Afschermen voor indringers

Hoe is een netwerk te maken dat de buitenwereld buiten houdt

35 Jaar geleden startte Modelec met de verkoop van elektronicaonderdelen. Na enige tijd kwamen daar computers bij en ondertussen heeft men zich gespecialiseerd in het leveren van complete systemen voor industriële netwerken, netwerken die bedoeld zijn voor de zware omstandigheden die we tegen komen bij grote bedrijven zoals de staal- en petrochemische industrie. Netwerken waar hoge eisen aan gesteld worden met betrekking tot de betrouwbaarheid want bij deze bedrijven heeft het uitvallen van het netwerk veelal grote financiële gevolgen.

Vorige maand schreef ik in mijn voorwoord over de problemen die kunnen ontstaan als netwerken niet goed afgeschermd zijn voor indringers van buitenaf. Tegenwoordig zijn immers vele netwerken direct gekoppeld aan internet om zo de koppeling met computers op afstand een stuk eenvoudiger te maken. Deze verbinding maakt het echter ook mogelijk dat hackers het netwerk binnen kunnen komen om vervolgens allerlei ongewenste acties uit te voeren.
Hoe hou je hackers buiten de deur? Dit vraagt naast kennis van de manieren waarop hackers te werk gaan ook om kennis van de diverse netwerkcomponenten die kunnen voorkomen dat hackers binnen kunnen komen. Gelukkig zijn er verschillende bedrijven de over deze kennis beschikken en ook de componenten maken om netwerken adequaat te beschermen.

Meer dan een wachtwoord

De eerste stap om een netwerk te beschermen, is het toepassen van wachtwoorden gekoppeld aan gebruikers. Deze methode wordt heel veel toegepast op internet, maar echt veilig is dit niet. Wachtwoorden kunnen immers achterhaald worden of al dan niet bewust op straat komen te liggen. Daarbij komt dan nog dat je als netwerkbeheerder met een wachtwoordsysteem nooit zelf goed kunt nagaan of de gebruiker van het wachtwoord een vertrouwde gebruiker is of een ongewenste gast.
Veel van de componenten die binnen een industrieel netwerk toegepast worden, zoals de PLC's en besturingscomputers hebben niet de mogelijkheden om een goede firewall of anti virussoftware te installeren. Wachtwoorden zijn dan de enige bescherming tegen indringers, maar voor kritische applicaties is dit echt niet de beveiliging die aan te raden is. Het hoeft ook niet, want er zijn ook hardwareoplossingen die wel voor de nodige beveiliging zorgen.

De juiste componenten

In ons land zijn er zeer veel pompstations, sluizen, bruggen en niet te vergeten alle matrixborden boven de snelweg die allemaal op afstand bediend worden. Al deze applicaties zijn gekoppeld aan een SCADA-systeem dat voor de verbinding gebruik maakt van een netwerk. Veelal verloopt dit netwerk gewoon via internet, omdat dit gemakkelijk is en de bediening vanuit elke plek op de wereld plaats kan vinden. Ook kunnen door de koppeling gemakkelijk foutmeldingen naar de juiste mensen verstuurd worden via email of SMS.
Het gemak van de koppeling met internet levert ook gevaren op. Vorige maand schreef ik al over de sluis die door hackers kon worden geopend omdat de beveiliging met een wel heel erg simpele wachtwoorden was uitgevoerd. Gelukkig heeft deze situatie geen grote schadelijke gevolgen opgeleverd, maar voor hetzelfde geld was dit wel volkomen fout gegaan. De situatie gaf wel aan dat hier een goede beveiliging ontbrak en er hoognodig iets gedaan moest worden.
Allereerst is dit natuurlijk het aanpassen van de wachtwoorden, maar veel beter is het om er voor te zorgen dat de verbinding met internet loopt via netwerkcomponenten die er voor zorgen dat alleen geautoriseerde berichten doorgegeven worden. Een goede hardware firewall is dan het gemakkelijkste. Dit apparaat filtert de gewenste berichten uit de grote brij aan ongewenste berichten en stuurt die door naar de netwerkonderdelen waarvoor deze bestemd zijn. Daarbij speelt snelheid een belangrijke rol, want het is immers niet wenselijk als er door de firewall de nodige vertraging optreedt. Zeker niet als er via het beveiligde netwerk ook videosignalen overgedragen moeten worden, een situatie die bij veel op afstand bestuurbare applicaties voorkomt. Op de plek waar de besturing plaats vindt, wil men immers wel zien wat er aan de andere kant van de 'lijn' allemaal gebeurt. Bij dit alles komt dan nog dat de gebruikte firewall geschikt moet zijn voor het netwerk en de gebruikte netwerktechnologie en niet te vergeten de omgevingsomstandigheden waar deze geplaatst wordt. In een pompstation ergens op een afgelegen plek zijn temperatuur en vochtigheid slechts zelden overeenkomstig met die in een bureauomgeving en ook mechanische belastingen zoals trillingen komen geregeld voor. Hier moeten natuurlijk alle netwerkcomponenten wel mee overweg kunnen en dus ook de toe te passen hardware firewall.

De specialist

Wie op internet gaat zoeken naar een hardware firewall, zal de nodige apparaten tegen komen, maar al snel zal duidelijk worden dat het lastig is om uit te zoeken welke voor uw applicatie het meest geschikt is. Het maken van de juiste keuze vraag de nodige netwerkkennis en ervaring. Ook de hacker heeft heel veel moeten studeren om de juiste manieren te vinden om een netwerk binnen te komen, dus zal ook degene die moet voorkomen dat de hacker binnen kan komen, over een minstens even grote hoeveelheid kennis moeten beschikken.
Het vinden van de beste oplossing is dan ook voer voor specialisten, specialisten zoals u die vindt bij Modelec. In de 35 jaar dat zij zich bezig houden met oplossingen voor de industrie heeft men zich dusdanig gespecialiseerd dat zij snel een oplossing kunnen bedenken die optimaal is voor uw applicatie. Daarbij worden zij weer ondersteund door verschillende leveranciers. Zo vertegenwoordigen zij Moxa, een bedrijf dat verschillende netwerkcomponenten maakt speciaal bedoeld voor industriële toepassingen. Hieronder ook intelligente firewalls die voorzien zijn van de juiste algoritmen om hackers buiten de deur te houden en voor versleuteld dataverkeer zorgen. Een bezoekje aan de site van Moxa is in dit kader dan ook meer dan interessant. In de afdeling white papers is de nodige achtergrondinformatie te vinden die u inzicht geeft in de problematiek. •

www.modelec.nl

Voor meer informatie www.etotaal.nl/achtergrond.
Artikel "Afschermen voor indringers".

Ewout de Ruiter