Multifunctionele printers: vaak onveilig!

Auteur: Eric Luijf > Ir. Eric Luijf is te bereiken via eric.luijf@tno.nl.

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 met 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 (1) die gebaseerd is op de 'controls' uit de meest recente versie van de Code voor Informatiebeveiliging (2).

Het ENISA rapport is gebaseerd op een onderzoek naar de Good Practices in 350 organisaties in Frankrijk, Engeland en Duitsland. Het probleem dat geconstateerd wordt 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 informatiebeveiliging, apparatuurbeheer, fysieke en omgevingsbeveiliging, communicatie en operationeel beheer, toegangscontrole, beveiligingincidentmanagement, configuratiebeheer en bedrijfscontinuïteit. Veilig afdrukken, scannen en kopiëren vereist echter een beheerste controle van de apparatuur, degenen die toegang tot de apparatuur hebben (eigen werknemers, ingehuurde derden, bezoekers) en de geproduceerde, verwerkte en verzonden documenten.

Gewaarschuwd wordt dat dergelijke fax/kopieer/printsystemen in veel bedrijven in een open, ongecontroleerde ruimte opgesteld staan (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 ligt of naast de printer rondzwerft, dan wordt al gauw gedacht dat een collega het waarschijnlijk per ongeluk meegenomen heeft 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 (bijvoorbeeld 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 waar de tijdige vernietiging niet van geregeld is (bijvoorbeeld conflict met Wet Bescherming Persoonsgegevens), het opzettelijk buiten gebruik stellen van de apparatuur enzovoorts.
Wat weinigen, zelfs niet de techneuten van 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 gestuurd worden. Ook kan een onderhoudstechnicus de harde schijf wisselen en vele gigabytes aan eerder gescande, gekopieerde en geprinte documenten meenemen. U bent tenslotte blij dat hij of zij de storing oplost en ook even preventief en 'gratis' de harde schijf vervangt.

Uitvalsbasis voor 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 voorzien zijn 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 aanvals- en uitvalsplatform bieden aan externe hackers, botnets en andere malware ontgaat de beveiligingsverantwoordelijken. Dit probleem is niet nieuw, een aantal jaren geleden al kon je als gast van een bedrijf in twee onbewaakte minuten de printer van de directeur logisch gezien omwisselen 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, Rusland... 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

vervolg onderaan volgende pagina>>

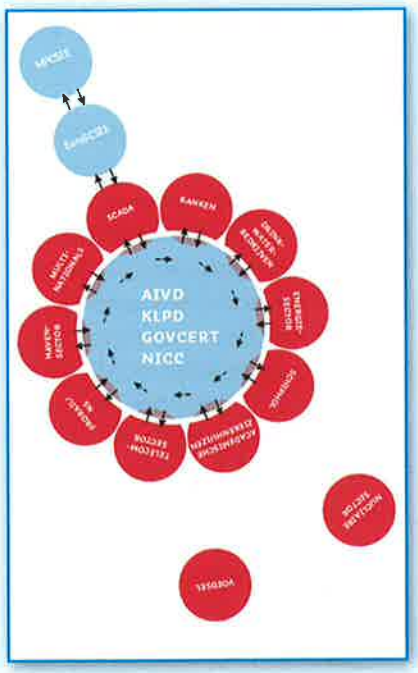
Verslag van het tweede Process Control Security Event van het NICC

Are you in control?

Auteur: Ing. Patrick Borsoi

Op 4 december jl. vond alweer het tweede Process Control Security Event van het NICC plaats, deze keer bij de TU Delft. In nummer 4, het juni-nummer van het afgelopen jaar, van dit blad is verslag gedaan van het eerste event.

Het event begon met een lopende lunch in de foyer van het aulagebouw, waar een tiental vendors bescheiden informatiestands had ingericht. De dag werd namelijk georganiseerd in samenwerking met de Federatie van Technologiebranches (FHI), die gelijktijdig haar Productie Proces Automatiseringsdag (PPA-dag) hield. In haar openingstoespraak maakte Annemarie Zielstra, programmamanager van het NICC, melding van een aantal nieuwe aansluitingen op het Informatieknooppunt Cybercrime, dat via het zogenoemde bloemblaadjesmodel per sector (bijvoorbeeld banken, energie, Schiphol, SCADA) faciliteert in het vertrouwelijk delen van informatie over incidenten, dreigingen en good practices. De kern van het bloemblaadjesmodel wordt gevormd door AIVD, KLPD, GovCERT en NICC. Belangrijke mijlpaal is het toetreden van deelnemers van de WIB (gebruikersorganisatie) tot de European SCADA Control Systems Information Exchange (EuroSCSIE) en de oprichting van een internationaal uitwisselingsplatform op het terrein van SCADA en Process Control. Het NICC participeert in beide platforms.



Het bloemblaadjesmodel

Het tweede deel van de plenaire sessie bestond uit een debat tussen dagvoorzitter Cor Ottens, Reinder Woldring van de Gasunie en in deze sessie optredend als co-moderator, Aad Dekker van Nuon en Ted Angevaare van Shell. Woldring introduceerde een alternatieve uitdrukking voor 'in control zijn': namelijk 'in secure zijn'. De spatie is bij deze term wel cruciaal! Process control security betekent volgens Aangevaare het robuust maken van systemen tegen aanvallen door hackers en virussen. Hij is in control als de verwachte olie- en gasproductie wordt gehaald. Dekkers visie was dat de klant er niets van mag merken als het een keer misgaat. Een vraag die deze middag steeds weer terugkeerde, was deze: wie is eindverantwoordelijk voor process control security? Bij Nuon ligt deze verantwoordelijkheid in de lijn, terwijl deze bij Shell bij de asset manager in een land ligt. Angevaare noemde het een misvatting dat één CIO wereldwijd verantwoordelijk zou kunnen zijn. Wel is binnen zijn bedrijf

vervolg volgende pagina>>

meer onheil aanrichten die niet alleen de vertrouwelijkheid, maar ook de integriteit van afgedrukte documenten aan kunnen tasten. Als een document uit de printer komt, dan zal dat 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 geïmplementeerd worden. Daaronder vallen de fysieke beveiliging van de printers en de omgeving waarin ze opgesteld staan, 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 als u toch naar de documentstromen kijkt, kijk dan eens tijdens de lunchpauze, 's avonds en in het weekeinde naar welke gevoelige documenten er bij de printers rondslingeren en welke er in de de daarnaast geplaatste afvalbakken liggen.

Dit artikel is eerder verschenen in het blad Beveiliging.

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)