Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

NBV Whitepaper
Kopieerapparaten en Multifunctionals

Recent onderzoek in de VS heeft wederom aangetoond dat afgestoten kopieermachines met harde schijven nog vele bedrijfsgeheimen of privacy gevoelige gegevens bevatten. Voldoende reden om ook in Nederland de zaak wederom onder de aandacht te brengen.

Inhoud

Risico's bij gebruik

Wat zijn multifunctionals?[1]

Multifunctionals is een verzamelnaam voor apparatuur veelal aangesloten aan een netwerk dat over een diversiteit aan functionaliteiten beschikt. Deze functies kunnen zijn:

1. kopiëren
2. scannen
3. faxen
4. printen
5. e-mailen

Het voordeel van zo'n machine is dat alle functies zijn geïntegreerd in één apparaat. Dit is vaak voordeliger dan allemaal losse apparatuur en bespaart aan-zienlijk op ruimtebeslag, maar vormt als single point of failure een kwetsbaarheid. Het onderhoud is veelal eenvoudiger en goedkoper doordat men met één leverancier te maken heeft.

Een multifunctional is voor de uitoefening van zijn functionaliteit aangesloten aan het computernetwerk en maakt ook integraal onderdeel daarvan uit. Voor het beheer en onderhoud gelden in principe dezelfde regels als voor computerapparatuur.

Bij een nadere beschouwing verschilt zo'n multifunctional nagenoeg niet van de gewone desktop PC. Onderzoek leert dat er juist veel overeenkomsten zijn. Een multifunctional beschikt namelijk eveneens over een:

1. netwerkkaart (en dus een IP -adres)
2. operating systeem
3. display
4. intern geheugen (RAM of flash memory)
5. harde schijf
6. modem (aansluiting op telefoonlijn)

Wat zijn de dreigingen en risico's?

Juist omdat de multifunctional zoveel overeenkomsten vertoont met de desktop PC, gelden ook hiervoor dezelfde dreigingen en risico's. Wat zijn deze specifieke risico's en dreigingen? De meest in het oog springende en ook meest over het hoofd geziene risico's vormen wel de interne harddisk en de netwerk en/of de modemaansluiting.

1. Voordat de multifunctional een afdruk maakt van een document, het per fax verzendt of scant, wordt het document in de meeste gevallen opgeslagen op de harde schijf. Nadat de functie is uitgevoerd blijft het document achter op de disk zonder dat het direct wordt gewist of overschreven. Recent onderzoek in de VS heeft wederom aangetoond dat afgestoten kopieermachines met harde schijven nog vele bedrijfsgeheimen of privacy gevoelige gegevens bevatten. Ook is er een levendige handel in tweedehands machines.
2. In veel gevallen zijn de multi-functionals voor onderhoudsdoel-einden van buitenaf toegankelijk voor de leverancier. Vaak gebeurt dit door middel van een modem-verbinding en soms ook door middel van een internet/netwerkverbinding. Deze remote access of monitoring verbindingen vormen een wellicht nog grotere dreiging op de vertrouwelijkheid van de gegevens zoals opgeslagen op de harde schijf van de multifunctional.
3. In de meeste gevallen maakt het randapparaat door middel van een netwerk-kop-peling deel uit van het interne bedrijfsnetwerk. Een ongecontroleerde externe koppeling, zoals hierboven beschreven of via internet, vormt een dreiging voor de vertrouwelijkheid en integriteit maar ook voor de beschikbaarheid van data binnen het bedrijfsnetwerk.

Wat zijn de oplossingen?

Om de risico's te beperken ten aanzien van deze apparatuur dienen ze bij afstoting dezelfde procedure te ondergaan als die geldt voor desktop PC's. Dat wil zeggen:

1. Alle geheugenonderdelen dienen te worden verwijderd, dan wel gewist. Harde schijven kunnen bijvoorbeeld worden gewist met de bekende Blancco Data Cleaner zoals die door het NBV is geëvalueerd. Ook het ingebouwde flash geheugen dient te worden geschoond of geheel te worden verwijderd bij afstoting.
2. Bij sommige typen is het mogelijk bij afsluiten van het contract te opteren voor een automatische wisfunctionaliteit[2]. Als het opgeslagen document niet meer benodigd is, wordt deze direct gewist.
3. Bij andere type multifunctionals is het zelfs mogelijk om de harde schijf de data automatisch te laten encrypten2 zodat bij afstoting alleen de sleutel vernietigd hoeft te worden.
4. Een remote access aansluiting is in feite een externe koppeling op uw netwerk en dient te voldoen aan uw interne beveiligingsrichtlijnen voor dergelijke koppelingen. Als er geen regelgeving voor bestaat of als u het risico op compromittering te groot acht, kunt u het nut en de noodzaak van deze remote access functionaliteit heroverwegen.

Samengevat

1. Bij afstoting harde schijven en flash memory wissen of verwijderen.
2. Automatische wisfunctionaliteit harde schijf als optie toevoegen via het contract met de leverancier.
3. Harde schijven encrypten als optie via het contract met de leverancier.
4. De remote access functionaliteit heroverwegen en/of afsluiten.

---

[1] Daar waar wordt gesproken over multifunctional wordt ook het gewone kopieerapparaat bedoeld.
[2] Nader onderzoek door bijv. het NBV zou de kwaliteit daarvan moeten uitwijzen.

Terug naar boven

Colofon

Voor nadere informatie kan contact worden opgenomen met het NBV: nbv@minbzk.nl

Deze whitepaper is ook terug te vinden op de NBV website.