

Firewall besnuffelt applicaties

De meeste organisaties denken niet meer echt na over de beschermingsmuur rond het netwerk, de firewall. Hij is een standaard netwerkcomponent geworden.

Toch staan de ontwikkelingen op het gebied van firewalls zeker niet stil. Application Aware Firewall (AAF) en Web Application Firewall (WAF) zijn inmiddels veelgehoorde termen. Gaat het hier om dezelfde wijn in nieuwe zakken?

CORNÉ DE KEIZER



De traditionele firewall is niet voldoende in het 'webtijdperk'. Bescherming van data moet nu voorop staan.

Het gebruik van applicaties vanaf of via internet neemt hand over hand toe. Daarbij gaat het ook om bedrijfsapplicaties die medewerkers op allerlei locaties gebruiken: op kantoor, thuis of onderweg. De grenzen van het netwerk vervagen. Dat betekent dat de rol van de firewall verandert.

cloud computing is het architectuurmodel voor webgebaseerd computergebruik. De cloud is daarbij een metafoor voor het open en ontastbare internet. In de cloud worden applicaties aangeboden en gebruikt als Software-as-a-Service (SaaS). De verandering van een interne, gesloten netwerkomgeving, naar cloud computing vraagt om een slimme en innovatieve beveiligingsstrategie. Daarin staat niet de verdedigingswal centraal, maar de te beschermen data. Waar deze zich ook bevindt; binnen of buiten de muren van de organisatie. De kennis, expertise en ervaring die ten grondslag liggen aan deze methodiek om beveiliging te optimaliseren, wordt het gedachtegoed van Jericho genoemd.

Volgens het Jericho Forum is het eigen bedrijfsnetwerk onderdeel van het onveilige internet. 'Jericho' verplaatst eenvoudigweg de beveiliging van het netwerk naar de gegevens zelf. De traditionele grens tussen binnen en buiten komt daarmee te vervallen. Een begrenzing is in het Engels een perimeter; daarom noemt het Jericho Forum dit concept 'De-perimeterization' ('ontgrenzing').



Volgens het Bijbelse verhaal is Jericho door de Israëlieten ingenomen door in zeven dagen totaal dertien keer rond de stadsmuur te lopen, waarna deze het bij de laatste keer begaf.

Hier een foto van het hedendaagse Jericho op de Westoever.

Firewalls verkennen nieuwe grenzen

Was een firewall voorheen een sterke muur die de 'bedrijfsvesting' beschermde, vandaag de dag hebben we te maken met telewerkers, extranetten en andere vormen van externe toegang. Daardoor zitten er tegenwoordig in de oude vertrouwde muur meer gaten dan in een Leerdammer kaas. Toch wil dat niet zeggen dat een firewall nutteloos is. Sterker nog, de rol is weliswaar anders, maar zeker niet kleiner.

Het Jericho Forum verspreidt kennis en promoot

een methodiek om IT-beveiliging ook in een open netwerkomgeving te handhaven. Data-beveiliging neemt daarbij de rol van firewalls over. In het gedachtegoed van Jericho zijn firewalls weliswaar niet langer houdbaar als enige of afdoende verdediging van het netwerk. De-perimeterization betekent echter niet dat firewalls hun langste tijd hebben gehad. Er zijn zelfs drie ontwikkelingen waardoor firewalls ook in het gedachtegoed van Jericho een belangrijke beveiligingsmaatregel blijven:

- 1 Volgens de richtlijnen van Jericho is het kantoornetwerk voortaan een onderdeel van internet. De introductie van beveiligingszones maakt het mogelijk het netwerk op te knippen in veilige delen die ieder een kleine set van informatiesystemen met hoge vertrouwelijkheid bevatten (Jericho beginsel 11). Dit wordt beveiligd met een netwerkfirewall met hoge doorvoersnelheden en intrusion preventietechnieken.
- 2 Jericho beginsel 5 onderschrijft de potentiële schade van malware (zoals virussen en spyware) voor kwetsbare pc's. Een veilig gebruik van internetdiensten is daarom essentieel. Firewalls met kennis van internetapplicaties vervangen daarom de traditionele firewalls. Dit heet een Application Aware Firewall (AAF). Een implementatie van eindpuntbe-



veiliging (het beveiligen van alle apparaten die toegang krijgen tot bedrijfsnetwerken via internet), is volgens Jericho nagenoeg altijd vereist.

- 3 Door de implementatie van beveiligde netwerkzones tussen het datacenter en internet zijn extra maatregelen te treffen voor gegevensbeveiliging. Dit geldt vooral voor het extra beschermen van (internet)applicaties tegen misbruik. Dit is te doen met een Web Application Firewall (WAF).

Organisaties met een hoog risicoprofiel passen de genoemde voorbeelden al toe. Dit onderschrijft de stelling dat De-perimeterization de stap maakt van hype naar trend.

Het nieuwe beveiligen

Het gedachtegoed van het Jericho Forum heeft veel gevolgen voor netwerkbeveiliging. Daar waar voorheen de nadruk lag op het onder controle krijgen van de verkeersstromen, werd de daadwerkelijke data vergeten. Terwijl de echte waarde juist terug te vinden is in de data zelf. Het Jericho Forum hanteert dan ook als één van de grondbeginselen dat de data zelf beveiligd moet worden, in plaats van de verkeersstromen.

De Web Application Firewall en de Application Aware Firewall geven concreet invulling aan dit beginsel. Deze systemen voegen veel toe aan de traditionele vormen van firewalling. Het

verschil tussen deze twee is echter groot en is terug te vinden in de toepassing.

Application Aware Firewall

De Application Aware Firewall (AAF) komt in plaats van de traditionele firewall en helpt de organisatie bij het technisch afdwingen van

het beleidsregels rond internetgebruik. De 'Application'-component richt zich vooral op het verkeer van binnen naar buiten. Met andere woorden: wat mag een gebruiker op welke website doen?

Deze vraag is vooral van belang als medewerkers binnen organisaties socialemediakanalen

Elf beginselen van het Jericho Forum

De principes van het Jericho Forum zijn in uitgebreidere vorm te vinden op www.jerichoforum.org. Het Jericho Forum is onderdeel van The Open Group, een consortium met een ideële visie op toegang tot informatie op basis van open standaarden. Het Jericho Forum onderzoekt en adviseert over richtlijnen voor IT-beveiliging in een open netwerkgeving. Het gedachtegoed van het Jericho Forum is gebaseerd op de volgende, vrij vertaalde, elf richtlijnen voor informatiebeveiliging:

Leg een goed fundament

- 1 De omvang en mate van beveiliging moet toepasselijk zijn voor, en in verhouding staan tot, het risico.
- 2 Beveiligingsmechanismen moeten diep- en vergaand zijn, eenvoudig, schaalbaar en beheersbaar.
- 3 Maak grensoverschrijdende aannames over de risico's die gelopen worden. Houdt bijvoorbeeld rekening met de beperkingen van maatregelen, en met beperkingen buiten de eigen organisatie zoals locatie, wetgeving, etc.

Overleven op een vijandig internet

- 4 Apparatuur en programmatuur moeten communiceren via open, en inherent veilige protocollen.
- 5 Alle apparatuur moet in staat zijn om de veiligheid te kunnen waarborgen op een inherent onveilig netwerk (lees: internet).

De noodzaak van vertrouwen

- 6 Het niveau van wederzijds vertrouwen bij transacties tussen systemen, processen en technologie dient helder en transparant te zijn vastgelegd.
- 7 Wederzijds vertrouwen moet voor beide partijen gewaarborgd zijn.

Identiteit, management en samenwerking

- 8 De processen voor authenticatie, autorisatie en verantwoording moeten altijd samenwerken en uitwisselbaar zijn met locaties buiten de (gecontroleerde) omgeving.

Toegang tot data

- 9 Toegang tot data moet worden gecontroleerd door de (beveiligings)eigenschappen van de data zelf.
- 10 Privacy van gegevens (en de beveiliging van de data met hoge mate van betrouwbaarheid en integriteit) moet voldoen aan de scheiding tussen het technische functiebeheer en privileges.
- 11 In beginsel dient alle data voldoende te zijn beveiligd. Of deze nu wordt gebruikt, opgeslagen of getransporteerd (zoals e-mailen of kopiëren).

en andere online diensten gebruiken. Gezien de maatschappelijke ontwikkelingen en de zakelijke kansen die sociale media bieden, willen veel organisaties dit toestaan, in plaats van dit zonder meer te blokkeren. Dat vraagt echter wel om bedrijfsbeleid voor het gebruik van socialemediakanalen. Dit is er in feite op gericht om gebruikers handvatten geven hoe om te gaan met sociale media. Verkeerd gebruik van sociale media kan namelijk grote gevolgen hebben voor het imago van de organisatie. Zo is het vrij eenvoudig om, door onwetendheid of met opzet, vertrouwelijke documenten te lekken via sociale mediakanalen. Denk bijvoorbeeld aan WikiLeaks, maar ook LinkedIn, Facebook of Gmail brengen deze risico's met zich mee.

De AAF kan voorkomen dat medewerkers bestanden via de webinterface op internet publiceren. Met een AAF kunnen netwerkbeheerders mensen bijvoorbeeld toegang geven tot de webinterface van Gmail, terwijl zij het onmogelijk maken een bijlage te verzenden. De AAF heeft inhoudelijke kennis van Gmail en weet hoe Gmail omgaat met (bijvoorbeeld) bijlagen. Zo is het mogelijk beleidsregels op te stellen en te implementeren rondom webmail, maar bijvoorbeeld ook rondom LinkedIn, Twitter en andere populaire media, waarbij de organisatie het naleven van deze regels door gebruikers technisch afdwingt.

De AAF mag echter niet gezien worden als de oplossing die alle vormen van het lekken van data voorkomt. Medewerkers beschikken ook over apparaten die zij privé hebben aangeschaft, maar wel zakelijk gebruiken, zoals een smartphone, netbook- of tablet-pc. Daarmee kunnen zij alles wat zij maar willen online publiceren. Daarom is het van groot belang eerst een strategie uit te stippelen voor Data Leakage Prevention (DLP) en daarna pas de maatregelen en beleidsregels te definiëren. De raakvlakken tussen de AAF en DLP zijn groot. Het is daarom goed om de keuze voor een Application Aware Firewall te combineren met beleid rondom DLP.

Web Application Firewall

In tegenstelling tot de Application Aware Firewall is de Web Application Firewall (WAF) niet



Deze foto van het huidige Jericho (een militaire controlepost) laat zien dat een muur alleen niet voldoende is: de inhoud van pakketjes (bij dataverkeer) moet ook worden gecontroleerd.

De Application Aware Firewall kan voorkomen dat medewerkers bestanden via de webinterface op internet publiceren.

bedoeld als vervanger van de traditionele firewall. De WAF wordt ingezet om gepubliceerde webapplicaties te beschermen tegen aanvallen van buitenaf. In omgevingen zonder WAF zien we vaak een traditionele firewall in combinatie met Intrusion Detection & Prevention (IDP) om de webapplicatie te beschermen. Deze constructie voorziet echter niet in het controleren (monitoren en eventueel blokkeren) van het verkeer op daadwerkelijke inhoud; hooguit op basis van afwijking van protocollen en herkenbare aanvallen.

De WAF voorziet daar wel in, en voegt zodoende een beveiligingsdimensie toe. Alle verkeer naar en van de webapplicatie verloopt via de WAF. De WAF kent de applicatie inhoudelijk en weet bijvoorbeeld wat de te verwachten input is in invoervelden binnen de webapplicatie. Op het moment dat afwijking van de beleidsregels wordt geconstateerd, grijpt de WAF in. Dit varieert van het sturen van een alarm tot het blokkeren van het verkeer. De WAF beperkt zich niet tot de bekende of meest gebruikte applicaties. Sterker nog, voor een WAF maakt het juist niet uit welk type applicatie hij moet beschermen. Bescherming vindt plaats op basis van het profiel van de applicatie dat de WAF zichzelf aanleert.

Bij de eerste typen WAF's moesten netwerkbeheerders dit profiel met de hand configureren. Zij moesten zelf regels invoeren over welke (invul-)velden een applicatie heeft, en wat de toegestane waarden daarvan zijn. Al dus ontstond een profiel van de applicatie. Dat

betekent in feite dat een applicatie twee maal wordt gebouwd, wat niet alleen een tijdrovend proces is, maar ook foutgevoelig.

Applicatieprofielen

Ook het doorvoeren van wijzigingen in de applicatie heeft gevolgen voor het profiel. Het dynamisch opbouwen van applicatieprofielen is dan ook een logische vervolgstap. In eerste instantie controleert de WAF het verkeer naar en van de webapplicatie. Op basis van deze controle stelt hij vast hoe de applicatie in elkaar zit en aan welke voorwaarden de componenten binnen de applicatie moeten voldoen. De nieuwste WAF's zijn voorzien van geavanceerde algoritmen voor het dynamisch opbouwen van applicatieprofielen. De WAF leert het normale gedrag van de applicatie, op basis waarvan de beleidsregels worden afgedwongen.

Het inzetten van een WAF is echter meer dan het vaststellen van het applicatieprofiel alleen. Een goede WAF gebruikt een combinatie van maatregelen. Stel dat bepaald verkeer opeens buiten het profiel van de applicatie valt, dan hoeft dat niet per definitie een aanval te zijn. Het kan ook gaan om een uitzondering die wel gewoon wordt doorgelaten, of misschien een wijziging in de applicatie. Voorbeeld: een online verzekeringsapplicatie staat bepaalde karakters niet toe in het veld klantnaam, terwijl een nieuwe klant (om wat voor reden dan ook) een dergelijk karakter wel in de naam heeft. Dit mag niet een blokkering van het verkeer tot gevolg hebben. In dat geval is de kans namelijk

groot dat de verzekeraar een klant misloopt. Dit voorbeeld maakt duidelijk dat (te) rigide beleidsregels de organisatie tegenwerken en een negatief effect op de bedrijfsvoering hebben. De WAF kijkt daarom behalve naar het applicatieprofiel ook naar andere componenten. Denk aan het toetsen van het verkeer aan de protocollen, het herkennen van bekende aanvallen en de reputatie van de gebruiker.

De WAS correleert de resultaten en op basis hiervan besluit hij verkeer al dan niet te blokkeren. Dit geeft een hogere mate van betrouwbaarheid van de beveiligingsomgeving.

Sturen op inhoud

De Web Application Firewall en de Application Aware Firewall zijn totaal verschillende oplossingen ieder met een eigen specifiek doel. De

Web Application Firewall wordt ingezet om (zelf)gepubliceerde applicaties te beschermen, terwijl de Application Aware Firewall dient om de beleidsregels rondom het gebruik van sociale mediakanalen en publieke webservices af te dwingen. Beide technologieën voegen veel toe aan de traditionele vormen van netwerkbeveiliging, omdat veel meer valt te sturen op inhoud dan op platte verkeerstromen. Voor veel organisaties is dit een uitkomst.

Beide maatregelen zijn echter net zo krachtig als het bewustzijn van gebruikers. Een gebruiker die al dan niet bewust vertrouwelijke of gevoelige bedrijfsinformatie twittert, is niet tegen te houden. Men kan tenslotte altijd gebruik maken van privémiddelen om informatie te lekken. Vertrouwen en verantwoordelijkheid blijven cruciale factoren in databeveiliging.

Iets voor mij?

Is deze technologie interessant voor mij? Welke technologie moet ik dan toepassen? Zijn beide voor mijn organisatie noodzakelijk?

Ook hier begint het zoals altijd bij beleid en classificatie. Leg vast wat de waarde van de te beschermen gegevens is (impactanalyse). Leg ook vast welk verkeer is toegestaan en wat niet. Op basis daarvan is een overwogen keuze te maken. Afhankelijk van de impactanalyse is vast te stellen welke beleidsregels de organisatie technisch moet afdwingen. Vervolgens is de juiste oplossing te kiezen. ■

Corné de Keizer (CISSP, CISA)

is security consultant bij Motiv.