INFO SECURITY MAGAZINE
JAARGANG 18 - JULI 2021 - WWW.INFOSECURITYMAGAZINE.NL

ONDERZOEK FORTINET: OT BEDRIJVEN EN SECURITY INCIDENTEN

MARTIJN HAKSTEGE TESORION SECURITY IS STRAKS EEN DIENST

ANDREW ROSE ERVARINGEN VAN DE DARK SIDE

FRED STREEFLAND CYBERSECURITY INDUSTRIE IS ZIEK

Zolang klassikaal trainen nog niet mogelijk is,
worden alle trainingen Live Online gegeven.

TECHNICAL SECURITY TRAININGEN

CEH	-	CERTIFIED ETHICAL HACKER
CHFI	-	COMPUTER HACKING FORENSIC INVESTIGATOR
ECSA/LPT	-	CERTIFIED SECURITY ANALYST / LICENSED PENETRATION TESTER
SSCP	-	SYSTEMS SECURITY CERTIFIED PROFESSIONAL
OSCP	-	OFFENSIVE SECURITY CERTIFIED PROFESSIONAL

SECURITY MANAGEMENT TRAININGEN

CISSP	-	CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISM	-	CERTIFIED INFORMATION SECURITY MANAGER
CISA	-	CERTIFIED INFORMATION SYSTEMS AUDITOR
CRISC	-	CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL
C|CISO	-	CERTIFIED CHIEF INFORMATION SECURITY OFFICER

PRIVACY TRAININGEN

CIPP/E	-	CERTIFIED INFORMATION PRIVACY PROFESSIONAL / EUROPE
CIPM	-	CERTIFIED INFORMATION PRIVACY MANAGER
CIPT	-	CERTIFIED INFORMATION PRIVACY TECHNOLOGIST
CDPO	-	CERTIFIED DATA PROTECTION OFFICER
CORE	-	PRIVACY CORE AWARENESS ELEARNING

CLOUD SECURITY TRAININGEN

CCSP	-	CERTIFIED CLOUD SECURITY PROFESSIONAL

ISO TRAININGEN

ISO 27001	-	FOUNDATION
ISO 27001	-	LEAD IMPLEMENTER
ISO 27001	-	LEAD AUDITOR
ISO 27005	-	RISK MANAGER

NIEUW CSA CERTIFIED SOC Analyst

www.tstc.nl

COLOFON

Infosecurity Magazine is het enige onafhankelijke vakblad in de Benelux dat zich expliciet bezighoudt met informatie-beveiliging. Het blad beweegt zich op het snijvlak van technologie en beleid. Vanaf het hekwerk tot in de boardroom. Toezending van Infosecurity Magazine vindt plaats op basis van abonnementen en controlled circulation. Abonnementen kunnen iedere maand ingaan en worden jaarlijks automatisch verlengd. Opzeggingen, uitsluitend schriftelijk, dienen uiterlijk twee maanden voor het einde van de abonnementsperiode in ons bezit te zijn.

Uitgever
Eric Luteijn
+31 (0)653 510 690
eric@luteijnmedia.nl

Associate Editor
Edwin Feldmann
+ 31 (0)6 45 93 10 06
redactie@infosecuritymagazine.nl

Communicatie en Marketing
Jos Raaphorst
+31 (0)6 - 34 73 54 24
jos@infosecuritymagazine.nl

Abonnementen
luteijn@mijntijdschrift.nl
+31 (0)88 -22 666 80

Vormgeving
Content Innovators, Den Haag

Druk
Veldhuis Media B.V., Raalte

Een uitgave van:
LuteijnMedia BV
Varenmeent 5
1218 AN Hilversum
www.infosecuritymagazine.nl

LuteijnMedia

Infosecurity Magazine is vernieuwd!

Cyberincidenten zijn aan de orde van de dag. En de impact op de samenleving kan groot zijn, concludeerde van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in juni in het jaarlijkse Cybersecuritybeeld Nederland. Schrokken we echt van dit rapport? Ik denk het niet. Het onderstreept wel opnieuw het belang van goede beveiliging van informatie en systemen. Vooral voor kritieke systemen die bijvoorbeeld de kwaliteit van het drinkwater regelen, de sluisdeuren van een waterkering of een andere belangrijke voorziening.

Hoe belangrijk cybersecurity is, welke ontwikkelingen zich afspelen in die markt en welke spelers daarbij belangrijk zijn, dat zijn onderwerpen die we in het vernieuwde Infosecurity magazine aan bod laten komen. Want Infosecurity magazine is in een nieuw jasje gestoken. Een nieuw gedreven team staat klaar om vanaf nu met regelmaat een nieuw magazine te maken vol met nieuws en de belangrijkste ontwikkelingen op het gebied van data, IT-security en privacy.

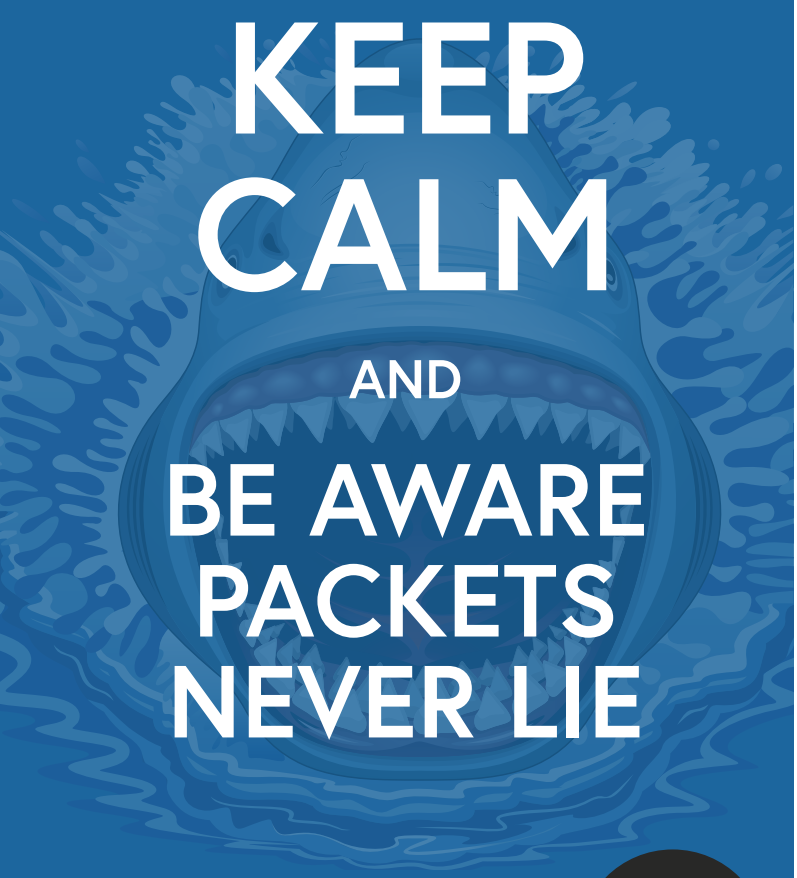
Zo lees je in deze editie onder meer over het belang van koude opslag en dat het niets te maken heeft met de temperatuur. Verder een artikel over cyberaanvallen op industriële IT-systemen en hoe je besmetting met ransomware kunt voorkomen. Kortom een positief magazine over de duistere kanten van het internet.

EDWIN FELDMANN

SCOS TRAINING

WIRESHARK UNIVERSITY
Certified Training Partner

Wireshark Tools and Training



NEW

Wireshark Certification

This certification training is designed for network, government and security personnel to obtain the **Wireshark WCNA certification** for their professional development using Wireshark.

Wireshark University Certified Training Partner

SCOS Software Amsterdam/Hoofddorp offers these official Wireshark University courses as the European Wireshark University Certified Training Partner of Gerald Combs, the creator of Wireshark. With more than 1 million downloads of Wireshark per month from Wireshark.org it has become the de facto open source analysis tool.

TCP/IP Analysis and Trouble-shooting with Wireshark

This course is designed for Networking, Government and Security personnel that need to develop a set of packet investigation and network optimization techniques through study of the Networking Protocols using Wireshark and other Open-Source Analysis tools.

Masterclass Network/Security

Advanced Network/Security Analysis with Open Source Tools. This course is designed for Networking, and Security Engineers that need to further enhance their Network Analysis skills through study of Advanced Network Analysis using Wireshark and other Open-Source Network / Security Analysis tools.

VIRTUAL CLASSROOM OR AMSTERDAM/HOOFDDORP

MORE INFO: WWW.SCOS.TRAINING

Inhoud

INFOSECURITY MAGAZINE - JULI 2021 - JAARGANG 19


Martijn Hakstege


Andrew Rose


Jeroen Remie

CEO Martijn Hakstege van security dienstverlener Tesorion:

Martijn Hakstege, CEO van Tesorion

‘Security is straks een dienst’

Martijn Hakstege is sinds deze zomer de nieuwe CEO van Tesorion. Hij vertelt waar de grootste zelfstandige Nederlandse cybersecurity dienstverlener voor staat en waarom hij zoveel aandacht heeft voor zijn personeel.

Tesorion is ontstaan door het samenvoegen van drie losse bedrijven. Quarantainenet uit Enschede, Nováccent uit Leusden en I-to-I uit Driebergen. “In plaats van een grote bestaande speler over te nemen, is er gekozen voor het bundelen van deze drie spelers,” zegt Martijn. “Er is samenhang tussen het trio specialisten. De eerste partij is goed in bouwen, de tweede bedient de machine en de derde groep consultants vult de machine.”

Focus mid market

Met deze combinatie van kennis en diensten richt Tesorion zich op de mid market. “Onze diensten sluiten goed aan op de wensen van bedrijven tussen de 100 en 5.000 medewerkers”, legt Martijn uit. “We helpen ook kleinere klanten als ze bijvoorbeeld vertrouwelijke data verwerken. Dat is een uitstekende match. Omvang en omzet zijn dus niet doorslaggevend, wij kijken naar het risicoprofiel.”

De markt van Tesorion is breed en groot. Als nieuwkomer mist het bedrijf nog wat naamsbekendheid. “Daar staat tegenover dat de markt behoorlijk in beweging is. Door consolidaties verdwijnen aanbieders of ze richten zich op segmenten in de bovenkant van de markt. Daarnaast vraagt de markt steeds meer om one-stop-shop cybersecurity. Daar profiteren we van”, geeft Martijn aan.

Met de overname van Compumatica heeft Tesorion nu ook klanten in de publieke sector. “Je kunt organisch groeien of je kunt overnemen. Wij hebben voor het laatste gekozen. We hebben nu deskundige collega’s en klanten in een segment waar we ondervertegenwoordigd waren.”

Aandacht voor personeel

Tijdens het interview komt regelmatig het personeel ter sprake. Ze zijn een belangrijk aandachtspunt voor Martijn. “Toen ik hier middenin de lockdown startte, werkte bijna iedereen vanuit huis. Dat was niet ideaal. Ook omdat we de koers moesten aanpassen zodat we sneller en beter konden inspelen op de marktbehoeften. Deze koerswijziging was voor een aantal collega’s vervelend. Maar we varen wel een nieuwe koers.”

Ook de overnames hebben een link met de aandacht voor het personeel. “We hebben een uitstekend CERT-team en SOC. Nu we groter worden, komen er meer interessante klanten en cases bij. Daarvoor ontwikkelen we ook nieuwe diensten. Zo wordt het steeds interessanter om bij ons te blijven werken”, zegt Martijn. “Medewerkers inspireren en vasthouden is belangrijk, want iedereen zit te springen om goed personeel. Nu we 180 personen aan boord hebben, is er ook ruimte voor doorstroming. Zo zijn we een aantrekkelijke werkgever.”

Op de vraag of er een doel is voor de personeelsomvang antwoordt Martijn dat het niet realistisch is om uit te gaan van sterke organische groei. “Ik sluit overigens niet uit dat er nog acquisities volgen, maar we moeten oog houden voor de cultuur en de ingrijpende veranderingen door corona. We hebben recent Kahuna overgenomen en dat proces moeten we in goede banen leiden.”

Beter dan de planning

Het eerste half jaar van 2021 verloopt voor Tesorion zeer positief. Martijn: “We lopen een half jaar voor op de planning van september 2020. Dat komt deels door onze consultants. Ondanks corona kunnen zij extern worden ingehuurd.”

Een andere reden is dat het CERT-team erg goed loopt. “Het is een dienst die je niet nodig wil hebben. Die rukken uit als het ergens fout is gegaan. Ze helpen klanten op een veilige en verantwoorde manier back-on-track. Het team werkt goed samen met een andere tak van Tesorion dat onderzoek doet en bijvoorbeeld decryptors maakt. Deze zijn beschikbaar via het platform NoMoreRansom. Zo helpen wij klanten die zijn getroffen door ransomware de data terug te krijgen zonder losgeld te betalen.”

Toekomst

Het is voor Martijn een uitgemaakte zaak dat beveiliging niet meer wordt gezien als hard- en software. “Security is straks een dienst en daar zijn we bij Tesorion op voorbereid”, voorspelt hij zonder concreet op ontwikkelingen vooruit te lopen. Wel wil hij met ITchannelPRO delen dat OT-security een zwaar onderbelicht terrein is. “Daar moeten organisaties meer aandacht aan besteden en dat zullen we de komende tijd zeker faciliteren.”

RASHID NIAMAT

Meer weten over Tesorion
Meer weten over Tesorion? Neem direct contact op met Martijn Hakstege via 06-21 535 622 of stuur een mail naar martijn.hakstege@tesorion.nl

‘Markt vraagt naar one-stop-shop cybersecurity’

EAGLE EYE NETWORKS

CYBERSECURE BY DESIGN

Een Modern Cybersecure Cloud Camera

Gebouwd door experts in Cybersecurity
met Analytics en AI die uw business
verder brengen en veiliger maken

#1 IN CLOUD VIDEOBEWAKING WERELDWIJD

LEES MEER OP
een.com

CONTACT US
+31 20 26 10 460

Wanneer spreken we van cold storage en waarom is dat belangrijk?

De afgelopen week is er weer een hoop geschreven over de voordelen van cold storage. Dat zou kunnen helpen de impact van ransomware besmettingen te verkleinen. De link die zo is gelegd klinkt logisch, maar is onjuist.

Andere datasets

Als het gaat om ransomware is het duidelijk dat als ergens actuele datasets liggen die niet besmet zijn het makkelijker is de boel weer onder controle te krijgen. Voor het gemak wordt er dan van uitgegaan dat die dataset complete images zijn en de servers en computers verder niet zijn besmet. Dat laatste zou namelijk elke herstelpoging om zeep helpen. Die datasets moeten dus vrij van fouten en besmettingen zijn. Er is voldoende software beschikbaar om het proces van aanmaken en controleren geautomatiseerd door te voeren. Waar die data wordt opgeslagen zal verschillen. In de regel wordt er weinig gesproken over warme, lauwe of koude opslag. Men heeft het, begrijpelijk, vooral over veilige opslag.

Cold storage biedt voordeel

Daarom valt het direct op als er in de marge van al het slechte nieuws over tsunami's van ransomware opeens weer de term cold storage (koude opslag) opduikt. De verwarring die daardoor kan ontstaan is dat een gebruiker er van uitgaat dat het "koud opslaan" een serieus voordeel biedt.

Koud of veilig

Koud is echter in principe niet te linken aan "veilig". Wie op zoek gaat naar de definities van cold storage ziet namelijk dat dit echt alleen maar betrekking heeft op het aantal keren dat deze data geraadpleegd wordt. Helaas zijn hyperscalers en andere vendoren van storage op dit punt heel actief met het gebruiken van eigen jargon. Er is dus geen eenduidige definitie van cold storage die iedere fabrikant en vendor gebruikt. Backblaze spreekt over cold storage als het gaat om dat die "seldom or never" wordt geraadpleegd. Die data staat daarom ook op HDD's en tape. Er zijn ook blogs en analisten die cold data omschrijven als data "already a closure and archived".

Harde criteria

Het mag duidelijk zijn dat dit ten eerste geen enkele link heeft met ransomware afweer of preventie. Daarnaast is het bijzonder vaag. Binnen SNIA en LTO zijn er ook andere omschrijvingen van data. Eigenlijk zijn die veel beter, omdat het om harde criteria gaat die voor iedereen begrijpelijk is. Warme data heet te zijn data die minder dan 10 dagen terug nog is geraadpleegd (lezen of schrijven), lauwe data is tot 30 dagen terug nog geraadpleegd. Cold storage is alles dat minimaal 30 dagen lang niet is aangeraakt.

Wie deze indeling aanhoudt snapt ook direct waarom het geen zin heeft de oplossing van ransomware te linken aan cold storage. In de regel is een dataset van meer dan een maand oud niet echt praktisch. Het is beter dan niets, maar daar houdt het dan ook mee op. Voor wie ransomware echt wil pareren is het belangrijk te weten dat de oplossing iets anders moet zijn dan vertrouwen op cold storage.

DOOR RASHID NIAMAT

Onderzoek Fortinet: **90% van de OT-bedrijven hebben**

Beveiligingsleverancier Fortinet heeft een onderzoek gedaan naar cyberbedreigingen en operationele technologie (OT), om inzicht te krijgen in hoe OT-team omgaan met beveiligingsrisico's. Fortinet ondervroeg managers van faciliteiten en fabrieken met meer dan 2.500 werknemers, die actief zijn in de sectoren industriële productie, energie en nutsvoorzieningen, gezondheidszorg en transport. Het rapport Fortinet 2021 State of Operational Technology and Cybersecurity Report beschrijft de punten waarop OT het kwetsbaarst is, de typen cyberaanvallen waarmee organisaties geconfronteerd worden, nieuwe beveiligingstechnieken en verbetergebieden voor beveiligingsprocessen.

Operationele technologie (OT) vormt de functionele basis van fabrieken, energiecentrales, transportnetwerken en nutsvoorzieningen. Veel organisaties hebben hun OT-infrastructuur met hun IT-omgeving geïntegreerd om toegang te krijgen praktisch inzetbare data in een omgeving die altijd hermetisch van de rest van het netwerk was afgesloten. Deze convergentie van OT- en IT-omgevingen vergroot de flexibiliteit en efficiëntie, maar brengt helaas ook nieuwe beveiligingsrisico's met zich mee.
Het onderzoeksrapport van Fortinet bevat vier belangrijke inzichten over de huidige staat van OT-beveiliging binnen organisaties:

1. Indringers blijven een probleem voor organisaties

De OT-managers die aan het onderzoek deelnamen hadden er moeite mee om te voorkomen dat cybercriminelen toegang kregen tot systemen en bedrijfsprocessen verstoorden. Negen van de tien organisaties kreeg het afgelopen jaar te maken met minimaal één succesvolle indringingspoging. Dit aantal is vrijwel identiek aan de resultaten van de enquête van 2020. Het is waar dat de coronacrisis onverwachte problemen met zich meebracht, maar een indringingspercentage van 90% is een significant probleem dat OT-managers meer zorgen zou moeten baren.

2. OT-managers waren niet voorbereid op de veranderingen die de pandemie met zich meebracht

OT-besluitvormers moesten hun investeringen snel opvoeren om grip te krijgen op de processen rond de connectiviteit van IT- en OT-systemen. Dit was van cruciaal belang om thuiswerkers van ondersteuning te voorzien. Security operation centers (SOC's) en network operations centers (NOC's) hadden meer personeel en apparatuur nodig doordat de coronacrisis de digitale transformatie in een stroomversnelling bracht. Technische medewerkers, OEM's en systeemintegrators zagen zich daarnaast gehinderd in hun vermogen om te reizen. Ze konden niet fysiek ter plekke komen om werkzaamheden uit te voeren. Dit resulteerde in een prangende behoefte aan oplossingen voor veilige toegang op afstand.

3. Organisaties kregen te maken met een groeiend aantal bedreigingen door insiders en phishing-aanvallen

De onderzoeksresultaten wezen op een forse toename van het aantal phishing-aanvallen. 58% van de respondenten maakte melding van een dergelijk incident. Vorig jaar lag dit percentage nog op 43%. Deze toename is te wijten aan het feit dat cybercriminelen misbruik maakten van de kwetsbaarheden die ontstonden toen organisaties snel veranderingen moesten doorvoeren om ondersteuning te bieden voor thuiswerkers. En nu werknemers vanuit huis blijven werken wordt duidelijk dat organisaties hun zero trust-strategie moeten uitbreiden naar alle endpoints om bescherming te bieden voor het groeiende aanvalsoppervlak.

4. OT-managers blijven worstelen met het meetbaar maken van de beveiliging

OT-managers die de beveiligingsprestaties meten en daarover rapporteren kennen het aspect "kosten" steevast een lagere prioriteit toe dan "risicobeoordeling" en "gevolgen voor de business". Kwetsbaarheden (70%) en indringers (62%) blijven

last van beveiligingsincidenten

de belangrijkste maatstaven die worden bijgehouden en waarover wordt gerapporteerd. Tastbare resultaten op het gebied van risicobeheer hebben het afgelopen jaar echter een prominentere rol gekregen (57%).

Samengevat: het afgelopen jaar is er duidelijk sprake geweest van een sterkere behoefte aan de veerkrachtige bescherming die mogelijk wordt gemaakt door best practices voor cybersecurity. Desondanks blijkt uit het rapport dat OT-managers met problemen blijven kampen. Slechts 7% van alle organisaties die aan het onderzoek deelnamen werd het afgelopen jaar niet door een beveiligingsincident getroffen. En ondertussen neemt de digitale verbondenheid van OT- en IT-netwerken alleen maar toe. Het is duidelijk dat veel organisaties moeite hebben met het toepassen van best practices voor cybersecurity en uiteindelijk ook het beschermen van hun infrastructuur tegen de steeds geavanceerdere cyberbedreigingen.

Ervaringen van de dark side - hoe je ransomware-aanvallen kunt voorkomen

In elk gesprek dat ik met CISO's heb over hun zorgen en prioriteiten komt gegarandeerd één ding naar boven: ransomware. Het is de nachtmerrie van de CISO. Een zeer openbaar beveiligingsincident dat de operationele capaciteit schaadt en ook nog eens gegevens laat verdwijnen, en dat alles met een fors kostenplaatje.

Uit recent onderzoek van Proofpoint is gebleken dat 44% van de bedrijven in 2020 werd getroffen door ransomware. Gezien de potentiële omvang van de impact is dat een angstaanjagend hoog cijfer. Van die organisaties besloot 34% het losgeld te betalen om hun positie te herstellen.

Interessant is dat 98% van de bedrijven die betaalden, hun gegevens konden terughalen. In het verleden was dit slechts 78%. Dit wijst op een professionalisering van de aanvaller. Die ziet in dat vertrouwen dat de betaling daadwerkelijk resulteert in gegevensherstel een manier is om het betalingspercentage op te drijven.
Een voorbeeld van dit toegenomen professionalisme was een recente aanval op een modemerk. In dit specifieke geval bestudeerde de aanvaller de gestolen gegevens om details te vinden over de cyberaansprakelijkheidsverzekering van de organisatie. Vervolgens stelde hij het losgeld vast op exact dat bedrag. De aanvaller onderhandelde met het slachtoffer over dit bedrag, op basis van zijn evaluatie van de financiële gezondheid van de organisatie. En uiteindelijk ontvang hij de overeengekomen betaling.
Dit soort professionalisme kun je zelfs als 'klantenbinding' zien. We zien vaak een niveau van technische ondersteuning, verleend via anonieme instant messaging platforms. De hacker helpt zijn slachtoffers bij de herstelwerkzaamheden zodra ze betaald hebben. Wat deze specifieke aanval interessant maakte, is dat de aanvaller de organisatie na de onderhandeling gedegen advies gaf over het voorkomen van nieuwe ransomware-aanvallen. Deze adviespunten geven ons een goed inzicht in wat we kunnen doen om onze organisatie beter te beschermen tegen het aangaan van deze pijnlijke, en kostbare, dans met de criminelen. Het advies omvatte onder meer het volgende:

• E-mailfiltering implementeren

Het belangrijkste advies was om e-mailfiltering in te voeren. Statistieken tonen aan dat ongeveer 94% van de cyberaanvallen beginnen via e-mail. Het is dus een echte 'brandslang' van risico's rechtstreeks uw organisatie in. In het begin maakten ransomware-aanvallen gebruik van poorten van het Remote Desktop Protocol (RDP) enzovoort. Nu blijkt uit onderzoek van Proofpoint echter dat het aantal ransomware-aanvallen via e-mail-gebaseerde phishing-campagnes toeneemt. Dit staat in schril contrast met voorgaande jaren, toen hackers voornamelijk gebruikmaakten van downloaders als initiële payload.

• Voer phishing-tests en penetratietests uit op werknemers

Meer dan 99% van de aanvallen die via e-mail binnenkomen, vereist dat de gebruiker een bepaalde actie onderneemt om een succesvolle inbreuk mogelijk te maken. Dat kan bijvoorbeeld het uitvoeren van een macro zijn, het delen van inloggegevens of het betalen van een valse factuur. Werknemers vormen het belangrijkste aanvalsoppervlak van een onderneming. Het is daarom van essentieel belang dat zij worden voorgelicht en getraind in het herkennen en aanpakken van bedreigingen. Dit moet ook worden ondersteund met regelmatige penetratietests. Die zorgen ervoor dat eventuele perimetermisconfiguraties of ongepatchte randapparatuur worden gedetecteerd en aangepakt voordat er misbruik van gemaakt wordt.

• Herzie het wachtwoordbeleid van Active Directory

Het derde advies van de cybercrimineel was om ervoor te zorgen dat het wachtwoordbeleid voldoende robuust was. Dit begint met Multi-Factor Authentication (MFA) voor externe toegang, die ook wordt uitgebreid naar het interne wachtwoordbeleid. Een onderdeel van de ransomware kill-chain is het uitbreiden van privileges. Dit stelt aanvallers in staat om toegang te krijgen tot grote hoeveelheden kritieke gegevens en deze te verwijderen voordat de encryptie wordt afgedwongen. Er wordt gebruikgemaakt van zwakke interne wachtwoorden, of een XLS-bestand van de databasebeheerders met alle belangrijke wachtwoorden binnen hun domein.

• Investeer in betere endpoint detectie en respons (EDR)-technologie

Het komt steeds vaker voor dat cybercriminelen creatief zijn in hun aanvallen. Een recente trend is dat actoren legitiem geïnstalleerde tools zoals PowerShell gebruiken om hun doelen te bereiken. Bij één ransomware-aanval gebruikten de aanvallers BitLocker om de apparaten te versleutelen. De les die we hieruit kunnen trekken is dat detectie van malware op basis van handtekeningen niet langer voldoende is. Slimmere endpointbescherming, met de mogelijkheid om voortdurend te controleren op verdacht gedrag en herstel mogelijk te maken, wordt essentieel.

• Het interne netwerk beter beschermen en kritieke systemen isoleren

Grote, platte netwerken zijn misschien eenvoudiger te beheren, maar ze maken het voor aanvallers eenvoudiger om hun doel te bereiken. Extra, concentrische lagen van netwerksegmentatie en -controle rond kritieke systemen en gegevens, zorgen ervoor dat één malware-infectie minder kans heeft om kritieke diensten te treffen. Zakelijke IT-systemen lopen meestal het grootste risico, omdat ze voortdurend e-mail verzenden en ontvangen. Daarom moeten ze gescheiden worden gehouden van de infrastructuur en gegevens van de 'kroonjuwelen' van een organisatie.

• Implementeer offline opslag en back-up op tape

Het concept van back-up is als gespreksonderwerp bijna verdwenen - en dat is een slechte zaak. De online, geautomatiseerde back-ups van vandaag zijn naadloos, handig en geautomatiseerd, maar helaas ook kwetsbaar voor aanvallen. Als een aanvaller de beheerdersgegevens kan stelen, kan hij de hele back-up wissen of beschadigen. Hierdoor is het niet meer mogelijk om de data te herstellen. De dagen van tapes en busjes zijn voorbij. Maar het is essentieel dat er een duidelijk model bestaat om back-ups naar echte offline opslag te verplaatsen om ze uit de handen te houden van externe kwaadwillenden.
Zes essentiële aanbevelingen, rechtstreeks van het toetsenbord van een miljoenenbende op het gebied van ransomware. Werk met dit basisadvies om ervoor te zorgen dat je organisatie de kans op besmetting verkleint. Onthoud dat veel van deze aanvallen opportunistisch zijn. Je hoeft geen perfecte beveiliging te hebben, maar wel net genoeg om ervoor te zorgen dat de aanvaller zich realiseert dat zijn kosten/batenanalyse elders beter uitpakt. Het is misschien egoïstisch, maar er schuilt een kern van waarheid in het oude gezegde: "Je slot moet beter zijn dan dat van de buren."

Andrew Rose is Resident CISO, EMEA bij Proofpoint

Cybersecurity industrie is ziek

Het aantal berichten over succesvolle ransomware stijgt onophoudelijk, het aantal gehackte bedrijven neemt nog dagelijks toe en de cybercriminelen verdienen meer geld dan ooit tevoren. Wat gaat hier mis?

Ondanks de hierboven genoemde feiten, nemen veel organisaties cybersecurity nog steeds niet serieus genoeg met als gevolg dat er te weinig wordt geïnvesteerd in cybersecurity. Dit blijkt vooral uit het feit dat relatief eenvoudige aanvallen, zoals ransomware, nog steeds zeer succesvol zijn (voor de cybercriminelen) en blijkbaar niet kunnen worden voorkomen. Waarschijnlijk ontbreekt de noodzakelijke basale cyber-hygiëne nog steeds bij een groot aantal organisaties, wat onbegrijpelijk is in de huidige digitale wereld. Tevens constateer ik dat er nog steeds teveel organisaties geen CISO met het benodigde mandaat hebben aangesteld. Een CISO met mandaat en die een Zero Trust aanpak nastreeft, kan in de huidige complexe tijd namelijk het verschil maken tussen wel of niet worden gehackt.

Aan de andere kant zijn er ook veel te veel securitybedrijven in de wereld, die allemaal hun eigen 'oplossing' promoten. Het draait blijkbaar alleen om hun eigen winst en niet om het algemeen belang. Uitzonderingen daargelaten, wordt er vooral geconcurreerd en niet samengewerkt. Daarnaast hebben investeringsmaatschappijen deze groeimarkt ook ontdekt, waardoor er een levendige handel is ontstaan in cybersecurity bedrijven. Het gevolg is dat er voortdurend nieuwe cybersecuritybedrijven worden opgericht, die allemaal met een vergelijkbare oplossing komen waardoor de cybersecurityindustrie nog voller wordt met 'point products'. Dit komt de overkoepelende aanpak van cybercriminaliteit niet ten goede.
Als wij dan iets verder inzoomen op de cybersecurity bedrijven zelf en met name op de bedrijven die cyberconsultancydiensten aanbieden, dan constateer ik nog steeds dat mensen met minimale cybersecurity ervaring, een dansdiploma en een certificering van een multiple-choice cybersecurity cursus bij klanten worden gepositioneerd als 'cybersecurity advisor' or ' cloud security architect'. Blijkbaar is echte cybersecurity ervaring in het veld niet noodzakelijk om gedegen cyber advies te kunnen geven. Daarnaast helpt het ook niet dat de organisaties, die CISO-vacatures plaatsen, geen idee hebben waar een CISO aan moet voldoen. Het gevolg is dat er een schaap met de vijf poten wordt gevraagd met minimaal 10 jaar ervaring voor een zeer mager salaris.

Hoe zit het dan bij de overheid?

Helaas is de situatie bij overheden niet veel beter, want ook hier wordt cybersecurity niet gezien als 'core business', maar meer als 'noodzakelijk kwaad'. Dit blijkt vooral uit de salarisschalen waarmee overheidsorganisaties proberen cybersecurity professionals aan te trekken. Een voorbeeld hiervan is de functie van CISO bij de Nationale Politie, die verantwoordelijk is voor de IT-beveiliging van het gehele (!) Nederlandse politiecorps. De vacature tekst beschrijft dat de maximale vergoeding ligt op een schaal 14 (6.889 euro bruto), hetgeen niet in verhouding ligt met de taken en verantwoordelijkheden van een CISO-functie voor de Nationale Politie. 'If you pay peanuts, you get monkeys'.

Daarnaast is cybersecurity binnen de overheid enorm versnipperd, hetgeen het delen van informatie en het leren van de 'lessons learned' niet ten goede komt. Er is geen centrale plaats of organisatie waar alle belangrijke informatie wordt verzameld, verbanden worden gelegd en waar de lessen daadwerkelijk kunnen worden geleerd op basis waarvan vervolgens beleid kan worden ontwikkeld. Er zijn weliswaar verschillende 'verzamelingscentra' (NCSC, Digital Trust Center, HSD, ECP, Brainport Eindhoven, AIVD, MIVD, Nationale Politie, High Tech Crime Team, regionale politiecorpsen, etc.) die allemaal hun eigen 'ding doen', maar van enige centralisatie is geen sprake.

Is het dan alleen maar 'kommer en kwel'?

Nee, gelukkig zijn er ook positieve ontwikkelingen te melden. De roep om een ministerie van Digitale Zaken wordt steeds luider, evenals de wens om het vak 'Digitalisering' op basis- en middelbare scholen in te voeren. Daarnaast zijn er natuurlijk organisaties die cybersecurity wel serieus nemen en de juiste investeringen durven te doen in cybersecurity. Dit zijn dan ook de bedrijven die het begrijpen en die wij NIET op de voorpagina's vinden als er weer een succesvolle ransomware aanval is geweest …

Helaas zijn dit de uitzonderingen en is het merendeel van de organisaties nog steeds niet echt wakker, wat in mijn ogen onbegrijpelijk is als je ziet hoe de digitale wereld werkt. Daarnaast werkt de cybersecurityindustrie ook niet echt mee en blijven de honderden (!) cybersecurity bedrijven hun 'point products' aanbieden, zoals ze al jaren doen … Helaas, omdat organisaties daar nog steeds om vragen. De cybersecurity industrie is ziek en moet snel beter worden!

Fred Streefland is directeur Cybersecurity (CSO/DPO) bij Hikvision.

Goed change management is cruciaal bij elk IAM-project

Bij een Identity & Access Management-project (IAM) is zelden tot nooit sprake van een greenfield-situatie. Elke organisatie werkt op de een of andere manier al met toegangsbeheer. Zodra er aanleiding is om te veranderen of te vernieuwen, betekent dit dat je als organisatie ingrijpt in een bestaande situatie. Change management dus, waarmee direct duidelijk wordt dat IAM niet alleen gezien moet worden als een IT-project. Eigenlijk liggen op IT-vlak de minste uitdagingen. Tools en oplossingen voor IAM zijn tegenwoordig immers volwassen, werken op basis van configuratie in plaats van op echt ontwikkelaarswerk, zijn gebaseerd op standaarden en er is veel keus.

Uiteraard is het belangrijk om een goede selectie te maken van oplossingen die bij de organisatie passen, maar belangrijk is – zeker in het voortraject – om eerst goed zicht te krijgen op het volgende drieluik: governance/organisatie/compliance, proces en informatie, en technologie. Door deze drie vlakken goed in kaart te brengen, leg je een solide basis voor een succesvolle IAM-implementatie.

Governance/organisatie/compliance

Bij governance/organisatie/compliance gaat het om verantwoordelijkheid, eigenaarschap en in control zijn. Centrale vraag die hier wordt beantwoord, is: 'wie mag wat?' Met andere woorden: welke medewerkers hebben toegang tot welke applicaties en data? Bij het beantwoorden van deze vraag is het zaak om het eigenaarschap goed te definiëren. Bij een IAM-implementatie zijn altijd veel stakeholders betrokken. Op het moment dat iedereen eigenaar is van het drieluik governance/organisatie/compliance is niemand eigenaar. Daarom is het absoluut nodig om alle verantwoordelijkheden tot in detail vast te leggen, welke rollen bestaan en welke verantwoordelijkheden en autorisaties daaraan gekoppeld zijn, zodat er geen enkel misverstand mogelijk is. Dat is ook de basis voor compliancy. Je kunt immers aantonen dat alles goed is vastgelegd en voldoet aan regels.

Wat dit punt nog lastig kan maken, is de balans tussen gebruiksgemak en veiligheid. Vanuit organisatieoogpunt zijn veilige data en applicaties cruciaal. Maar dat beperkt een gebruiker in gebruiksgemak, waardoor het risico ontstaat dat medewerkers work-arounds gaan zoeken. Dat betekent dat alle spelregels glashelder moeten zijn en dat de juiste manier ook de makkelijke manier moet zijn. Het gaat uiteindelijk om enablement van elke gebruiker.

Processen en informatie

Onder deze punten regel je als organisatie belangrijke onderwerpen als instroom, doorstroom en uitstroom. Hoe verloopt het proces van autoriseren, welke uitzonderingen zijn bijvoorbeeld mogelijk? Bij deze onderwerpen speelt niet alleen de IT- of security-afdeling een belangrijke rol, maar vaak ook HR. Bij informatie gaat het om de kwaliteit van de data. Een proces kan 100 procent juist zijn, maar als de data die erbij horen, niet correct zijn, heeft zo'n proces geen of - nog erger - een tegengesteld effect.

Technologie

Wanneer de twee bovenstaande issues volledig zijn doorgelicht, kun je als organisatie op basis van productselectie met de juiste requirements een zoektocht starten naar de juiste technologie, die vervolgens geïmplementeerd kan worden. Daarbij is er altijd de kans op weerstand. Zoals al eerder opgemerkt, leidt een IAM-implementatie altijd tot een verandering van bestaande processen. Niet iedereen zal daar even blij mee zijn. Verandering kan bijvoorbeeld betekenen dat de IT-afdeling niet zomaar meer even snel een account aanmaakt of dat medewerkers accounts met elkaar kunnen delen. Daarom is het cruciaal om al bij de start heel goed te kijken naar alle persoonlijke belangen die er zijn. Elke medewerker zal overtuigd moeten zijn van het belang van goed en veilig toegangsbeheer.

Een IAM-project stopt niet als de tool is geïmplementeerd en in gebruik is genomen. IAM vraagt om continue aandacht. Het gaat erom een stabiele omgeving te creëren én die voor de lange termijn te houden. En juist daarom is een goede voorbereiding met oog voor alle aspecten van change management een voorwaarde voor een succesvolle en veilige inzet van IAM.

Jeroen Remie is securityconsultant bij Traxion