Kantoorprinters: vaak onveilig!

Hoge resolutie, dubbelzijdige afdrukken, geniet, in kleur en verbonden aan het netwerk: het printwerk wordt steeds mooier en sneller. De keerzijde is dat steeds vaker onveilig wordt omgegaan met de 'originelen' en de informatie die opgeslagen raakt in de printer zelf. Van die keerzijde probeert het European Network Information Security Agency (ENISA) ons allen te doordringen met een publicatie die is gebaseerd op de 'controls' uit de meest recente versie van de Code voor Informatiebeveiliging.

Het ENISA rapport (*1) is gebaseerd op een onderzoek naar de Good Practices in 350 organisaties in Frankrijk, Engeland en Duitsland. Het probleem dat wordt geconstateerd is dat de documentenstroom die via de moderne multifunctionele kopieer-, fax- en printersystemen loopt, veelal bedrijfsvertrouwelijke of nog gevoeliger informatie bevat. De scanner/copiers/printers worden echter vaak op plaatsen opgesteld waar niet of nauwelijks toezicht is, noch op kwaadwillige medewerkers, noch op de onderhoudstechnicus want het is 'toch maar een printer'. Het ENISA rapport kijkt naar de Code voor Informatiebeveiliging (*2) en enkele andere Good Practice standaarden. Geconstateerd wordt dat voor printers de volgende aspecten geregeld moeten zijn: beleid, de organisatie van de informatiebeveiliging, apparatuurbeheer, fysieke en omgevingsbeveiliging, communicatie en operationeel beheer, toegangscontrole, beveiligingincidentmanagement, configuratiebeheer en bedrijfscontinuïteit. Veilig afdrukken, scannen en kopiëren vereist echter een beheerste controle over de apparatuur, degenen die toegang tot de apparatuur hebben (eigen werknemers, ingehuurde derden, bezoekers) en de geproduceerde, verwerkte en verzonden documenten.

Management-summary

Stilaanderwijs worden printers steeds beter. Ze worden ook steeds intelligenter, multifunctioneler en hangen aan het bedrijfsnetwerk. Dat printers en printsystemen ook een keerzijde hebben ontgaat nog menig beveiligingsverantwoordelijke. Ook de wijze waarop wordt omgegaan met de vaak bedrijfsvertrouwelijke afgedrukte documenten kan beter. Zelfs de Europese Unie is opgevallen dat het risico moet worden ingeperkt.

Herhaalknop Gewaarschuwd wordt dat dergelijke fax/kopieer/printsystemen in veel bedrijven in een open, ongecontroleerde ruimte staan opgesteld (gangen, zijkamertjes, naast de koffieautomaat). Ze geven ongeautoriseerden inzicht in de concept- en eindoffertes, verkoopprognoses en vele andere gevoelige documenten. Een ongeautoriseerde kan met een simpele druk op de kopieer- of herhaalknop een extra afdruk maken of het document direct per fax naar buiten sturen; geen haan kraait daarnaar. En als het 'origineel' niet in de printerbak of naast de printer rondzwerft, dan wordt al gauw gedacht dat een collega die waarschijnlijk per ongeluk heeft meegenomen in zijn stapel afdrukken. Even opnieuw op de printknop drukken... niemand denkt na over de mogelijkheid van bedrijfsspionage. Het door het ENISA rapport geïdentificeerde risico omvat onder andere imago- en reputatieschade door lekkage (bijvoorbeeld een rechtstreeks aan een krant gefaxte kopie), bedrijfsschade (zoals een verloren offerte), gevoelige informatie in verkeerde handen (zowel intern, denk aan personeelsvertrouwelijke informatie, als extern), risico van het bestaan van extra elektronisch gescande documenten waarvan de tijdige vernietiging niet is geregeld (bijvoorbeeld conflict met Wet Bescherming Persoonsgegevens) en het opzettelijk buiten gebruik stellen van de apparatuur.

Wat weinigen, zelfs niet de techneuten in de meeste organisaties, beseffen is dat veel van de moderne (multifunctionele) printers een normaal computersysteem bevatten met uitgebreide netwerkfaciliteiten, een normaal besturingssysteem zonder dichtgetimmerde beveiliging en een grote harde schijf waarop de gescande documenten worden opgeslagen en de afdruk- en verzendopdrachten eerst klaargezet worden. Dat geeft de mogelijkheid van het ongezien versturen of afdrukken van kopieën of documenten door onbevoegde derden. Eerder gescande documenten kunnen naar een ongeautoriseerde binnen of buiten de organisatie worden gestuurd. Ook kan een onderhoudstechnicus de harde schijf wisselen en vele Gigabytes aan eerder gescande, gekopieerde en geprinte ▸

documenten meenemen. De office manager is al gauw blij dat naast het oplossen van de storing ook even preventief en 'gratis' de harde schijf wordt vervangen.

Hackers Daar de multifunctionele printers vaak door een administratieve afdeling of de repro worden aangeschaft en daarna door ICT-beheer op een namiddag in het netwerk moeten worden gehangen, wordt over het hoofd gezien dat dergelijke printsystemen vaak zijn voorzien van een breed palet aan protocollen, zodat ze probleemloos in iedere netwerkomgeving kunnen worden aangesloten. Dat de veelal te open instellingen van FTP, Telnet, SNMP en webservers daarmee een aanval- en uitvalsplatform bieden aan externe hackers, botnets en andere malware ontgaat de beveiligingsverantwoordelijken. Dit probleem is niet nieuw, een aantal jaren geleden was het als gast van het bedrijf al mogelijk in twee onbewaakte minuten de printer van de directeur logisch gezien om te wisselen met de printer in de bewakingsloge of ervoor kiezen de gehele printstroom naar buiten te brengen. Binnen de Amerikaanse Defensie liep zelfs een printstroom via een systeem in Kiev, Oekraïne.
Met de nieuwe printsystemen is de problematiek alleen maar groter geworden. Hackers kunnen tegenwoordig de netwerkprinters herconfigureren, printstromen omleiden, eerder gescande, gekopieerde en afgedrukte documenten naar buiten sturen en nog meer onheil aanrichten die niet alleen de vertrouwelijkheid, maar ook de integriteit van afgedrukte documenten kunnen aantasten. Als een document uit de printer komt, dan zal die toch wel gelijk zijn aan de verstuurde afdruk?

Good Practices Om het risico uit te sluiten geeft ENISA in het tweede deel van het rapport een aantal aanbevelingen en checklists met maatregelen. Afhankelijk van de grootte en complexiteit van de organisatie, kunnen die in lichtere of zwaardere mate worden geïmplementeerd. Daaronder vallen de fysieke beveiliging van de printers en de omgeving waarin ze staan opgesteld, het oog houden op de ingebouwde harde schijven, goed systeembeheer en het dichtzetten van ongebruikte toegangen, controle op faxberichten, controle op onderhouds- en reparatieactiviteiten. En voor wie toch eens naar de documentstromen kijkt: kijk eens met de lunchpauze, 's avonds en in het weekeinde naar welke gevoelige documenten er bij de printers rondslingeren en in de daarnaast geplaatste afvalbakken liggen!

■ Ir. Eric Luiijf
Eric.Luiijf@beveiliging.nl

Referenties
1) ENISA report 'Secure Printing', april 2008. http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf
2) ISO/IEC 17799:2005 – ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management, in Nederland bekend als de Code voor Informatiebeveiliging (NEN-ISO/IEC 17799:2005 / NEN-ISO/IEC 27002:2007).