AAZOO

AAZOO MAAKT HET ONZICHTBARE ZICHTBAAR

WHITEPAPER

3 tips

om securitydreigingen in uw netwerk snel inzichtelijk te maken

cisco SECURE Partner

INHOUD

MAAK HET ONZICHTBARE ZICHTBAAR 3

1. INTERNET SECURITY: BRENG EEN SCHILD AAN RONDOM UW ORGANISATIE 4

2. AAZOO SECURE OPERATIONS – BEVEILIGING EN CONTROLE OVER NETWERK EN END-POINTS 7

3. OVERWEEG SECURITY UIT TE BESTEDEN 10

AAZOO MAAKT HET ONZICHTBARE ZICHTBAAR

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 en controle tot en met de end-points. Wat niet weet wat niet deert? Als u de continuïteit van uw IT-netwerk en organisatie wilt waarborgen, gaat die vlieger niet op!

IEDER BEDRIJF LOOPT EEN RISICO: EXTERN EN INTERN

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 een schild aan rondom uw organisatie

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.

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

VAN DE MALWARE GEBRUIKT DNS

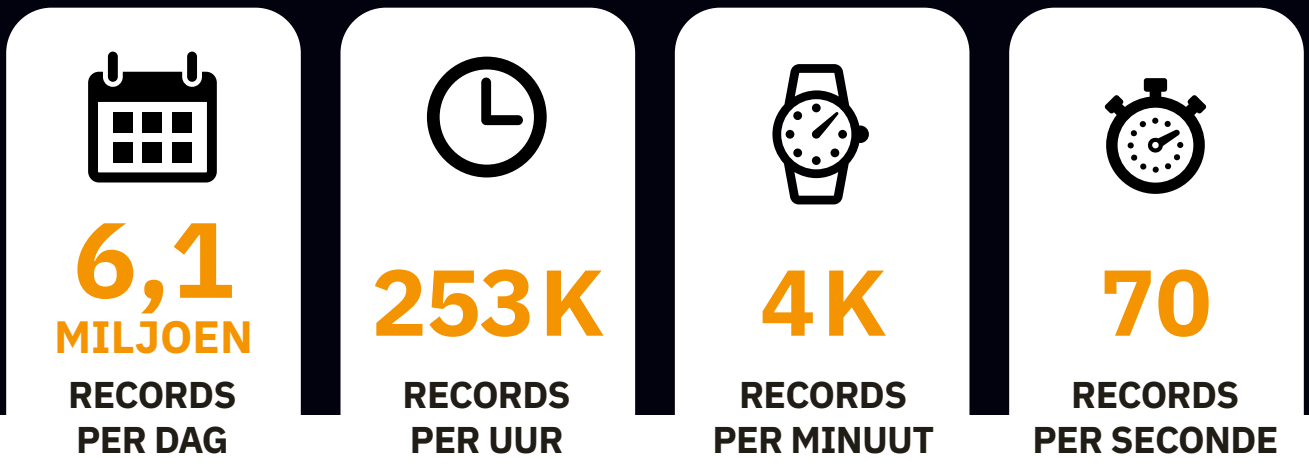
Onderzoek DNS bedreigingen onder diverse organisaties
Bron: Global DNS Threat Report 2019 van IDC

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. DNS is namelijk een belangrijk doelwit voor kwaadwillende hackers die het systeem willen misbruiken voor verschillende soorten aanvallen, zoals DNS spoofing, cache poisoning en DDoS-aanvallen. 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!

CLOUD BEVEILIGINGSPLATFORM

Het implementeren van beveiliging op DNS-niveau vraagt niet om een grote investering vooraf. Zo heeft Cisco bijvoorbeeld het cloud beveiligingsplatform Umbrella Secure Internet Gateway 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 Secure Internet Gateway automatisch bestaande en nieuwe bedreigingen nog voordat deze schade aanrichten. Het automatisch

HOEVEELHEID DATA DIE WORDT VERLOREN OF GESTOLEN



Statistieken verlies of diefstal van data - Augustus 2019
Bron: breachlevelindex.com

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 potentiële 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.

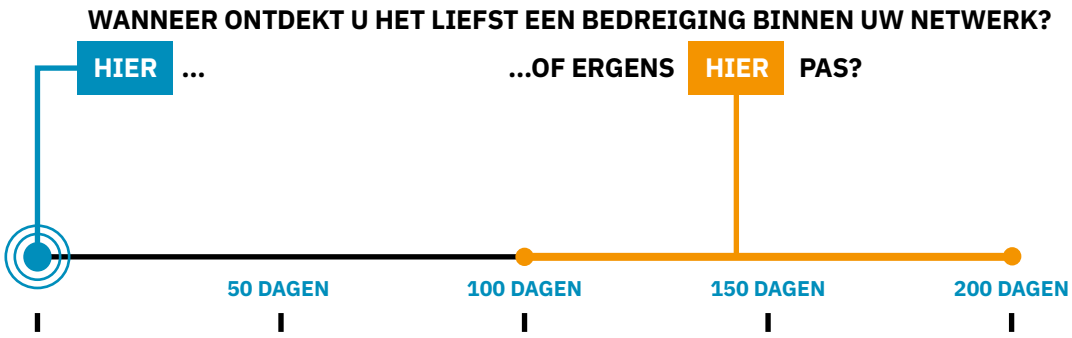
FIREWALL IN DE CLOUD

Daarnaast biedt Cisco Umbrella een vanuit de cloud geleverde firewall die organisaties kunnen gebruiken om gecentraliseerde internettoegang te omarmen. Dit cloud-native alternatief kan eenvoudig worden beheerd en geschaald zonder de dure refresh-cycli en onderhoudsproblemen van traditionele beveiligingsservices. Umbrella's cloud-geleverde firewall is essentieel om de beveiligingseffectiviteit te verbeteren en consistentie te handhaven. Het biedt zichtbaarheid en controle over internetverkeer en beschermt tegen malware, phishing en ongepast gebruik. Umbrella stuurt verschillende verkeerstypen intelligent door naar de juiste functie om een ideale balans te bereiken tussen beveiligingseffectiviteit, gebruikersprestaties en beheersgemak.

RAPPORTAGES VOOR INZICHT

Op het moment dat u kiest voor beveiliging op cloud-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 phishingmails zijn onderschept. Belangrijke informatie die u ook helpt om het bewustzijnsniveau binnen de organisatie te verhogen.

2. aaZoo Secure Operations beveiliging en controle over netwerk en endpoints



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.

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 2020-2021 dat in 2020 39 procent van de Nederlandse bedrijven te maken heeft gehad met cyberincidenten. Daarnaast leverden deze hacks schade op als product- en arbeidskosten voor herstel en preventie, reputatieschade en minder gebruik van digitale diensten. Om schade te voorkomen en de continuïteit van uw organisatie te bewaken, is het essentieel dat dreigingen gedetecteerd worden voor het te laat is.

Endpoint Detection and Response (EDR) is een belangrijk onderdeel van detectie. EDR stelt organisaties in staat om de end-points van hun netwerk te monitoren op verdachte activiteit. Door end-point monitoring kunnen organisaties sneller potentiële bedreigingen detecteren en voorkomen dat deze zich verspreiden naar andere delen van het netwerk.

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.

ABNORMAAL GEDRAG DETECTEREN

Het detecteren van abnormaal gedrag binnen het netwerk is essentieel om veiligheidsdreigingen te voorkomen. Endpoint Detection and Response (EDR), zoals Cisco Secure Endpoint, biedt realtime monitoring van end-point activiteiten, waardoor bedrijven kunnen reageren op incidenten voordat deze schade veroorzaken.

GEMIDDELDE DOWNTIME NA DDOS-AANVAL

54 MINUTEN

GEMIDDELDE KOSTEN DOWNTIME

€20.000,- PER MINUUT

VAN DE BEDRIJVEN KENT DE OORZAAK VAN HUN DATA-LEK NIET

bron: Cisco, onderzoek onder 600 bedrijven

Cisco Secure Network Analytics is een oplossing voor interne netwerkverkeer monitoring die bedrijven in staat stelt om alles wat voorbij de firewall komt te detecteren en hierop geautomatiseerd in te grijpen. Het biedt diepgaande inzichten in netwerkactiviteiten en helpt u ook te reageren op incidenten voordat deze schade veroorzaken. Cisco Secure Network Analytics is beschikbaar als een dienst, waardoor budget geen drempel meer is voor bedrijven om deze essentiële beveiligingsoplossing te implementeren.

EXTENDED DETECTION AND RESPONSE (XDR)

eXtended Detection and Response (XDR) is een aanpak die endpoint, netwerk en cloud events combineert en analyseert. XDR biedt organisaties een uitgebreider overzicht van hun netwerkactiviteiten en stelt hen in staat om bedreigingen te detecteren die anders misschien over het hoofd gezien zouden worden. XDR is vooral handig voor organisaties die meerdere end-points hebben en verschillende incidentbronnen moeten beheren, zoals endpoints, cloud, e-mails, netwerkdetectie en firewall logbestanden. Door deze gegevensbronnen te combineren met bedreigingsinformatie en geautomatiseerde reactie, wordt een uitgebreide detectie en respons (XDR) benadering geboden. Deze aanpak stelt beveiligingsteams in staat om snel bedreigingen te detecteren en te reageren, ongeacht waar ze zich bevinden in het netwerk en het endpoint. Dit kan resulteren in snellere reactietijden en minder schade voor uw organisatie.

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 de Cisco Security Cloud, bestaande uit geavanceerde oplossingen voor security operations centers die de XDR-principes volgen en geautomatiseerde remediation op basis van machine learning bieden, wisten wij het probleem bloot te leggen. Maar veel liever bent u de problemen natuurlijk voor! 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.

THREAT HUNTING & INCIDENT RESPONSE

Met de geavanceerde oplossingen die we gebruiken in ons Secure Operations Center (SOC) volgen we de XDR-principes en passen we geautomatiseerde remediation toe. Op basis van machine learning en het bijsturen door onze experts kan het aantal false-positives en false-negatives worden verminderd. Automatisering vermindert de menselijke fouten en verhoogt de kwaliteit van SOC-analisten door hen te bevrijden van tijdrovende taken. Geautomatiseerde incidentrespons is een andere belangrijke factor die de efficiëntie van een SOC verbetert. Het vermogen om snel en geautomatiseerd te reageren op een incident zorgt ervoor dat er geen kostbare tijd verloren gaat in het geval van een bedreiging.

Het is belangrijk om onderscheid te maken tussen bedreigingsjacht (threat hunting) en incident response. Threat hunting is een proactieve activiteit om bedreigingen te ontdekken die bestaande beveiligingsoplossingen kunnen omzeilen. Incident response daarentegen, richt zich op het reageren op een al gedetecteerd incident om schade te minimaliseren en het herstel te versnellen. Bij ons Managed SOC maken we gebruik van beide methoden op een geautomatiseerde manier om ervoor te zorgen dat onze klanten optimaal beveiligd zijn tegen dreigingen vaak nog voordat ze van impact zijn op de organisatie.

VAN INZICHT NAAR STUREN: ÉÉN TOTAALAANPAK

Tegenwoordig vereist beveiliging een gelaagde en geïntegreerde aanpak. XDR (Extended Detection and Response) biedt een totaaloplossing doordat het informatie van verschillende beveiligingsoplossingen zoals firewalls, e-mailbeveiliging en endpoint detection and response combineert. Ook maakt XDR gebruik van de intelligentie die wordt verzameld uit onze eigen onderzoeken, bedreigingsinformatie van het NCSC en openbaar beschikbare informatie van bedreigingsonderzoekers. Het is van cruciaal belang om inzicht te hebben, van internetverkeer tot aan de gebruiker. Maak het onzichtbare zichtbaar. Zorg dat u weet wat er op uw netwerk gebeurt door beveiliging op cloud-niveau aan te brengen en detectie van afwijkend gedrag te implementeren. Overweeg het uitbesteden van uw beveiliging om er zeker van te zijn dat de veiligheid van uw netwerk ook in de toekomst gewaarborgd blijft.

Wij zijn aaZoo Network & Security 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.

DE KRACHT VAN KENNIS

cisco SECURE Partner

Wij zijn aaZoo. Wij passen onze enterprisekennis en -ervaring zorgvuldig toe op diverse vraagstukken. Het resultaat? Perfecte en constante netwerkomgevingen, ingericht en onderhouden door gedreven vakmensen. Dat noemen wij de kracht van kennis.

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