AAZOO MAAKT HET ONZICHTBARE ZICHTBAAR

WHITEPAPER

3 tips

om securitydreigingen in uw netwerk snel inzichtelijk te maken

Maak het onzichtbare zichtbaar

Van kleine mkb'ers tot grote multinationals, iedereen realiseert zich dat optimale security geen 'nice to have', maar een must-have is. Met een toename in dreigingen en de steeds professionelere aanpak van cybercriminelen, staan IT-afdelingen voor een aantal grote security-uitdagingen. Eén van de belangrijkste is het verkrijgen van inzicht. Wat niet weet wat niet deert? Als u de continuïteit van uw IT-netwerk wilt waarborgen, gaat die vlieger niet op!

CONTROLE OVER SECURITYDREIGINGEN

Denkt u bij security nog vooral aan firewalls en antivirussoftware? Losse producten die in de infrastructuur worden geprikt om kwaadwillenden buiten het netwerk te houden? Vandaag de dag is dat niet meer afdoende. Security is echt een strategie en dat vereist een gelaagde aanpak: voor ieder type bedrijf. Slachtoffers van een botnet of ransomware zijn namelijk altijd willekeurig. Dit betekent dat of u nu een groot of klein bedrijf heeft u altijd een risico loopt. Een risico dat u alleen verkleint door diepgaand inzicht in het verkeer naar en binnen uw IT-netwerk te creëren. Zo voorkomt u dat kwaadwillenden zich maandenlang ongemerkt binnen uw netwerk bewegen en u continu achter de feiten aanloopt. Bovendien komt de dreiging niet altijd van buitenaf, maar ook van binnenuit. Denk aan medewerkers die per ongeluk bestanden naar verkeerde personen versturen, op links in phishingmails klikken of ontevreden medewerkers die informatie verkopen. Ook dan wilt u weten dat er iets aan de hand is.

GEEN GROTE INVESTERINGEN

Hoewel iedereen het belang van een veilig IT-netwerk inziet, worstelen veel bedrijven nog altijd met de vraag hoe zij dit aan moeten pakken. Als resources en budgetten beperkt zijn, hoe realiseer je dan toch een hoog securityniveau?

In deze whitepaper delen wij 3 tips om de onzichtbare securitydreigingen, en de impact hiervan, in uw netwerk snel zichtbaar te maken. Door inzicht te creëren vanaf de basis (DNS) voorkomt u dat u veel tijd en geld besteedt aan het blussen van brandjes. En het goede nieuws is: hier zijn geen grote investeringen vooraf voor nodig!

1. Internet Security
Breng beveiliging op DNS-niveau aan

Vandaag de dag is iedere organisatie afhankelijk van het internet. Het is dus ook niet gek dat veel van de securityproblemen via deze weg de organisatie binnenkomen. Phishingmails die worden geopend, malafide advertenties die worden aangeklikt, een fout is zo gemaakt. Om veilig gebruik te maken van het internet en niet continu bang te hoeven zijn, begint een veilig IT-netwerk dan ook bij de basis: inzicht in het internetverkeer en beveiliging van DNS.

CONTROLE OVER SECURITYDREIGINGEN

IT-afdelingen steken veel tijd en moeite in het detecteren van dreigingen als ransomware, malware en phishing en het oplossen van eventuele verstoringen of schade als gevolg hiervan. Geen gemakkelijke klus, want doordat er steeds meer locaties en devices beschermd moeten worden, ontbreekt vaak het totaalinzicht in alle internetactiviteit. Bovendien neemt de complexiteit van security-omgevingen in hoog tempo toe, doordat steeds meer producten aan de omgeving worden toegevoegd. Deze producten zijn vaak moeilijk te beheren en integratie met andere oplossingen is niet altijd mogelijk. Terwijl IT-afdelingen voor deze uitdagingen staan, neemt tegelijkertijd het aantal dreigingen via het internet toe. Om ervoor te zorgen dat u niet continu bezig bent met het blussen van brandjes, is het belangrijk om bedreigingen vanaf het begin in de kiem te smoren. Dit kan door beveiliging op het niveau van Domain Name System (DNS) te implementeren. Beveiliging op DNS-niveau fungeert als eerste verdedigingslinie voor gebruikers tegen bedreigingen op het internet.

VAN DE MALWARE GEBRUIKT DNS

Bron: Cisco

DNS ALS RISICO

Om iedere medewerker veilig gebruik te laten maken van het internet, is het belangrijk om te beginnen bij de basis. Alle internetactiviteit begint bij DNS. DNS wordt gezien als het telefoonboek van het internet. Het vertaalt namen van computers naar IP-adressen en andersom. DNS vormt voor veel organisaties echter ook een groot risico. Wist u bijvoorbeeld dat maar liefst 91 procent van de malware DNS gebruikt om 'command and control' te verkrijgen, een ongeautoriseerde gegevensoverdracht uit te voeren of om webverkeer om te leiden?

Uit het Global DNS Threat Report 2019 van IDC blijkt bovendien dat er een flinke toename is in het aantal DNS-aanvallen. In het afgelopen jaar werd maar liefst 82 procent van de onderzochte organisaties getroffen door een DNS-aanval. Als gevolg hiervan had 63 procent te maken met downtime van interne applicaties, van 45 procent werd de website gecompromitteerd en 13 procent had te maken met diefstal van informatie. Diefstal van gegevens is een van de meest serieuze risico's voor iedere onderneming en de werkelijkheid is dat DNS op allerlei onconventionele manieren misbruikt kan worden. Dat maakt het de perfecte achterdeur voor hackers die op zoek zijn naar gevoelige gegevens. Gelukkig is er een snelle manier om deze achterdeur te sluiten!

Organisaties getroffen door een DNS-aanval	**82%**
Interne downtime als gevolg van DNS-aanval	**63%**
Website gecompromitteerd	**45%**
Diefstal van informatie	**13%**

Onderzoek DNS bedreigingen onder diverse organisaties
Bron: Global DNS Threat Report 2019 van IDC

HOEVEELHEID DATA DIE WORDT VERLOREN OF GESTOLEN

6,1 MILJOEN

RECORDS PER DAG

253K

RECORDS PER UUR

4K

RECORDS PER MINUUT

70

RECORDS PER SECONDE

Bron: breachlevelindex.com - Augustus 2019

CLOUD SECURITYPLATFORM

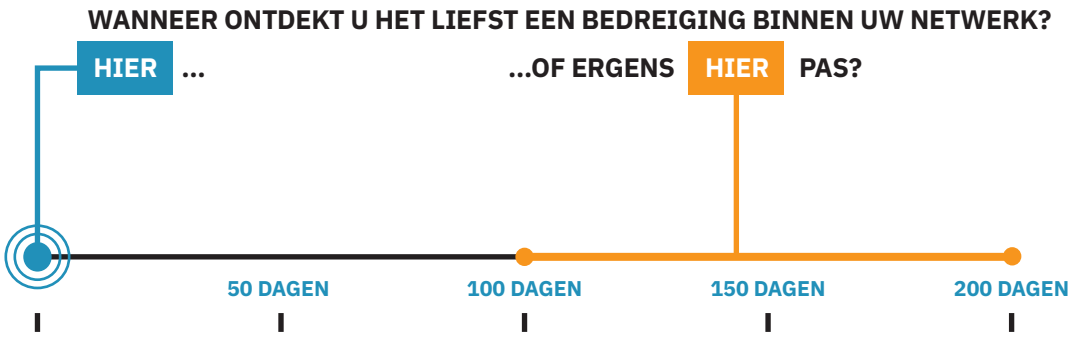
Het implementeren van beveiliging op DNS-niveau vraagt niet om een grote investering vooraf. Zo heeft Cisco bijvoorbeeld het cloud securityplatform Umbrella ontwikkeld. Deze dienst is af te nemen via een maandelijks abonnement. De wereldwijde infrastructuur van Cisco verwerkt meer dan honderd miljard internetverzoeken per dag. Door te leren van de analyses van al deze verzoeken en andere patronen in internetactiviteit, onthult Umbrella automatisch bestaande en nieuwe bedreigingen nog voordat deze schade aanrichten. Het automatisch detecteren van dreigingen biedt een belangrijk voordeel in de strijd tegen cybercrime. Het zorgt voor inzicht en helpt kwetsbaarheden in het netwerk tijdig op te lossen. Zo worden malwarebesmettingen automatisch tegengehouden en verbindingen naar command & control servers vanaf besmette computers worden gestopt. Een medewerker die op een link in een phishingmail drukt, vormt zo geen risico meer voor de organisatie.

Door beveiliging op DNS-niveau uit de cloud af te nemen, worden niet alleen werknemers op kantoor beschermd, maar ook de mobiele gebruiker die niet in het netwerk aanwezig is. Alle DNS-aanvragen worden veilig verstuurd door een beveiligde verbinding van het mobiele apparaat naar de Umbrella Cloud. De ingestelde beleidsregels en bescherming tegen malware zijn dan ook actief op het mobiele apparaat.

RAPPORTAGES VOOR INZICHT

Op het moment dat u kiest voor beveiliging op DNS-niveau kunt u niet alleen met een gerust hart gebruikmaken van het internet, maar krijgt u ook meer inzicht. Denk aan informatie over het aantal malwarebesmettingen dat is tegengehouden, welke potentieel schadelijke domeinen er zijn geblokkeerd en hoe vaak er kliks op phishing mails zijn onderschept. Belangrijke informatie die u ook helpt om het bewustzijnsniveau binnen de organisatie te verhogen.

2. Smart Networking Monitoring
Implementeer netwerkdetectie



Wist u dat organisaties gemiddeld 100 tot 200 dagen nodig hebben om een bedreiging op het netwerk te detecteren? De kans is erg groot dat u tegen die tijd geen idee meer heeft wie er op het netwerk geweest is en waar deze persoon toegang toe heeft gehad. Voor een veilig en betrouwbaar IT-netwerk is inzicht door middel van detectie dan ook onmisbaar.

"Organisaties hebben gemiddeld 100 tot 200 dagen nodig om een bedreiging te detecteren"

WIE KOMT ER DOOR DE FIREWALL?

Om kwaadwillenden buiten uw IT-netwerk te houden, is het plaatsen van een firewall niet langer afdoende. De methodes waarmee cybercriminelen zichzelf toegang verlenen tot het netwerk worden namelijk steeds geavanceerder. Dat u de voordeur op slot doet, wil dan ook niet zeggen dat er niemand meer binnen komt!

Eén van de redenen dat een firewall niet alles tegenhoudt, is dat internetverkeer steeds vaker versleuteld wordt waarbij end-to-end encryptie wordt afgedwongen. Dit is natuurlijk een hele goede manier om internetverkeer te beschermen, maar het zorgt er ook voor dat de firewall niet meer naar de inhoud van de pakketten kan kijken en cybercriminelen een opening vinden. Dit maakt een firewall niet overbodig, maar wel minder waard. Dit is dan ook de reden dat het implementeren van netwerkdetectie een onmisbare stap is in het verkrijgen van inzicht. Het is te vergelijken met een discotheek: de firewall is de toegang tot de discotheek, de detectie fungeert als uitsmijter. Wanneer u zich eenmaal binnen toch blijkt te misdragen, wordt u verwijderd door de uitsmijter.

SCHADE DOOR ONZICHTBARE DREIGINGEN

Doordat securitydreigingen ongemerkt maanden op de loer kunnen liggen in uw IT-netwerk, is de schade op het moment dat het misgaat vaak aanzienlijk. Zo blijkt bijvoorbeeld uit de Risicorapportage Cyberveiligheid Economie 2018 dat in 2016 11 procent van de Nederlandse bedrijven kosten gemaakt heeft ten gevolge van een hack. Daarnaast leverden deze hacks schade op als product- en arbeidskosten voor herstel en preventie, reputatieschade en minder gebruik van digitale diensten. Ook DDoS-aanvallen zijn kostbaar. De gemiddelde kosten per 1 minuut downtime komen neer op €20.000,-. Deze kosten lopen al snel op als u bedenkt dat de gemiddelde downtime ten gevolge van een DDoS-aanval 54 minuten is. Om schade te voorkomen en de continuïteit van uw organisatie te bewaken, is het essentieel dat dreigingen gedetecteerd worden voor het te laat is.

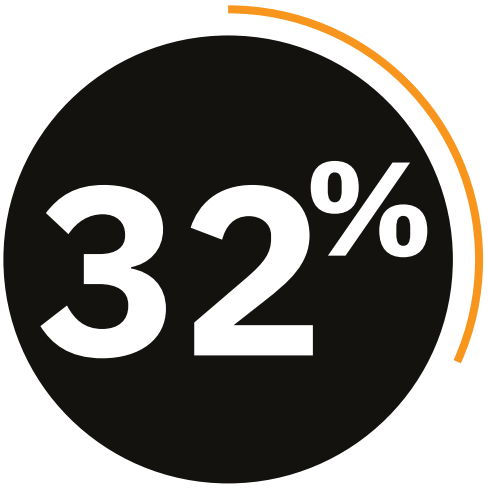
GEMIDDELDE DOWNTIME NA DDOS-AANVAL

54 MINUTEN

GEMIDDELDE KOSTEN DOWNTIME

€20.000,- PER MINUUT

Bron: Ponemon Institute's Cyber Security on the Offense: A Study of IT Security Experts



VAN DE BEDRIJVEN KENT DE OORZAAK VAN HUN DATALEK NIET

bron: Cisco, onderzoek onder 600 bedrijven

ABNORMAAL GEDRAG DETECTEREN

Het doel van netwerkdetectie is het detecteren en signaleren van abnormaal gedrag binnen het netwerk. Denk bijvoorbeeld aan een enorme toename van netwerkpakketten met vrijwel dezelfde karakteristieken. Dit kan wijzen op een DDoS-aanval. Maar ook abnormale activiteiten van gebruikers, zoals het inloggen op afwijkende tijden of binnen korte tijd vanaf verschillende locaties. Een persoon kan niet op dit moment in Amsterdam inloggen en tien minuten later in Parijs. Met Smart Network Monitoring maakt u het netwerkverkeer inzichtelijk tussen de firewalls en end-points, waardoor u meer grip krijgt op de veiligheid van uw IT-netwerk. Eén van de oplossingen om uw interne netwerkverkeer realtime te monitoren, is Flowmon. Alles wat voorbij de firewall komt wordt gedetecteerd, waardoor tijdig (geautomatiseerd) kan worden ingegrepen. Net als Cisco Umbrella is Flowmon af te nemen als een dienst, waardoor budget geen drempel meer is.

3. Overweeg security uit te besteden

De afhankelijkheid van het IT-netwerk is niet voorbehouden aan grote bedrijven. Bijna ieder bedrijf in Nederland heeft behoefte aan een netwerkomgeving die niet alleen betrouwbaar en snel is, maar bovenal ook veilig. Een flinke uitdaging in een tijd waarin technologische ontwikkelingen elkaar razendsnel opvolgen, specialisten schaars zijn en cybercrime steeds geavanceerder wordt. Om securitydreigingen snel inzichtelijk te maken én te houden, kan het uitbesteden van security uitkomst bieden. Dit verhoogt niet alleen de veiligheid, maar geeft bedrijven ook de rust om zich te focussen op de core business.

DETECTEREN, REAGEREN EN OPNIEUW

Veel organisaties hebben (onterecht) nog altijd een gevoel van veiligheid en het idee dat ze dreigingen zelf in de hand kunnen houden. Dit komt echter vooral omdat er te weinig écht naar het netwerk gekeken wordt en daardoor niemand weet wat hij mist. Ook worden signalen dat er iets mis is op het netwerk lang niet altijd herkend. Zo ontdekten wij bij een klant die dacht netwerkproblemen te hebben dat er een virus genesteld zat in de productiesystemen. Dat virus werd gebruikt in een botnet. Al langere tijd werden de productiesystemen langzamer en viel de netwerkverbinding zo nu en dan uit. Tot tenslotte alle systemen plat lagen. Met behulp van Internet Security en Smart Network Monitoring wisten wij het probleem bloot te leggen, maar veel liever bent u de problemen natuurlijk voor!

Met oplossingen als Cisco Umbrella en Flowmon maakt u snel en eenvoudig onzichtbare dreigingen zichtbaar, maar daarmee bent u er nog niet. Het veilig houden van het IT-netwerk is een continu proces en vereist een hoog kennisniveau. Het inzichtelijk maken en detecteren van de dreigingen zijn de eerste stappen, maar vervolgens moet er ook actie ondernomen worden. Wanneer dit is gebeurd, begint alles weer van voren af aan. In een tijd waarin securityspecialisten schaars zijn en bovendien niet iedere organisatie over de middelen beschikt om specialisten in dienst te nemen, is het daarom raadzaam om het uitbesteden van security te overwegen. Zo hoeft u zelf niet te investeren in kennis en tooling en weet u zeker dat er altijd iemand is die exact weet wat er op het netwerk gebeurt.

VAN INZICHT NAAR STUREN: ÉÉN TOTAALAANPAK

Vandaag de dag vereist security een gelaagde en geïntegreerde aanpak. Het is cruciaal om te zorgen voor inzicht: van het internetverkeer tot aan de gebruiker. Maak het onzichtbare zichtbaar. Zorg dat u weet wat er op uw netwerk gebeurt door beveiliging op DNS-niveau aan te brengen en netwerkdetectie te implementeren. Wilt u zeker weten dat de veiligheid van uw netwerk ook in de toekomst gewaarborgd blijft? Overweeg dan om uw security uit te besteden.

AAZOO MAAKT HET ONZICHTBARE ZICHTBAAR

Wij zijn aaZoo Network Solutions uit Emmeloord. Wij geloven in de kracht van kennis. Kennis die ervoor zorgt dat uw netwerk perfect is én direct bijdraagt aan het verbeteren van uw business en uw concurrentiepositie. Als netwerkspecialisten zijn wij altijd bezig met het bepalen, beschermen en bewaken van de perfecte netwerken voor organisaties. Wij realiseren de vooruitstrevendste netwerken en werken met de meest geavanceerde securityoplossingen en geselecteerde datacenters. Zo weet u zeker dat u de beste oplossing heeft voor uw organisatie: veilig, snel, flexibel, schaalbaar en van de hoogste kwaliteit.

www.aazoo.nl | info@aazoo.nl | 088 12 62 400