COLUMN

Ir. Teus van der Plaat, IVENT Research en Innovatie Centrum

CYBER: NIEUWE TERM, OUD PROBLEEM

Cyber is een breed begrip. Cyber warfare, cyber defense, cyber intelligence, cyber….., er zijn veel invalshoeken. In deze column wil ik het thema vooral behandelen vanuit de ervaringen die IVENT en daarvoor DTO al vele jaren heeft met de onveiligheid op internet.

Het is misschien al tien jaar geleden dat we in de bedrijfskantine van Maasland tijdens de lunchpauze een hevige discussie hadden over de toen al aanzwellende gevaren van de koppeling met internet. De eerst firewall was al in bedrijf voor uitsluitend e-mail en file transfer contact met de buitenwereld. De BA (BeveiligingsAutoriteit) van Defensie voorzag toen al de gevaren van een directe koppeling met het internet voor het browser verkeer. In de discussie werden vele opties besproken om een koppeling te maken, maar iedere keer kwam het erop neer dat een open IP-koppeling, hoe goed deze ook zou worden beveiligd of hoe weinig poorten open zouden worden gezet, altijd een aanzienlijk beveiligingsrisico zou inhouden. Op een servetje werd toen het idee geboren om de IP stroom te onderbreken door naar de browser te kijken via een thin client protocol en de directe IP koppeling niet toe te staan. Na vele uren discussie en testen gaf de BA uiteindelijk een waiver om een dienst te ontwikkelen met behulp van het Citrix protocol. Dat ging letterlijk met horten en stoten en bleek ook vrij duur te zijn. Immers, alle processing van de browser moest op speciale servers geschieden. In de piektijd van deze oplossing draaiden er bijna 70 servers, die elk enkele tientallen Internet Explorer browsers draaiden. De situatie was niet ideaal, maar er was een connectie. Na enige tijd kwam de Firefox browser opzetten en kreeg een steeds groter marktaandeel. Daarnaast was er behoefte tot uitbreiding. Door het Kenniscentrum en later het RIC is toen een nieuwe variant ontwikkeld met uitsluitend Open Source software. Dit had een groot aantal voordelen. Allereerst bleek uit testen dat met exact dezelfde hardware er veel meer performance uit een Firefox, Linux en open source terminal emulatie software combinatie te halen viel dan de oude configuratie. Per saldo was er een performance winst van zeker 100%. Daarnaast bleek de virusgevoeligheid van Firefox een stuk kleiner en kon het Linux operating system zodanig worden gestript dat uitsluitend die elementen aanwezig waren die nodig zijn om een browser goed te laten draaien. Daarnaast kon ook de belasting van het systeem sterk worden opgevoerd en werden de opeenvolgende releases van Firefox steeds sneller en zuiniger met de CPU cycles.

Uiteindelijk heeft dit geresulteerd in een nieuwe versie van IODW (internet op de werkplek) die momenteel nagenoeg probleemloos draait. Konden in de oude setting maximaal 2.400 concurrent gebruikers gebruik maken van internet, op dit moment kan dat met minder servers gemakkelijk door 6.000 concurrent gebruikers. Als u dit leest zijn de thans aanwezige 32 servers vervangen door 16 nieuwe blade servers die gezamenlijk een capaciteit hebben van 8.000 concurrent gebruikers. De nieuwe blade servers beschikken over 22 cores per blade. Deze alternatieve oplossing biedt ook grote voordelen aan de client kant. Immers, hoewel men uiteraard de desktop en laptop goed moet beheren door daar antivirus op te draaien en tijdig patches aan te brengen, is de cliënt veel minder kwetsbaar geworden omdat er geen directe internetkoppeling aanwezig is. Dus ook de patchbeheerinspanningen van de client kunnen op een meer rustige en evenwichtige wijze worden uitgevoerd. Ten aanzien van de cyber kwetsbaarheid kan worden gesteld dat via deze koppeling nagenoeg geen infecties plaatsvinden op het defensienetwerk (98% van alle hackpogingen hebben volgens recent onderzoek van Verizon altijd een patroon van infectie van eindstations of servers, waarna via een ip-verbinding contact wordt gezocht met het internet om de server op afstand te modificeren of om data te lekken). Aangezien de door Defensie gebruikte constructie geen open internetverbinding kent, stranden nagenoeg alle pogingen in schoonheid. Inmiddels zijn de kosten van beheer van reguliere oplossingen dusdanig toegenomen dat de defensieoplossing, ook door de gedaalde hardware kosten en het gebruik van uitsluitend Open Source producten, aanzienlijk goedkoper is geworden dan commerciële oplossingen. Dus het is veiliger en goedkoper dan oplossingen uit de markt. Er zit een nadeel aan de oplossing: streaming audio en video werkt niet geweldig. Maar de behoefte daaraan is niet zo groot en over enige tijd komt er een softwareversie aan die ook dat goed gaat ondersteunen. In feite is ook de telestick op min of meer dezelfde principes gebaseerd, zij het dat de oplossing daar “omgekeerd” wordt toegepast. De ontwikkeling van de hardware staat niet stil. In de nabije toekomst komen er veel krachtiger servers op de markt die ook nog weer aanzienlijk goedkoper zijn en minder stroom vergen. Zo komt er binnenkort een server uit met bijna 3.000 cores gebaseerd op de ARM architectuur. Een enkele server kan dan gemakkelijk de totale defensie-internetload verwerken met een capaciteit die normaal zeker een factor twee groter zal zijn. De echte dreiging komt momenteel vanuit de vele nieuwe Buy Your Own Device (BYOD) apparatuur zoals smartphones, tablets en andere apparatuur. Vele bedrijven maken zich ernstige zorgen over de beveiliging na introductie van deze apparatuur, veelal zelf gekocht door de medewerkers. Recent is IVENT in contact gekomen met Intel, dat een prachtige beveiligingsarchitectuur heeft ontworpen voor alle voorkomende apparatuur, waarbij plaats-, tijd- en locatieafhankelijke data wel of niet ontsloten wordt. IVENT gaat een studie maken van deze architectuur om te kijken of er elementen of delen te gebruiken zijn binnen Defensie. Immers ook binnen Defensie hebben we in toenemende mate te maken met medewerkers die hun eigen spullen meenemen en onwillekeurig is een trend om daar toch defensie-informatie op te zetten, gewenst of niet. Hoewel officieel alleen unclass wordt toegestaan, is een foutje bewust of onbewust zo gemaakt en halen we weer de krant met nu niet een verloren USB-stick, maar met een verloren tablet of e-reader….. De imagoschade is dan gelijk heel groot. Daarom onderzoeken we of er ook een versie van de telestick kan worden gemaakt voor tablets. Hoewel we al op sommige tablets succesvol geboot hebben, ligt hier nog een lange weg te gaan. Een volgende keer zal ik hier wel meer over schrijven.