor dat aan geverifieerde gebruikers een rol wordt toegewezen als Niet-aangemelde gebruiker/Aangemelde gebruiker, Systeembeheerder of Accountadministratiebeheerder. Bij elke rol horen specifieke bevoegdheden en een bepaald toegangsniveau tot functies, opdrachten en eigenschappen van de printwachtrijen. Systeembeheerders kunnen exact kiezen welke functies toegestaan zijn voor een bepaalde rol. Zodra een gebruiker zich bij de machine aanmeldt met gebruikersnaam en toegangscode, kan de machine vaststellen welke rollen aan die specifieke gebruiker zijn toegewezen. Beperkingen worden toegepast op basis van de toegewezen rollen. Als een volledige functie beperkt is, kan deze na verificatie vergrendeld of helemaal niet worden weergegeven voor de gebruiker.

Niet-aangemelde gebruiker/ Aangemelde gebruiker	Systeembeheerder	Accountadministratiebeheerder

Gebruikersrechten voor print

Met Xerox gebruikersrechten kan de toegang beperkt worden tot printfuncties op gebruiker, op groep, op tijd van de dag of op applicatie. Gebruikers en groepen kunnen worden ingesteld met verschillende toegangsniveaus tot printfuncties. Er kunnen bijvoorbeeld beperkingen worden ingesteld dat kleurenprintopdrachten alleen tijdens bepaalde uren van de dag zijn toegestaan; Microsoft® PowerPoint® presentaties automatisch dubbelzijdig worden geprint; of dat Microsoft Outlook® e-mails altijd in zwart-wit worden geprint.



Gebruikersrechtenvoor kleur en andere printbeperkingen instellen via intuïtieve grafische interfaces.

Verificatie via smartcard

Verificatie via smartcard, ook wel Proximity-pas of contactloze smartcard genoemd, beveiligt uw printer of MFP tegen toegang door onbevoegden. Xerox®-printers ondersteunen de belangrijkste smartcards (CAC/PIV, .NET, Rijkspas en andere smartcards en proximity-passen) en circa 30 verschillende typen kaartlezers en 65 verschillende proximity-passen. Bij verificatie via smartcard kunnen gebruikers geverifieerd worden via een tweeledige identificatie – presentatie van de pas en een PIN die op de printergebruikersinterface wordt ingevoerd – om toegang te krijgen tot de toepassingen op de machine of via het netwerk.

De Common Access Card/Personal Identity Verification (CAC/PIV) is een smartcard die wordt uitgegeven door het Amerikaanse ministerie van Defensie als standaard identificatiebewijs voor dienstdoende militairen, reservisten, burgerpersoneel, niet-overheidsmedewerkers en bevoegd personeel van contractors. De CAC/PIV kan behalve als toegangsbewijs tot printers/MFP's en de netwerken waarmee deze zijn verbonden, gebruikt worden als algemeen identiteitsbewijs, toegangspas tot gebouwen en voor verificatie van persoonlijke computers.

De 144k CAC/PIV is een versie van de smartcard. Gebruikers kunnen met behulp van tweestaps identificatie geverifieerd worden om toegang te krijgen tot de functies op de machine.

De 144k CAC/PIV-smartcard biedt de volgende voordelen:

- S/MIME-versleuteling bij Scannen naar e-mail voor de afzender of elke ontvanger in het lokale adresboek op de MFP of het LDAP global adresboek;
- Digitale ondertekening met behulp van het e-mailondertekeningscertificaat van de kaarthouder;
- Automatische invoer van het veld „Aan:" bij gebruik van Scannen naar e-mail op de MFP;
- Certificaatsleutel van max. 2048-bits;
- Uitgaande verzendingen beperken tot ontvangers met geldige certificaten;
- E-mailbevestigingsoverzichten ontvangen en auditlogboeken bijhouden;
- Eénmalige aanmelding (SSO) voor Scannen naar Home en LDAP.

Stroomdiagram voor Common Access Card (CAC)/Personal Identity Verification (PIV)

1. Een kaart wordt in de kaartlezer geplaatst en de gebruiker wordt gevraagd een PIN in te voeren op de MFP.
2. De MFP controleert op de OCSP-server of het certificaat van de kaart niet is verlopen en verifieert de „vertrouwensketen" terug naar een bekende certificeringsinstantie.
3. De MFP initieert een versleutelde vraag/antwoord-dialoog tussen de domeincontroller en de CAC-smartcard. Als dit succesvol is, geeft de domeincontroller een TGT (Ticket Granting Ticket) uit en is de autorisatie voltooid.
4. Na autorisatie zijn de volgende toepassingen op de MFP ontgrendeld voor machinegbruikers:
   - Scannen naar e-mail
   - Kopiëren
   - Faxen
   - Aangepaste functies
   - Workflow scannen

Xerox® PrintSafe software

Xerox® PrintSafe software biedt verificatiefunctionaliteit voor het veilig printen van gegevens op al uw multifunctionele printers van zowel Xerox® alsook andere fabrikanten. Deze software werkt met een scala aan veilige kaartlezers en kaarten die aan de industriestandaard voldoen.

Beveiligde, handige en flexibele printworkflows

De gebruiker verzendt het document.

Nadat op „Printen" is gedrukt, wordt het document vastgehouden totdat verificatie heeft plaatsgevonden.

De gebruiker kan op elke printer of MFP op het netwerk een PrintSafe-opdracht accepteren en zich eenvoudig verifiëren door het doorhalen van de kaart of invoeren van een PIN.

Nadat de gebruiker is geverifieerd, kan hij/zij een enkele opdracht of alle beveiligde opdrachten op de printer of MFP vrijgeven.

Xerox® PrintSafe software is niet uitsluitend voor Xerox® apparaten. Op elke printer of MFP* die geregistreerd is bij Xerox® PrintSafe software kunnen PrintSafe-opdrachten worden uitgevoerd.

Dankzij flexibele workflows kan de gebruiker software op de PC-client laden voor rechtstreeks printen of printen via een bestaande printserver die eenvoudig kan worden geconfigureerd voor Xerox® PrintSafe software.

*Voor niet-Xerox® machines is een netwerkaccessoire vereist; raadpleeg uw Xerox accountmanager voor informatie over de merken/modellen die worden ondersteund.

Toegang tot machinegebruikersinterface en externe gebruikersinterface

Systeembeheerders kunnen onbevoegde gebruikers de toegang tot de machine-instellingsschermenverbieden vanaf het bedieningspaneel en een Remote User Interface om zodoende de configuratiegegevens van de machine te beschermen.

2. Machinedetectie

In het onwaarschijnlijke geval dat de bescherming van uw data en netwerk wordt doorbroken, kan Xerox® ConnectKey® technologie een allesomvattende firmwareverificatietest uitvoeren, ofwel bij het opstarten* of nadat dit door geautoriseerde gebruikers is geactiveerd. U wordt gewaarschuwd als er schadelijke wijzigingen aan de printer of MFP zijn gedetecteerd. Als er afwijkingen worden gedetecteerd, verschijnt er een bericht dat de gebruiker adviseert de firmware opnieuw te laden. Onze meest geavanceerde ingebouwde oplossingen maken gebruik van McAfee® Whitelisting** technologie die continu bewaking en automatische preventie biedt tegen het uitvoeren van kwaadaardige malware.

In samenwerking met Cisco heeft Xerox onze apparaatprofilering in Cisco® Identity Services Engine (ISE) geïmplementeerd. Dankzij de integratie met Cisco Identity Services Engine (ISE) worden Xerox® machines automatisch in het netwerk gedetecteerd en ten behoeve van beveiligingsbeleid en naleving als printer geclassificeerd.

Raadpleeg voor meer informatie de volgende whitepapers:

Whitepaper over McAfee Whitelisting (alleen in het Engels beschikbaar):
http://www.office.xerox.com/latest/SECWP-03.PDF

Whitepaper over Cisco ISE (alleen in het Engels beschikbaar):
http://www.office.xerox.com/latest/SECWP-04.PDF

*Xerox® VersaLink® printers en multifunctionele printers
**Xerox® AltaLink® en i-Series multifunctionele printers

3. Bescherming van documenten en gegevens

Bescherming van documenten

Zelfs wanneer alle noodzakelijke netwerkbeveiligingsmaatregelen zijn getroffen om kritieke gegevens te beschermen tijdens het dataverkeer tussen de computers van gebruikers en kantoorprinters, moeten beveiligingstechnologieën ook de verzekering bieden dat gevoelige papieren documenten alleen door de beoogde ontvangers worden ontvangen en bekeken. Xerox maakt gebruik van de laatste technologieën ter bescherming van uw uitvoer, zowel bij het printen van afdrukken als bij de distributie van elektronische documenten.

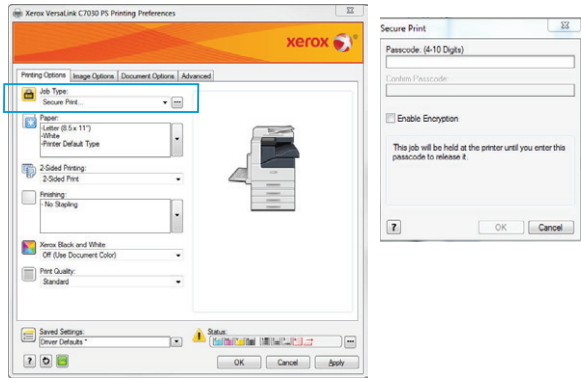
Versleuteling van scangegevens

Gebruikers van onze i-Series, VersaLink® en AltaLink®-serie smart MFP's voorzien van Xerox® ConnectKey® technologie hebben ook de mogelijkheid om PDF-bestanden met een toegangscode te versleutelen bij gebruik van de functie Scannen naar e-mail.

- Bescherming buiten de firewall
  - Gegevens beveiligen in een onbeveiligde omgeving
  - Gebruik van industriestandaard protocollen zoals TLS en Beveiligde PDF

Versleuteling van de printstream

De Xerox® Global Print Driver® en sommige productdrivers ondersteunen documentversleuteling wanneer beveiligde printopdrachten worden verzonden naar machines met ConnectKey technologie. Xerox® AltaLink en i-Series multifunctionele printers ondersteunen ook documentversleuteling voor normale printopdrachten. Voor versleuteling via de printerdriver is geen extra hardware vereist.



Beveiligd printen

Vertrouwelijke printopdrachten worden vastgehouden op de printer of MFP totdat de documenteigenaar deze vrijgeeft door een unieke PIN in te voeren via de gebruikersinterface van de machine. Dit verzekert dat de beoogde ontvanger van een document in persoon aanwezig is wanneer gevoelige informatie wordt geprint en de aflevering onmiddellijk uit de printer of MFP kan halen voordat het onder ogen komt van andere machinegebruikers.

Bij beveiligd printen op basis van Common Access Card (CAC)/Personal Identity Verification (PIV)-kaarttechnologie wordt het identiteitscertificaat van de opdrachtverzender aan de printopdrachttoegevoegd. Bij de machine moet de gebruiker zich verifiëren met zijn/haar CAC/PIV-kaart voordat de opdracht wordt vrijgegeven.

Versleutelde PDF/PDF met toegangscodebeveiliging

Bij het scannen van een papieren document voor elektronische distributie via Scannen naar e-mail, kunnen op Xerox® MFP's 128-bits of 256-bits AES-versleutelde PDF's of PDF's met toegangscodebeveiliging worden gemaakt. Deze worden vervolgens beveiligd over het netwerk verzonden en kunnen alleen geopend, geprint of gewijzigd worden door diegenen die in bezit zijn van de juiste toegangscode.

Fax doorsturen naar e-mail en netwerk

Op Xerox® MFP's met de mogelijkheid tot het doorsturen van faxen, kunnen inkomende faxen naar het postvak IN van de e-mail van specifieke ontvangers worden geleid en/of naar een beveiligde netwerkopslagplaats, waar uitsluitend geautoriseerde personen toegang tot ze hebben.

Faxontvangstbevestiging

De afzender van een fax ontvangt een automatische bevestiging dat de door hem/haar verzonden fax is ontvangen door de beoogde ontvanger.

Beveiligingsoverzicht

Digitale handtekeningen

Een digitale handtekening is een cryptografische methode die de verificatie van een digitaal bericht of document aantoont. Een digitale handtekening wordt gebruikt om de firmware vande machine te beschermen tegen ongedetecteerde wijzigingen en voor verificatie van de oorsprong van gegevens. Bij gebruik van smartcards kunnen e-mails digitaal worden ondertekend met het certificaat van de afzender. Een geldige digitale handtekening geeft de ontvanger het vertrouwen dat het bericht inderdaad afkomstig is van een bekende afzender en dat het onderweg niet is gewijzigd.

Beveiligde watermerken

Sommige Xerox® printers en MFP's beschikken over de functie Beveiligd watermerk die moet voorkomen dat originelen met gevoelige informatie worden gekopieerd. Als een document met een beveiligd watermerk wordt gekopieerd, wordt de watermerkafbeelding zichtbaar. Dit geeft duidelijk aan dat het document gevoelige informatie bevat en op niet legitieme wijze is gekopieerd.

Gebruiker-/tijd-/datumstempel

Via de Xerox® drivers kan een gebruiker-/tijd-/datumstempel worden aangebracht op elk document dat door een netwerkmachine wordt geprint. Dit zorgt voor een audittrail van wie wat heeft afgedrukt en op welk tijdstip.

Filteren op IP-adres

Met behulp van IP-filtering kunnen systeembeheerders regels opstellen om informatie die ontvangen wordt op de MFP te accepteren of te weigeren op basis van specifieke IP-adressen of een bereik van adressen. Hiermee kan de systeembeheerder bepalen wie wel en niet toegang krijgt tot de machine.

Geregistreerde IP-adressen:
Beschikbaar

Niet geregistreerde IP-adressen:
Niet beschikbaar

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Veel organisaties zijn verplicht om beveiligingsbeleid na te leven waarbij alle transacties tussen de client en printer of MFP beveiligd moeten plaatsvinden via beveiligde webtransacties, beveiligde bestandsoverdrachten en beveiligde e-mails. Gegevens die onversleuteld over het netwerk worden verzonden, kunnen door iedere netwerksniffer worden gelezen. Dit risico wordt door Xerox beperkt door het gebruik van SSL/TLS voor gegevensoverdrachten via protocollen als HTTPS en IPP.

IPsec-versleuteling

Internet Protocol Security (IPsec) beveiligt alle communicatie op de IP-laag en wordt hoofdzakelijk gebruikt voor het versleutelen van printgegevens naar de printer. Het versleutelt alle dataverkeer tussen punt A en punt B zodanig dat alleen vertrouwde gebruikers informatie kunnen verzenden en ontvangen, de gegevens niet worden aangepast tijdens de overdracht en dat alleen geautoriseerde gebruikers de informatie kunnen ontvangen en lezen.

IPsec is ontworpen om de volgende beveiligingsfuncties te bieden:

- Versleuteling van dataverkeer (voorkomen dat privécommunicaties onbedoeld door anderen worden gelezen)
- Integriteitscontrole (verzekeren dat het dataverkeer onderweg niet is aangepast)
- Verificatie van peer (verzekeren dat het dataverkeer afkomstig is van een vertrouwde partij)
- Anti-replay (bescherming tegen herhaling van dataverkeer in de beveiligde sessie)

Netwerkpoorten in-/uitschakelen

Met de functie voor het in-/uitschakelen van netwerkpoorten kunnen onnodige poorten en diensten uitgeschakeld worden om toegang door onbevoegden of kwaadwillenden te voorkomen. Op kleinere desktopprinters kunnen deze opties worden aangepast via het printerbedieningspaneel of via configuratiesoftware op PC's. Op grotere MFP's zijn er hulpprogramma's voor het instellen van beveiligingsniveaus en het uitschakelen van specifieke poorten en services.

Beveiligingsoverzicht

Digitale certificaten

Digitale certificaten zijn elektronische documenten die gebruik maken van een digitale handtekening om een openbare sleutel te binden aan een identiteit, d.w.z. informatie zoals de naam van een persoon of organisatie, adres, enzovoort. Het certificaat kan worden gebruikt om te verifiëren dat een openbare sleutel aan een persoon toebehoort.

MFP's kunnen digitale handtekeningen toevoegen die de bron en de authenticiteit van een PDF-document waarborgen. Wanneer ontvangers een PDF-bestand openen dat met een digitale handtekening is opgeslagen, kunnen ze de documenteigenschappen weergeven om de inhoud van de handtekening te bekijken, zoals de certificeringsautoriteit, systeemproductnaam, het serienummer en de tijd-/datumstempel wanneer het bestand is gemaakt. Als de handtekening een machinehandtekening is. Bevat dit ook de naam van de machine. Een gebruikershandtekening waarborgt de identiteit van de geverifieerde gebruiker die het document heeft verzonden of opgeslagen.

Op Xerox® MFP's kan een certificaat worden geladen dat door een certificeringsautoriteit zoals VeriSign is ondertekend. De systeembeheer-der kan ook een zelfondertekend certificaat op de machine zelf maken. Door een certificaat op uw machine in te stellen, kunt u versleuteling voor specifieke typen workflows inschakelen.

SNMPv3

Simple Network Management Protocol (SNMP) is een standaard internetprotocol voor het beheer van machines op IP-netwerken dat meer beveiliging biedt door gegevens te beschermen tegen manipulatie, het beperken van toegang tot geautoriseerde gebruikers door middel van verificatie en de versleuteling van verzonden gegevens over een netwerk.

SNMP wordt doorgaans ondersteund door machines zoals routers, switches, servers, werkstations, printers, modem racks, enzovoort. Het wordt het meest gebruikt in netwerkbeheersystemen voor monitoring van verbonden netwerkapparaten voor omstandigheden die de aandacht van de beheerder vergen. SNMP is onderdeel van de Internet Protocol (IP)-suite zoals gedefinieerd door de Internet Engineering Task Force (IETF). Het SNMPv3-protocol biedt aanmerkelijk betere beveiligingsfuncties, zoals versleuteling van berichten en verificatie.

SNMP-communitynaamstrings

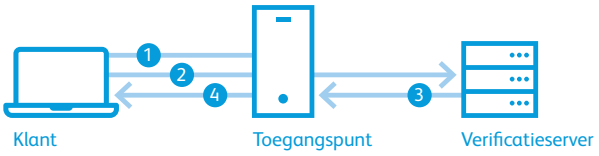
Management Information Base (MIB)-gegevens maken doorgaans gebruik van de tekenreeks „public" en de communitystrings zijn ingesteld op „private". Een applicatie kan met de communitynaamstrings „read-write" de configuratie-instellingen van de machine wijzigen met behulp van MIB-variabelen. Op Xerox® machines kunnen de communitynaamstrings read-write door de systeembeheerder worden gewijzigd voor hogere beveiliging bij het beheer van MFP's via SNMP.

802.1X-verificatie

IEEE 802.1X is een IEEE-norm voor netwerktoegangsbeheer op basis van poort 802.1X. Het maakt deel uit van de groep IEEE 802.1 netwerkprotocollen. Het biedt een verificatiemechanisme aan machines die verbinding willen maken met een lokaal netwerk (LAN) of een draadloos lokaal netwerk (WLAN). IEEE 802.1X-functionaliteit wordt door veel ethernet-switches ondersteund en blokkeert verbinding met uw netwerk aan gasten, indringers of onbeheerde systemen die niet geverifieerd kunnen worden.

Hoe het werkt: 802.1X-verificatie

802.1X-verificatie voor draadloze LAN's biedt centrale, servergebaseerde verificatie van eindgebruikers.



1. Een client stuurt een „start"-bericht naar een toegangspunt, dat vraag om de identiteit van de client.
2. De client reageert met een antwoordpakket dat de identiteit bevat, waarna het toegangspunt het pakket doorstuurt naar een verificatieserver.
3. De verficatieserver verzendt een „acceptatie"pakket naar het toegangspunt.
4. Het toegangspunt zet de poort voor de client in een geautoriseerde staat, zodat dataverkeer wordt toegestaan.

Beveiligingsoverzicht

Het 802.X-protocol is meer in opmars geraakt met de toegenomen populariteit van draadloze netwerken. Veel organisaties vergrendelen met dit protocol de poorttoegang tot hun interne netwerken. Dit voorkomt dat informatie aan het netwerk wordt doorgegeven voordat de machine is geverifieerd. Vanuit het oogpunt van risicobeheer verplicht dit zowel draadloze als bekabelde machines hun identiteit te bewijzen voordat ze informatie aan het netwerk kunnen doorgeven. Bij een ongeautoriseerde toegangspoging blijft de poort vergrendeld totdat deze door de systeembeheerder wordt ontgrendeld.

Het Extensible Authentication Protocol (EAP) is een raamwerk voor verificatie dat gebruikt wordt als onderdeel van 802.X-verificatie. Xerox® MFP's ondersteunen momenteel de volgende EAP-typen:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (AltaLink® en i-Series-machines)

Firewall

Een firewall is een deel van een computersysteem of netwerk dat bedoeld is om externe bedreigingen en ongeoorloofde toegang tot de machine te blokkeren terwijl geautoriseerde communicatie wordt toegestaan. Een firewall kan geconfigureerd worden om netwerkverkeer toe te staan of te weigeren op basis van een set regels en andere criteria. Netwerkbeheerders kunnen de toegang tot netwerksegmenten, services en poorten van de machine beperken om machines te beveiligen.

Scheiding van fax en netwerk

Door de faxinterface van de netwerkcontroller te scheiden neemt dit het beveiligingsrisico weg dat een hacker via de faxlijn op het kantoornetwerk kan binnendringen.

De MFP heeft geen functie om via de faxtelefoonlijn toegang te geven tot het netwerk. Het Faxklasse 1 protocol dat op de MFP wordt gebruikt, reageert alleen op faxcommando's die de uitwisseling van faxgegevens toestaat. De gegevens die vanaf de client-PC kunnen worden doorgegeven mogen uitsluitend gecomprimeerde beeldgegevens met bestemmingsinformatie zijn. Alle andere data dan de beeldgegevens (zoals een virus, beveiligingscode of controlecode die rechtstreeks toegang zoekt tot het netwerk) worden bij ontvangst afgebroken en de MFP beëindigt de oproep onmiddellijk. Er is dus geen mechanisme om via de faxlijn toegang te krijgen tot het netwerksubsysteem.

Gegevensbeveiliging

Technologie heeft de manier van werken van medewerkers volledig veranderd. Documenten worden tegenwoordig niet alleen in traditionele vorm op papier opgesteld, waaronder geschreven notities en kladversies van communicaties, maar veelal elektronisch op desktops en in e-mail. Omdat deze elektronische documenten anders dan papieren documenten worden gemaakt, opgeslagen, gedeeld en gedistribueerd, kan deze informatie blootgesteld worden aan nieuwe soorten risico's. Een bedrijf dat concurrerend wil blijven moet deze bedreigingen aanpakken door beveiliging van de documenten en de documentbeheersystemen die het waardevolste bedrijfsmiddel van een bedrijf bevatten – kennis.

Informatie- en documentbeheersystemen hebben te maken met een groot scala aan beveiligingsbedreigingen. Deze variëren van vormen van spionage, zoals computerhacking, diefstal, fraude en sabotage, tot onopzettelijke acties, zoals menselijke fouten en natuurrampen. Informatiebeveiliging is meer dan beveiliging. Het moet snelle toegang tot en beschikbaarheid van documentinhoud garanderen om bedrijfsprocessen en prestaties te verbeteren. Daarnaast moet het de originele inhoud beheren en voldoen aan overheidsvoorschriften en regelgeving.

Al vanaf de eerste digitale producten heeft Xerox het risico ingezien dat gegevens die op deze systemen zijn opgeslagen op ongeoorloofde wijze uit het niet-vluchtige geheugen zouden kunnen worden opgehaald en heeft voorzieningen en tegenmaatregelen in de machines geïmplementeerd om de gegevens van klanten te beschermen.

Versleuteling van beeldgegevens

Veel Xerox® machines maken gebruik van 128-bits of 256-bits AES-gegevensversleuteling van onder andere opdracht-, beeld- en klantgegevens, die de op uw Xerox® MFP's opgeslagen gegevens beschermen tegen ongeoorloofde toegang. Bij gegevensversleuteling wordt de schrijf gepartitioneerd en alleen de partitie met gebruikersgegevens wordt versleuteld. Besturingssysteempartities zijn niet en kunnen niet worden versleuteld.

- AES 128-bits of 256-bits versleuteling met Federal Information Processing Standard (FIPS) 140-2 validatie
- Alle gebruikersgegevens op de harde schijf worden versleuteld.

Beveiligingsoverzicht

Advanced Encryption Standard (AES) is een kleine, snelle en lastig te kraken versleutelingsstandaard die geschikt is voor een groot scala aan machines en applicaties. Het is een ultramoderne technologie die een combinatie van beveiliging, prestaties, efficiency, gemak van implementiatie en flexibiliteit biedt. Veel Xerox® machines kunnen in de modus FIPS 140-2 worden gezet. Dit houdt in dat ze uitsluitend FIPS 140-2 gecertificeerde versleutelingsalgoritmen gebruiken.

Beeldoverschrijving

Met beeldoverschrijving worden de beeldgegevens op de harde schijf van de Xerox® machine gewist zodra de gegevens niet langer nodig zijn. Dit kan automatisch worden gedaan nadat elke opdrachtverwerking is voltooid, op periodieke basis worden gepland of op verzoek van de systeembeheerder. Xerox® machines beschikken over de opties voor direct en op verzoek overschrijven.

Vluchtig en niet-vluchtig geheugen

De controller in elke Xerox® MFP bevat zowel vluchtig geheugen (RAM) als niet-vluchtig geheugen (harde schijf). Alle beeldgegevens in het vluchtig geheugen gaan na het uitschakelen of het opnieuw opstarten van het systeem verloren. Beeldgegevens in het niet-vluchtig geheugen worden doorgaans opgeslagen in flashgeheugen of de harde schijf van de MFP en worden behouden tot ze gewist worden.

Met de toenemende zorgen over gegevensbeveiliging willen klanten weten hoe en waar de integriteit van gegevens kan worden aangetast. Statements of Volatility (systeemgeheugenoverzichten) zijn documenten die inzicht geven waar de beeldgegevens van klanten zich op Xerox® machines bevinden. In een Statement of Volatility worden de locaties, capaciteit en inhoud van het vluchtig en niet-vluchtig geheugen in een bepaalde Xerox® machine beschreven.

Statements of Volatility zijn voor veel Xerox® machines opgesteld ten behoeve van klanten die beveiliging serieus nemen. U kunt deze documenten verkrijgen door contact op te nemen met uw lokale Xerox klanten support team (bestaande klanten), een Xerox accountmanager of via www.xerox.com/security.

Beveiligd faxen

Vertrouwelijke inkomende faxen worden vastgehouden totdat deze door de systeembeheerder worden vrijgegeven.

Scannen naar mailbox met toegangscodebeveiliging

Bij gebruik van de functie Scannen naar mailbox op een MFP kan de mailbox met een toegangscode worden beveiligd zodat alleen geautoriseerden toegang hebben tot de in de mailbox opgeslagen scans. De beveiliging voor Scannen naar mailbox wordt vergroot door versleuteling van de beeldgegevenspartitie op de harde schijf.

S/MIME voor Scannen naar e-mail

Secure/Multipurpose Internet Mail Extensions (S/MIME) biedt de volgende cryptografische beveiliging voor de functie Scannen naar e-mail: verificatie, berichtintegriteit en onweerlegbaarheid van de oorsprong van data (met behulp van digitale handtekeningen) en privacy- en gegevensbeveiliging (dankzij versleuteling).

Wanneer bij S/MIME-communicatie gegevens naar het netwerk worden verzonden, wordt aan elk e-mailbericht een handtekening toegevoegd op basis van de certificaatgegevens die zich op de machine bevinden. Bij het verzenden van de gegevens vindt versleuteling plaats op basis van het certificaat met betrekking tot het opgegeven adres van elk e-mailbericht. Het certificaat wordt geverifieerd wanneer de informatie voor de gegevensoverdracht wordt ingevoerd en op het moment dat de gegevens worden verzonden. S/MIME-communicatie wordt alleen uitgevoerd wanneer de geldigheid van het certificaat is bevestigd.

Versleuteling voor Scannen naar e-mail

Met e-mailversleuteling via smartcard-verificatie kunnen gebruikers tot 100 versleutelde e-mails verzenden naar meerdere ontvangers in een LDAP-adreslijst van een organisatie met behulp van de openbare sleutels van de ontvangers. De meeste Xerox® MFP's met smartcard-verificatie bieden tevens de mogelijkheid om e-mails digitaal te ondertekenen. Gebruikers kunnen de certificaten van mogelijke ontvangers bekijken voordat ze de e-mail versturen. De MFP staat e-mailverzending naar gebruikers zonder versleutelingscertificaat niet toe. Bovendien legt de MFP alle records van verzonden e-mail in een logboek vast, met de optie voor de beheerder om bevestigingsoverzichten te ontvangen.

Opdrachtenlog verbergen

De standaardfunctie Opdrachtenlog verbergen zorgt ervoor dat opdrachten die via de machine worden verwerkt, niet zichtbaar zijn voor machinegebruikers of via de externe gebruikersinterface. Ondanks het feit dat de informatie in het opdrachtenlog is verborgen, is deze nog steeds toegankelijk voor de systeembeheerder, die het opdrachtenlog kan printen om het kopieer-/fax-/print- en scangebruik op de machine te zien.

Beveiligingsoverzicht

Harde schijf behouden

Xerox biedt klanten met een Xerox® machine die zich zorgen maken dat beeldgegevens gevoelige of zelfs geclassificeerde informatie bevatten de mogelijkheid om de harde schijf te behouden. Tegen betaling heeft de klant het recht bij verhuizing/retourneren van de machine de harde schijven te behouden en deze te wissen of te vernietigen op zodanige wijze dat hun beeldgegevens beveiligd blijven.

Gegevensvalidatie voor externe diensten

Veel Xerox® machines vragen eerst klantgegevens op voordat ze persoonlijk identificeerbare gegevens (PII) en informatie die klanten identificeert (CII) via externe diensten aan Xerox kunnen verzenden.

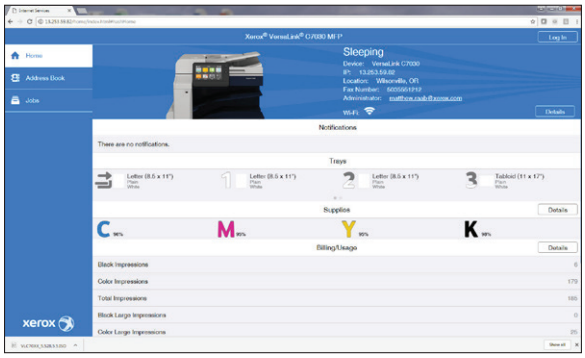
PostScript-toegangscodes

Er is een risico met betrekking tot het printen bij het gebruik van de Adobe® PostScript® paginabeschrijvingstaal (PDL). PostScript bevat commando's waarmee printopdrachten het standaardgedrag van de machine kunnen veranderen en de machine mogelijk kwetsbaar maken. Aangezien de PostScript-taal zeer krachtige hulpprogramma's bevat die gebruikt zouden kunnen worden om de beveiliging van een machine aan te tasten, kunnen beheerders de machine zo configureren dat bij PostScript-opdrachten een toegangscode wordt vereist om het standaardgedrag van de machine te wijzigen. De basisbevoegdheden van de PostScript-interpreter in de controller zijn met opzet beperkt, maar beheerders zijn tot op zekere hoogte in staat om de werking van het PostScript-subsysteem te sturen.

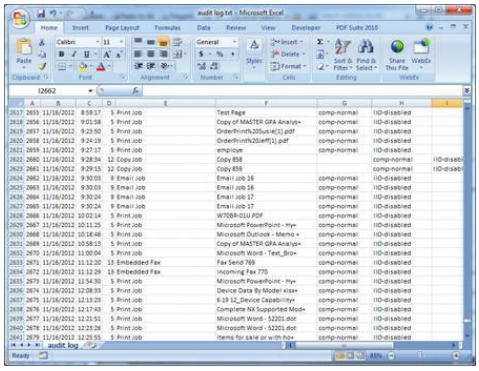
Auditlogboek

Xerox® MFP's en veel van onze printers kunnen controlelogboeken bijhouden om activiteiten per document, per gebruiker en per functie te volgen. Op nieuwere machines is het auditlogboek standaard ingeschakeld en kan door de systeembeheerder worden in- of uitgeschakeld. Het kan de toegang tot de machine en de toegangspogingen bijhouden en auditlogboeken naar een SIEM-systeem of auditlogserver verzenden. Een voorbeeld van een ingang in het auditlogboek: „Gebruiker xx heeft zich aangemeld bij de Xerox® AltaLink® MFP om 12:48 AM en heeft 10 pagina's gefaxt naar 888.123.1234."

Bij Xerox® multifunctionele printers met ConnectKey® technologie kan het auditlogboek automatisch en beveiligd naar een SIEM-systeem worden verzonden voor voortdurende monitoring van de MFP.



Systeembeheerders hebben vanaf hun werkstation via een standaard webbrowser toegang tot de interface van het auditlogboek.



Het logboek kan vervolgens worden geëxporteerd in een .txt-bestand en worden geopend in Microsoft® Excel®.

4. Externe partners

Xerox werkt samen met organisaties die testen op naleving van normen en leiders in de beveiligingssector zoals McAfee om hun overkoepelende normen en kennis te integreren met de onze. De volgende anti-malware beveiligingsvoorzieningen zijn beschikbaar op Xerox® MFP's met ConnectKey® technologie (Xerox® AltaLink® en i-Series multifunctionele printers).

McAfee® Embedded Control – Verbeterde beveiliging

Xerox® MFP's met Xerox® ConnectKey® technologie zijn voorzien van McAfee Embedded Control-integratie ondersteund door Intel® Security; Dit is de eerste generatie multifunctionele printers in de industrie die zichzelf beschermen tegen potentiële bedreigingen van buitenaf. De whitelisting-technologie van McAfee detecteert ongeautoriseerde pogingen tot het lezen, schrijven of toevoegen aan beveiligde bestanden en mappen en stuurt een melding als deze optreden. Verder biedt het naadloze integratie met de Xerox® CentreWare® websoftware, de Xerox® MPS-toolset en met McAfee ePolicy Orchestrator® (McAfee ePO™) is monitoring vanaf een PC-console naar keuze mogelijk.

McAfee Embedded Control – Integriteitscontrole

Integriteitscontrole is gebaseerd op de Enhanced Security-functionaliteit en voorkomt dat nieuwe bestanden op ongeoorloofde wijze worden uitgevoerd vanaf elke locatie. Alleen goedgekeurde software mag worden uitgevoerd, waardoor zowel algemene als doelgerichte aanvallen worden tegengehouden. De whitelisting-technologie van Xerox en Intel Security is bijzonder nuttig in ondernemingbrede beveiligingsimplementaties. Het garandeert dat uw machines alleen die functies uitvoeren die ze als diensten moeten leveren. Dezelfde technologie wordt toegepast om servers, geldautomaten, kassa's en embedded systemen zoals mobiele apparaten te beveiligen.

McAfee ePolicy Orchestrator (ePO)

McAfee's ePolicy Orchestrator (ePO) is een softwareprogramma voor beveiligingsbeheer dat het managen van risico's en naleving eenvoudiger maakt voor organisaties van groot tot klein. Aan de hand van drag-and-drop dashboards beschikken gebruikers over beveiligingsinformatie tussen eindpunten – data, mobiel en netwerken – voor onmiddellijk inzicht en snellere responstijden. ePolicy maakt gebruik van de bestaande IT-infrastructuur door het management van beveiligingsoplossingen van zowel McAfee als van derden te verbinden met LDAP, IT-operaties en configuratiebeheerprogramma's.

Als onafhankelijk bewijs van derden dat Xerox het hoogste niveau van naleving biedt, meten certificeringsinstanties zoals Common Criteria (ISO/IEC 15408) en FIPS 140-2 onze prestaties tegen internationale normen. Xerox wordt door hen erkend voor onze allesomvattende benadering van printerbeveiliging.

Cisco® Identity Services Engine (ISE) Integratie

Rol centraal printerbeveiligings-policies uit en beheer deze. Onze partnerschap met Cisco zorgt voor betere Xerox® Printer detectiemogelijkheden hetgeen weer resulteert in een fijnmazigere toepassing van het beveiligingsbeleid. Xerox® machines worden automatisch herkend en geclassificeerd door Cisco ISE, waarmee netwerktoegang wordt verkregen en overhead wordt verkleind omdat niet langer printerinformatie handmatig moet worden ingevoerd. Onze printerprofilering via de Cisco ISE dwarsboomt spoofing pogingen door saboteurs om onbelemmerde toegang tot gevoelige systemen te krijgen. Xerox® printerintegratie met Cisco ISE is een praktische benadering om de doelstellingen van het veiligheidsbeleid te behalen.

Naleving van regelgeving en beleid

Bij moderne printers en MFP's wordt veel gelet op naleving vanwege de persoonlijke en vertrouwelijke gegevens waartoe ze toegang hebben, op het systeem hebben opgeslagen of doorgeven. Het niet naleven van normen kan leiden tot het missen van zakelijke kansen, verlies van bestaande klanten of zelfs tot strafrechtelijke vervolging. Niveaus van de vereiste naleving verschillen per land en per verticale markt.

De Health Insurance Portability and Accountability Act (HIPAA) in de Verenigde Staten en de Wet bescherming persoonsgegevens in Nederland zijn voorbeelden van normen waaraan bedrijven moeten voldoen wil men legitiem zaken blijven doen.

Common Criteria certificering is een internationaal erkende beveiligingsnorm die aan de specificaties van het Amerikaanse ministerie van Defensie voldoet.

Met beveiligingsvoorzieningen die toonaangevend zijn in de industrie en de mogelijkheid tot flexibele configuratie en inbedrijfstelling voldoen Xerox® machines aan elke norm en beschikken over de functies die op elke behoefte kunnen worden afgestemd.

Xerox® systemen, software en diensten voldoen aan erkende industrienormen en de laatste overheidsregelgeving op het gebied van beveiliging. Met de voorzieningen die onze producten bieden zijn klanten in staat aan die normen te voldoen. De normen hieronder zijn voorbeelden:

- Gegevensbeveiligingsstandaard versie 3.0 van de betaalkaartenbranche (PCI)
- Sarbanes-Oxley
- Basel II Framework
- Health Insurance Portability and Accountability Act (HIPAA)
- E-privacyrichtlijn (2002/58/EG)
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act (FERPA) - Amerikaanse onderwijswet
- The Health Information Technology for Economic and Clinical Health Act (HITECH)
- Dodd-Frank Wall Street Reform and Consumer Protection Act - verzamelen en rapporteren van financiële gegevens
- ISO-15408 Common Criteria voor evaluatie van beveiliging van IT-producten
- ISO-27001 Normgeving voor Information Security Management System
- Control Objectives for Information and Related Technology (COBIT)
- Statement on Auditing Standards (SAS) Nr. 70
- NIST 800-53 (beveiligings- en privacynormen) in 2014 aangenomen door de Amerikaanse federale overheid en het ministerie van Defensie
- Federal Risk and Authorisation Program (FedRAMP)

Evaluatie van productbeveiliging

Documentbeveiliging betekent geruststelling. Een van de kenmerken van de Xerox® productlijn is de toewijding aan informatiebeveiliging. Xerox® systemen, software en diensten voldoen in alle aspecten aan erkende industrienormen en de laatste overheidsregelgeving op het gebied van beveiliging.

Common Criteria certificering

Common Criteria certificering omvat een onafhankelijke validatie door een objectieve derde partij van de betrouwbaarheid en kwaliteit van IT-producten. Het is een norm waarop consumenten kunnen vertrouwen bij het nemen van goed ingelichte beslissingen over de aanschaf van IT-producten. Common Criteria zet specifieke doelen voor informatiebescherming, waaronder strikte niveaus van integriteit, geheimhouding, beschikbaarheid van systemen en gegevens, verantwoording op individueel niveau en de garantie dat aan alle doelen moet zijn voldaan. De Amerikaanse federale overheid hanteert Common Criteria certificering als vereiste voor de hardware en software van apparaten die gebruikt worden in nationale beveiligingssystemen.

Common Criteria certificering behalen

Common Criteria certificering is een rigoureus proces dat onder andere bestaat uit producttests door een onafhankelijk laboratorium dat door het National Voluntary Laboratory Accreditation Program (NVLAP) geaccrediteerd is om productevaluaties uit te voeren aan de hand van beveiligingsvereisten. Producten worden getest aan de hand van functievereisten voor beveiliging op basis van voorgedefinieerde Evaluation Assurance Levels (EALs) of gespecialiseerde zekerheidsvereisten.

In de gezondheidszorg, financiële dienstverlening en andere marktsectoren is de noodzaak voor beveiliging zeker net zo belangrijk. Of het nu gaat om de bescherming van de privacy van hun klanten of intellectuele en financiële bedrijfsmiddelen, de zekerheid dat netwerken, harde schijven en telefoonlijnen veilig zijn en beschermd tegen hackers, virussen en andere kwaadaardige activiteiten is cruciaal. Hoewel certificering volgens Common Criteria geen vereiste is buiten de overheidssector, kan dit een onafhankelijke validatie verschaffen.

Xerox heeft een van de grootste series MFP's met Common Criteria certificering, met ongeveer 150 machines die het volledige certificeringsproces hebben doorstaan. Xerox was bovendien de eerste fabrikant die certificering voor het gehele machine heeft gekregen en de enige fabrikant die altijd de hele machine laat certificeren.

Zie www.xerox.com/information-security/common-criteria-certified als u wilt weten welke Xerox® MFP's gecertificeerd zijn op basis van Common Criteria.

Risico-analyse en risicovermindering

Proactieve beveiliging tegen nieuwe bedreigingen

Het aanbieden van de veiligste producten en oplossingen die momenteel op de markt verkrijgbaar zijn is slechts een deel van ons verhaal op het gebied van informatiebeveiliging. Onze wetenschappers en technici werken hard aan de ontwikkeling van de volgende generatie innovatieve beveiligingstechnologieën in de strijd tegen toekomstige dreigingen en om uw documenten veilig te houden: micro-printing, printbeveiliging door toepassing van fluorescentie en infrarood, printmarkeringstechnologie met Xerox® Glossmark® en correlatiemarkeringen, om er enkele te noemen. Zie voor meer informatie over deze technologieën www.xerox.com/security.

Andere initiatieven van Xerox:

De laatste risicio's goed in de gaten houden

Wij houden de clearinghouses voor kwetsbaarheden nauwlettend in de gaten om op de hoogte te blijven van de laatste informatie.

Beveiligingsbulletins uitgeven

Wij zijn proactief met het aanbieden van beveiligingspatches en indien nodig updates om uw apparatuur up-to-date en uw gegevens veilig te houden.

RSS-feeds distribueren

Updates worden van minuut tot minuut automatisch via RSS-feeds verspreid naar de readers van klanten.

Een schat aan informatiebronnen aanbieden

Als u zelf meer over dit onderwerp te weten wilt komen, is er een steeds uitgebreidere bibliotheek aan beveiligingsartikelen, white papers en handleidingen.

Ga naar www.xerox.com/security voor toegang tot ons volledige aanbod aan beveiligingsbronnen.

Naast de eigen uitvoerige interne tests, controleert Xerox regelmatig de clearinghouses voor kwetsbaarheden die beschikbaar gesteld worden door instanties en bronnen zoals US-CERT en de Oracle® Critical Patch Updates-rapporten, Microsoft® beveiligingsbulletins voor diverse kwetsbaarheden in software en besturingssystemen en bugtraq, SANS.org en secunia.com voor kwetsbaarheden in opensource. Tevens wordt er gebruik gemaakt van een robuust intern beveiligingstestprogramma, dat onder andere analyse van kwetsbaarheden en penetratietests omvat om uitvoerig geteste patches te leveren. Zie www.xerox.com/security als u het beleid over management en openbaarmaking van kwetsbaarheden wilt lezen.

Beveiligingsbulletins en implementatie van patches

Ontwikkelaars bij Xerox volgen een formele Security Development lifecycle voor de afhandeling van beveiligingsproblemen door middel van identificatie, analyse, prioriteitbepaling, codering en testen. Wij streven ernaar patches zo snel mogelijk te leveren al naar gelang de aard, oorsprong en ernst van de kwetsbaarheid. Afhankelijk van de ernst van de kwetsbaarheid, de grootte van de patch en het product, kan de patch apart worden gedistribueerd of in de vorm van een nieuwe softwarerelease voor dat product.

Afhankelijk van welk Xerox® product een patch vereist, kunnen klanten beveiligingspatches downloaden via www.xerox.com/security. Voor andere Xerox® producten worden beveiligingspatches beschikbaar gesteld als onderdeel van een nieuwe release van een systeemsoftwareversie. U kunt u registreren als u regelmatig beveiligingsbulletins wilt ontvangen. In de Verenigde Staten moeten klanten zich inschrijven voor de RSS-beveiligingsfeed. Buiten de Verenigde Staten moet u contact opnemen met de lokale Xerox klantenservice.

Op de website van Xerox www.xerox.com/security hebt u toegang tot actuele informatieupdates en belangrijke bronnen:

- Beveiligingsbulletins
- RSS-feed: Get Security Bulletins (Xerox-beveiligingsbulletins)
- Veelgestelde vragen over Xerox® productbeveiliging
- Information Assurance Disclosure-documenten (technische toelichtingen m.b.t. informatiebeveiliging)
- Producten met Common Criteria-certificering
- Beleid over beheer en openbaarmaking van kwetsbaarheden
- Hulp bij productbeveiliging
- Artikelen en white papers
- Statements of Volatility (systeemgeheugenoverzichten)
- Software Release Quick Lookup Table (snelle referentietabel bij softwarerelease)
- FTC-handleiding voor digitale kopieermachines en MFP's

www.xerox.com/security is de Xerox portal tot diverse informatiebronnen met betrekking tot beveiliging, waaronder bulletins, white papers, patches en nog veel meer.

Beveiligingspraktijken met betrekking tot productie en leveranciers

Xerox en onze belangrijkste productiepartners zijn lid van de Electronic Industry Citizenship Coalition (http://www.eicc.info).
Door het onderschrijven van de gedragscode van de EICC geven Xerox en andere bedrijven aan dat ze strikt toezicht en controles uitoefenen op hun productieprocessen.

Xerox onderhoudt daarnaast contractuele betrekkingen met haar primaire en secundaire leveranciers die Xerox toestaan audits op locatie uit te voeren om de integriteit van het proces tot op componentniveau te waarborgen.

Xerox is tevens lid van de Amerikaanse Customs Agency Trade Partnership Against Terrorism (C-TPAT), een samenwerkingsverband van bedrijven met de douane in de VS. Dit initiatief richt zich op de beveiliging van de toeleverketen. Voorbeelden van handelspraktijken die door Xerox onder dit programma zijn ingevoerd, zijn maatregelen om diefstal of kaping te voorkomen. In Noord-Amerika worden alle aanhangwagens die tussen de fabriek en productdistributiecentra en tussen de distributiecentra en logistieke vervoerscentra rijden op het vertrekpunt verzegeld. Op alle trucks zijn GPS-trackers geïnstalleerd die voortdurend gemonitord worden.

Retourzending en afvoer van producten

Harde schijf behouden van Xerox® producten

Xerox biedt klanten in de Verenigde Staten de zogenaamde „Hard Drive Retention Offering", waarbij klanten tegen betaling de harde schijf van een geleast Xerox® product mogen behouden. Deze service wordt mogelijk vereist door klanten met zeer gevoelige of zelfs geclassificeerde gegevens, of waarbij het interne beleid of regelgevende normen specifieke afvoerprocessen van harde schrijven voorschrijven.

Als een klant een verzoek voor deze service indient, gaat een Xerox-technicus naar de klantlocatie om de harde schijf te verwijderen en deze in de huidige staat (zoals hij is) aan een vertegenwoordiger van de klant te overhandigen. Xerox biedt op locatie bij de klant momenteel geen optie tot het schoonmaken, wissen of vernietigen van de harde schijf. Klanten moeten zelf maatregelen treffen voor de uiteindelijke afvoer van de fysieke harde schijf die ze van de technicus in ontvangst nemen.

Zie www.xerox.com/harddrive om te bepalen of uw Xerox® product een harde schijf bevat of om te zien welke beveiligingsvoorzieningen beschikbaar zijn om data op harde schijven te beveiligen.

Neem voor meer informatie over dit programma contact op met uw Xerox-accountmanager of ga naar www.xerox.com/security en raadpleeg de artikelen en white papers onder Security Resources (Beveiligingsbronnen).

Bovendien zijn vrijwel alle nieuwe Xerox® printers en MFP's standaard voorzien van 256-bits AES-versleuteling van de harde schijf evenals het drie keer overschrijven van beeldgegevens, zodat de klantgegevens op een nieuwe machine vanaf de eerste dag zijn beveiligd.

Samenvatting

Netwerk- en gegevensbeveiliging behoren tot de vele uitdagingen waarmee bedrijven dagelijks geconfronteerd worden. De printers en MFP's van tegenwoordig zijn netwerkmachines die een belangrijke rol in het bedrijf innemen en ontvangen en verzenden belangrijke gegevens via een groot aantal functies. Het zorgen voor een allesomvattende beveiliging is dan ook uiterst belangrijk.

Het hele systeem van een MFP, inclusief alle machinebeheersoftware op het netwerk, moet geëvalueerd en gecertificeerd worden zodat de informatiebeveiliging is gewaarborgd en alle werknemers van een organisatie verzekerd zijn dat hun documenten en netwerk veilig en beschermd zijn tegen iedereen die uit is op het roven van de informatie – of zelfs tegen interne beveiligingsschendingen. In dat opzicht zijn Xerox® MFP's toonaangevend in de industrie. Onze allesomvattende benadering, gebaseerd op fundamentele, functionele, geavanceerde en bruikbare beveiliging is noodzakelijk voor de beveiliging van de informatiebronnen van onze klanten.

Vanuit dit besef worden alle producten bij Xerox ontworpen en geproduceerd om de hoogst mogelijke beveiliging te garanderen op alle potentiële kwetsbare punten. Onze missie is het beveiligen van uw data zodat u zich kunt richten op de zaken en activiteiten die uw bedrijf of organisatie zo succesvol mogelijk maken.

Ga naar www.xerox.com/security voor meer informatie over de vele beveilligingsvoorzieningen en informatiebronnen die Xerox biedt.

Checklist beveiliging

IT-beveiligingsmanagers worden al overstelpt met uitdagingen op beveiligingsgebied die ze het hoofd moeten bieden. Kleine bedrijven moeten kunnen vertrouwen op effectieve systemen en beveiligingssoftware die het grootste deel van het werk voor hen doen. Het laatste waar u en uw medewerkers op staan te wachten is meer tijdrovende inspanning of handmatige interventie om elke machine en datastream in uw omgeving te monitoren en up-to-date te houden, inclusief uw MFP's en printers.

Een allesomvattend netwerkbeveiligingsplan moet drie belangrijke punten omvatten, met een geïmplementeerde strategie voor elk punt die garandeert dat het plan zal werken.

1. Autonome, zelfbeschermende machines die robuuste beveiliging bieden tegen nieuwe aanvallen.
2. Naleving van de meest up-to-date beveiligingsnormen en regelgeving.
3. Volledige zichtbaarheid op het netwerk.

De nieuwe beveiligingsstandaard voor een nieuw tijdperk

- Beveiliging mag niet pas als laatste aan bod komen.
- Informatie is een steeds waardevoller intellectueel eigendom.
- Firewalls zijn onvoldoende; beveiligingsbeleid moet holistisch en alom aanwezig zijn.
- Beveiliging voor embedded systemen vormt nu een integraal onderdeel van de huidige noodzakelijke beveiligingsvereisten.

Xerox biedt allesomvattende beveiliging op meerdere niveaus, die u eenvoudig implementeert en beheert en uw bedrijf helpt bij de naleving van industrie- en overheidsnormen. Xerox® technologie is getest en gevalideerd om bescherming te bieden tegen ongeautoriseerde toegang, gegevens en identiteiten.

Gebruik de checklist hiernaast wanneer u Xerox® MFP's vergelijkt met de producten van andere fabrikanten om na te gaan of de apparaten van concurrenten hetzelfde niveau van end-to-end beveiliging bieden als Xerox.

		Concurrent		
	Xerox	**1**	**2**	**3**
Filteren op IP-/MAC-adres	✓			
IPsec-versleuteling	✓			
IPv6	✓			
802.1X-verificatie	✓			
Beveiligd printen	✓			
Versleuteling voor Scannen naar e-mail	✓			
Versleutelde PDF/PDF met toegangscodebeveiliging	✓			
Digitale handtekeningen	✓			
256-bits AES Versleuteling van harde schijf	✓			
Beeldoverschrijving	✓			
Beveiligd faxen	✓			
Poortblokkering	✓			
Scannen naar mailbox met toegangscodebeveiliging	✓			
Harde schijf behouden	✓			
Printbeperkingen	✓			
Auditlogboek	✓			
Op rollen gebaseerd toegangsbeheer	✓			
Verificatie via smartcard	✓			
Ondersteuning van CAC/PIV-smartcards	✓			
Gebruikersbevoegdheden	✓			
Common Criteria-certificering van het „hele systeem”	✓			
Integratie met standaard netwerkbeheerprogramma's	✓			
Beveiligingsupdates via RSS-feeds	✓			
Embedded McAfee-beveiliging ondersteund door Intel® Security	✓			
McAfee® Integrity Control	✓			
Integratie met McAfee® ePolicy Orchestrator®	✓			
Cisco® Identity Services Engine (ISE) integratie	✓			

Ga voor meer informatie naar **www.xerox.com**.