april 2008 nummer 2

INFORMATIEBEVEILIGING

Risicomanagement krijgt vaste plaats in ITIL

Introductie: discussiemodel voor integrale beveiliging

Virtualisatie, de ins en outs

Sociale netwerksites onschuldig?

De menselijke kant van informatiebeveiliging

ib

PvIB
Platform voor
InformatieBeveiliging

Beveiliging multifunctionals

Auteur: Ronald Eygendaal > Ronald Eygendaal is werkzaam als Security Consultant bij Getronics PinkRoccade. Hij heeft meer dan vijftien jaar ervaring in beveiliging, fraudeonderzoeken en informatiebeveiliging in het bijzonder. Eygendaal is voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN). E-mailadres: ronald.eygendaal@getronics.com.

Het is een trend om meer en meer gebruik te maken van zogenaamde multifunctionals, ook wel MFC's genoemd. Multifunctionals zijn apparaten waarin de functionaliteit van een printer en/of fax en/of scanner en/of kopieerder samen zijn gebracht. Een moderne multifunctional is uitgerust met een webserver die de af te drukken bestanden via een netwerk binnenkrijgt en deze voor bijvoorbeeld het printen verwerkt. Dit maakt het mogelijk dat de MFC direct in een netwerk kan worden opgenomen en door middel van een standaard internetbrowser beheerd kan worden. Ook gebruikers kunnen via bijvoorbeeld Internet Explorer verbinding maken met de webserver in de multifunctional om bijvoorbeeld documenten voorrang te geven in de wachtrij of om het papierniveau controleren. Verder is het mogelijk om vanaf een individuele werkplek van een gebruiker een verbinding op te zetten naar een multifunctional om zodoende van de scanfunctionaliteit gebruik te kunnen maken.

Als het kwaadwillenden lukt om via een netwerk toegang te krijgen tot de webserver en/of harde schijf waarop de data van afdruk, fax of scan worden bewaard dan kunnen zij deze informatie oneigenlijk gebruiken ofwel misbruiken met alle gevolgen van dien. Ook al is er grondig nagedacht over virusbestrijding, firewalls en dergelijke, het besef dat multifunctionals als spin in het web waardevolle informatie bevatten en een waardevol proceselement vormen, mag wel wat sterker aanwezig zijn. Juist vanwege die centrale positie die multifunctionals in de netwerken innemen, is de beveiliging ervan een serieus punt. Evaluaties van de beveiliging van MFC's hebben aangetoond dat voor een veilig gebruik hiervan het noodzakelijk is richtlijnen op te stellen en te handhaven. Sterker nog, beveiliging van multifunctionals moet een integraal onderdeel vormen van het beveiligingsbeleid van een organisatie. Kortom; bij de beveiliging van multifunctionals spelen fysieke en technische maatregelen een belangrijke rol. Eigenschappen als authenticatie, encryptie, harddrive databeveiliging, scanbeveiliging en document serverbeveiliging zijn uitermate belangrijk.

Technische beveiliging

In tegenstelling tot de personal printer staan multifunctionals doorgaans op de gang of in algemene ruimten. Vooral dit soort ruimten zijn gewild bij kwaadwillenden, omdat ze hier ongemerkt afdrukken kunnen wegnemen. Speciaal hiervoor zijn de moderne multifunctionals voorzien van een pincodefunctionaliteit. Een gebruiker kan bij het printen een pincode ingeven, vervolgens naar de printer lopen en daar met behulp van zijn pincode het betreffende document uitprinten. Daarnaast bestaat er de mogelijkheid multifunctionals te voorzien van een kaartlezer zodat bij het aanbieden van een toegangspas voor het gebouw de printopdrachten van de betreffende medewerker uitgeprint worden.

Om te voorkomen dat ongeautoriseerde personen toegang verkrijgen via het interne netwerk, wordt er in het netwerk een logische scheiding aangebracht tussen het normale netwerk en het multifunctionals netwerk. Dit gebeurt bij voorkeur via zogenaamde V-Lan's. Omdat multifunctionals over de eigenschappen van een complete server beschikken, zoals harde schijven, geheugen et cetera, dienen deze op dezelfde wijze beveiligd te zijn als een server.

Ook ongeautoriseerde handelingen en zelfs netwerkaanvallen zijn mogelijk vanuit deze optiek dus dient de toegang tot het netwerk en tot multifunctionals te worden beperkt.

Een verdere veiligheidsmaatregel zou kunnen zijn om FTP-communicatie (File Transfer Protocol) te blokkeren en de blokkering alleen even op te heffen als er daadwerkelijk een afdrukopdracht binnenkomt. Immers, het FTP-protocol is ook geschikt om bestanden te transporteren, waarmee een aanval op het netwerk uitgevoerd kan worden.

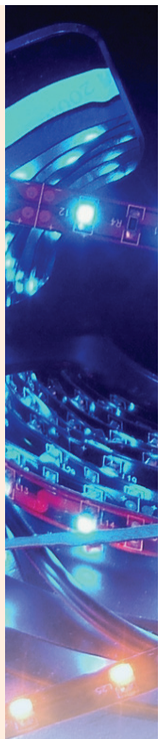
Om te voorkomen dat onbevoegden via de faxlijn van een multifunctional toegang krijgen tot het interne bedrijfsnetwerk, moet de faxfunctie gescheiden kunnen worden van de andere circuits in het apparaat. Een verbinding tussen die twee netwerken is er niet, dus kan een potentiële hacker ook niet via de telefoonlijn op het bedrijfsnetwerk komen. De enig mogelijke communicatie van buitenaf is de fax. Als aanvullende maatregel zou nog overwogen kunnen worden om enkel gerichte telefoonlijnen te gebruiken. (Met een enkel gerichte telefoonlijn kan men uitsluitend één kant op bellen, bijvoorbeeld alleen uitgaand.)

Verder zijn multifunctionals uitgerust met een harddisk waarop de data van afdruk, fax of scan worden bewaard. Vanuit deze optiek dienen multifunctionals een functionaliteit te bevatten waardoor data, die bij gebruik achterblijven op de interne harde schijf, overschreven worden. Dit overschrijven moet zodanig gebeuren dat reconstructie van de overschreven data niet meer mogelijk is. Bij Nashuatec wordt deze functionaliteit Data Overwrite Security (DOS) genoemd. Xerox spreekt over de Image Overwrite-functie, andere leveranciers gebruiken hiervoor weer andere benamingen.

Het overschrijven van data dient bij voorkeur te geschieden ná het afronden van elke kopieer, print- en/of scanopdracht. Data die achterblijven na het uitvoeren van een scan- of faxopdracht dienen dagelijks te worden overschreven gedurende de nachtelijke uren.

Enge functionaliteiten.

Multifunctionals bezitten, gezien vanuit een beveiligingsoptiek, hele enge functionaliteiten. Zo is het bij de meeste multifunctionals bijvoorbeeld mogelijk om een document te scannen en dit tegelijkertijd te e-mailen of te faxen. Dit zijn zeer laagdrempelige functies met een groot risico op het lekken van vertrouwelijk informatie. Het is zeer eenvoudig te doen alsof je een kopie maakt en ondertussen de scan naar e-mailfunctie te gebruiken om vertrouwelijk informatie naar een wazig e-mailadres te sturen. Over de beveiliging van deze functionaliteit moet dus goed worden nagedacht. Een mogelijk oplossing kan zijn om uitsluitend intern e-mailen toe te staan



op de desbetreffende multifunctional. Of nog beter; e-mail via een pincode zodat de e-mail traceerbaar is. Uiteraard geldt ditzelfde scenario voor faxen.
Het ontvangen van faxen introduceert ook de nodige risico's te meer omdat de multifunctionals veelal in algemene ruimten worden geplaatst. Had vroeger de secretaresse nog zicht op binnenkomende faxberichten en was er daardoor nog een vorm van sociale veiligheid, tegenwoordig komen de faxen binnen op een multifuntional in een algemene ruimte. Hierdoor is het voor onbevoegden vrij eenvoudig binnenkomende faxberichten te laten verdwijnen. Oplossingen hiervoor moeten worden gezocht in het plaatsen van faxservers. Opvallend is dat verschillende leveranciers deze oplossingen aanbieden.
Omdat een moderne multifunctional voorzien is van een harde schijf is het mogelijk dat gebruikers deze schijf gebruiken (bewust of onbewust) als opslagmedium voor bestanden (bijvoorbeeld archivering). Vanuit een beveiligingsoogpunt is dit ongewenst.

IEEEE P2600

Gelukkig hebben de fabrikanten van multifunctionals niet stil gezeten en hebben ze het probleem van beveiliging geïdentificeerd. Vervolgens hebben de fabrikanten beveiligingswerkgroepen gevormd. Hierin participeerden Hewlett-Packard, Lexmark, Canon, Xerox, Sharp, Ricoh, IBM, Epson, Okidata, Equitrac en Oce. Zij hebben gezamenlijk, onder supervisie van de standaardisatie organisatie IEEE, gewerkt aan de zogenaamde P2600. IEEE P2600 zal fabrikanten, systeembeheerders en gebruikers helpen de vele potentiële veiligheidsaansprakelijkheden verbonden aan hardcopy apparaten te beheersen.
De P2600 beschrijft de gehele printketen, dus de printerque, het transport van data, de oplage van data en het vrijgeven en printen van data. De P2600 security printing standaard geeft fabrikanten de mogelijkheid hun multifunctional te certificeren tegen de Common Criteria. De P2600 kent een viertal niveaus van beveiliging die onder andere afhankelijk zijn van de wijze van authenticatie. Te weten; één single-factor- en drie two-factor authentication technieken.
P2600.1 Primary PIN (or card swipe) only
P2600.2 Primary PIN (or card swipe) and secondary PIN
P2600.3 Network user ID and password
P2600.4 Primary PIN (or card swipe) and network password

Lease of huur?

Binnen veel organisaties worden multifunctionals geleased of gehuurd. Dit kan de implementatie van beveiliging in de weg zitten. Veel organisaties zijn terecht bang voor het lekken van informatie via de harde schijf in de multifunctional.
Zoals reeds eerder beschreven worden alle data opgeslagen op de harde schijf in de multifunctional. Ervaring leert dat de wisfunctionaliteit in een aantal gevallen onvoldoende is. De Gutmann-standaard, maar ook de Amerikaanse standaard DOD 5220.22M, gaat uit van 35 keer overschrijven met bepaalde karakters. Aangezien de meeste leveranciers hebben gekozen voor driemaal overschrijven, is het dus mogelijk om gewiste data terug te halen.
Daarom is het verstandig om in het geval van lease of huur goede afspraken te maken. Ten minste dat zodra de multifunctional de organisatie verlaat, de harde schijf fysiek wordt verwijderd en wordt vernietigd.

Vervangingsrisico's faxen

Zoals eerder aangegeven bevatten multifunctionals functionaliteiten van faxmachines. Het is dan ook logisch dat bij de introductie van een multifunctional veelal de faxmachine wordt vervangen. In dit vervangingsproces kunnen risico's op het lekken van informatie zitten en dan vooral wanneer het thermische faxen betreft. Deze faxmachines faxen 'thermisch' op gewoon A4-papier. Het inktmechanisme in dit soort faxmachines is een carbonrol ook wel donorrol genoemd, waarmee de afdrukken worden gemaakt. Carbon is papier dat aan één kant zwart is en waarmee via een thermisch proces afdrukken gemaakt kunnen worden. Door het gebruik van een carbonrol in een fax kan deze qua afmetingen compact blijven, al zijn er wel beperkingen tegenover de kwalitatief betere inkjettechnologie. Ook in printcapaciteit kent de carbonrol zijn beperkingen en is deze afhankelijk van merk en type fax na een beperkt aantal afdrukken vol. Als de carbonrol vol is, dient deze vervangen te worden.
Op de volle carbonrol staan dan alle ontvangen faxen in spiegelbeeld. Dit is zeer interessant voor kwaadwillenden. Immers wanneer een carbonrol wordt afgerold en op een lichtbak wordt gelegd, zijn alle ontvangen faxberichten eenvoudig te lezen. Het is dus belangrijk om gebruikte carbon- of donorrollen zorgvuldig af te voeren en te vernietigen.
Vanuit het oogpunt van informatiebeveiliging is het inrichten van een proces voor de vernietiging van carbonrollen een belangrijke kwestie die niet mag worden vergeten.

Conclusie

De aanschaf en vervanging van kopieermachines, faxapparaten en printers door multifunctionals is het facility management ontstegen. Meer en meer IT-functionaliteiten komen beschikbaar op multifunctionals. Regelmatig komen er zelfs software patchs beschikbaar voor multifunctionals. Het is dus zaak om een multifunctional te zien als een volwaardig IT-component en de processen en procedures in te richten zoals we dat in IT gewend zijn.

Tips:

- *Sta niet toe dat de harde schijf van een multifunctional als opslagmedium wordt gebruikt voor bestanden (bijvoorbeeld archivering).*
- *Zet bij een multifunctional de mogelijkheid om data te wissen (disk overwrite) aan. Data wordt dan gewist direct na het verwerken van een opdracht.*
- *Verwijder dagelijks de achtergebleven opdrachten (bijvoorbeeld scan-, print- en kopieeropdrachten) die zijn opgeslagen op de harde schijf.*
- *Stel de multifunctional zo in dat data in zijn geheel gewist kunnen worden, mocht dit noodzakelijk worden geacht.*
- *Zet, indien mogelijk, versleuteling van de harde schijf aan.*
- *Sta 'scan to e-mail' en 'scan to fax' alleen toe indien wordt voorkomen dat ongeautoriseerd gegevens buiten de organisatie worden gebracht en niet achterhaald kan worden wie de verzender is.*
- *De standaard administrator wachtwoorden/ pincodes voor multifunctional zijn algemeen bekend, verander deze dus.*
- *Voer regelmatig penetratietesten uit op multifunctionals.*
- *Verwijder en vernietig bij einde lease- of huurcontract de harde schijf uit de multifunctional.*

Links

- *http://www.governmentsecurity.org/articles/HackingMulti-FunctionalPrinters.php*
- *http://www.scmagazineus.com/Copiers-are-also-a-compliance-issue/article/35180/*