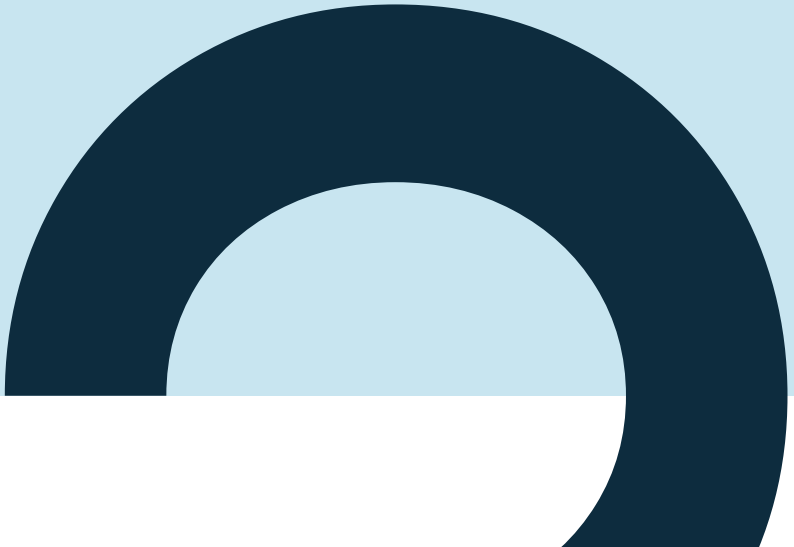
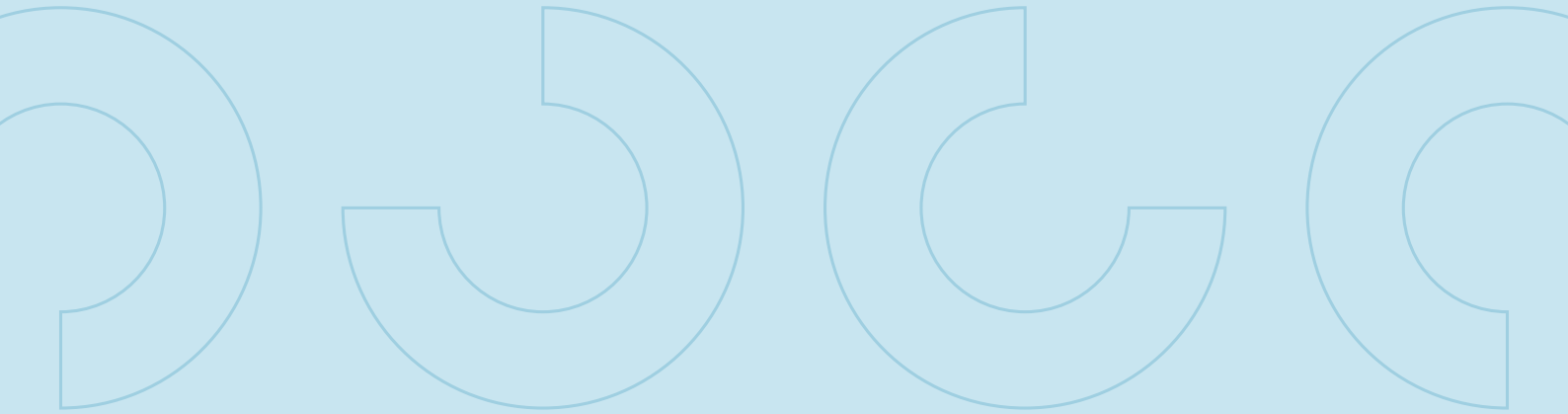
pinewood

2022

Cybersecurity Dreigingsbeeld en Adviesrapport NL

We see risks
before they hurt





Inhoudsopgave

Voorwoord

Met de juiste mix maken we een vuist tegen cybercrime

Voor u ligt het Cybersecurity Dreigingsbeeld & Advies Rapport NL dat wij – met grote hulp van onze klanten en externe en interne experts – samenstelden. We delen hierin onze kijk op de aanpak van cybersecurity maar ook die van gebruikersorganisaties en experts om ons heen. Hun scherpe blik en praktijkervaring op de huidige status van cybercrime en hun vaak interessante en gevarieerde visies op de bestrijding ervan, verrijkt ons eigen inzicht. Samen delen we best practices en tips waarmee u als lezer direct aan de slag kunt. In die zin is dit dreigingsbeeld dan ook zeker niet bedoeld om alleen te waarschuwen, laat staan angst aan te jagen, maar is het nadrukkelijk óók een middel om samen tot passende oplossingen te komen om uw organisatie veiliger te maken.

Gebalanceerde mix

Ransomware is in 2021 behoorlijk op de kaart gezet met gerichte aanvallen, waar bijvoorbeeld Mandemakers, VDL Nedcar, Mediamarkt en Bakker Logistiek over mee kunnen praten. Daarnaast zien we zero-day aanvallen door kwetsbaarheden van softwareleveranciers die hele ketens raken. Denk aan de recente voorbeelden van Microsoft Exchange server, Kaseya en natuurlijk Log4j. Deze bedreigingen vragen om een passend antwoord. En wat Pinewood betreft bestaat dat antwoord uit een gebalanceerde mix van vier pijlers: predictie, preventie, detectie en respons.

Predictie & Preventie

Met predictie signaleren we door middel van zowel menselijke als technologische intelligentie in een zeer vroeg stadium wat er gebeurt bij onze klanten. Met behulp van threat intelligence data, security-reviews en pentesten kijken we naar gaten en risico's, want wie vooruit kan kijken, is op (bijna) alles voorbereid. In de preventie-pijler adviseren we allerlei beveiligingsmaatregelen, zoals firewalls, mailbeveiliging, awareness kweken en kwetsbare plekken dichten. We bouwen in feite een klein bataljon. Dit is het element waar klanten het meeste gevoel bij hebben en ook relatief het meeste budget voor vrijmaken. Een slot op de deur is herkenbaar voor iedereen en als dat slot niet goed werkt kopen we een beter slot. Maar zoals we ook weten van dat slot: preventie alleen is niet genoeg. En dat brengt ons bij de volgende stap: detectie oftewel een camera op het huis.

Detectie & respons

Hoe zorgt u ervoor dat u zo snel mogelijk op de hoogte bent van een aanval? Dat de tijd waarin de kwetsbaarheid in uw infrastructuur wordt uitgebuit zo kort mogelijk is? Detectie geeft inzicht in risico's voordat het echt pijn gaat doen. Detectie is helaas – net zoals respons – lange tijd een ondergeschoven kind geweest. Maar ik zie langzaamaan een kentering. Organisaties ontdekken bovendien dat het mes van detectie aan twee kanten snijdt: het stelt de organisatie ook in staat om haar securitybeleid beter in te richten. Detectie geeft inzichten in organisatie zwakheden, en die zijn niet zelden ook mens-gerelateerd. Medewerkers die bewust of onbewust andere paden kiezen dan de IT-afdeling aanreikt; ongeoorloofd gebruik van een admin account, dat ene praktische tooltje uit de cloud,

user accounts met de verkeerde privileges of het wifi van een onbeveiligd koffiezaakje gebruiken.

Dankzij detectie kunt u risico's in een zo vroeg mogelijk stadium ontdekken. Maar ook hiervoor geldt dat dit geen 100% garanties geeft tegen hackers. Heeft u de schade toch niet kunnen voorkomen? Heeft de aanvaller langer dan u lief is zijn gang kunnen gaan? Dan is het belangrijk dat u kunt terugvallen op een van tevoren opgesteld respons-plan, waarin exact staat wat er moet gebeuren om de business weer op de rit te krijgen, wie waarvoor verantwoordelijk is en welke communicatie-stappen er gezet moeten worden.

Sterke beveiligingsketen

De meeste aanvallen kunt u met een van de vier pijlers ondervangen. Als u preventie goed inricht, voorkomt u al 95% van de ellende. Met een goede detectie houdt u nog eens 4% buiten de deur. De 1 of 2% die dan overblijft, is het risico dat u loopt. Hier vallen o.a. zero-day aanvallen onder, zoals de recente Log4j-kwetsbaarheid. Zelfs de duurste firewall helpt niet om dit soort uitwassen te voorkomen. Het gaat bij dit soort cases om de vraag: hoe snel detecteer en reageer je? De huidige trend van gerichte malware-aanvallen vraagt om een sterke beveiligingsketen.

Vuist tegen cybercrime

Met een integrale aanpak van predictie, preventie, detectie en respons maakt u pas écht een vuist tegen cybercrime. Bij Pinewood geven we een antwoord op alle vier de pijlers. Met ruim 28 jaar ervaring en meer dan 50 security specialisten bieden we een uitgekiende mix aan beveiligingsmaatregelen en advies. Met onze bewezen aanpak detecteren we en reageren we op digitale risico's in alle stadia voordat het pijn doet.

Ik wil de mensen die hebben meegewerkt aan de totstandkoming van dit rapport hartelijk danken voor hun bijdragen. Door het delen van kennis en samenwerking, brengen we security voor iedereen op een hoger niveau.

Ik wens u veel inspiratie en inzichten toe bij het lezen van ons Cybersecurity Dreigingsbeeld & Advies Rapport NL!

Sebastiaan Kors, CEO Pinewood

Situatie Oekraïne

Wij krijgen veel vragen van klanten over wat de situatie in de Oekraïne voor gevolgen heeft op onze cybersecurity. Op het moment van dit schrijven zien wij geen verontrustende activiteiten. Wel hebben we een verhoogde alertheid op het monitoren van bepaalde indicatoren. Het zijn open deuren, maar we blijven daarnaast hameren op de basismaatregelen die maar al te vaak niet op orde zijn: updaten, segmenteren, bewustzijn creëren, multi-factor authenticatie en monitoring. Een opgenomen webinar over dit onderwerp kunt u hier terugzien

Fotografie: Arenda Oomen

Column

Petra Oldengarm, directeur van Cyberveilig Nederland

Cyberdreigingen nemen toe in aantal en worden steeds complexer. Criminelen organiseren zich constant op een andere manier en dat maakt ze ongrijpbaar. En hoewel de meeste bedrijven inmiddels wel degelijk aan risicomanagement doen, zie ik dat de effecten van deze exercitie afnemen.

Hoe dat komt? Bij risicomanagement maak je een rekensom: wat zijn de kroonjuwelen van mijn bedrijf, welke dreigingen liggen er op de loer, hoe groot is de kans dat een dreiging mij bereikt, wat is dan de potentiële impact en welke maatregelen kan ik nemen? Het lastige is dat deze rekensom niet een eenduidige en goed te interpreteren uitkomst kent. Het is bijvoorbeeld haast onmogelijk om de kans dat een aanval jou treft, goed te kwantificeren. Onder meer doordat je simpelweg niet alles kúnt overzien. Je kunt als bedrijf oneindig aan risicomanagement doen en toch een kwestie als Log4j niet zien aankomen. Logisch: het probleem is te abstract, te groot en te onoverzichtelijk.

> 'Cybercrime as a service wint gestaag aan terrein'

Dat komt ook doordat het dreigingslandschap complexer wordt. Cybercriminelen werken

steeds meer in een keten. Vroeger was één crimineel verantwoordelijk voor het gehele incident; van voorbereiding tot aanval tot afpersing. Tegenwoordig werken criminelen slim samen en nemen ze elk een eigen stukje van de aanvalsketen voor hun rekening. Zo ontstaat een ware killchain met allerlei verschillende criminele partijen die hun eigen expertise hebben, hun eigen kunstje uitvoeren en dat vervolgens doorverkopen aan de volgende. Cybercrime as a service wint gestaag aan terrein.

Deze ketenaanpak in cybercrime vraagt om een ketenaanpak in de verdediging. Bij de ontwikkeling van cybersecurity moeten we minder kijken naar wat ieder individu doet en het meer zoeken in groter verband. Eilandjes (lees: silo's) aan elkaar verbinden. Informatie uitwisselen. Bedrijven moeten zelf hun weerbaarheid op orde brengen én breder met elkaar gaan samenwerken. En daar schort het nou net aan. Bedrijven die alleen naar preventie kijken maar niets doen, delven het onderspit. Wil je weerbaarder worden tegen die killchain dan moet je gaan voor het totaalpakket van preventie, detectie en respons. En we moeten breder met elkaar beschikbare informatie uitwisselen over aanvallen en verdedigingstechnieken. Alleen dán winnen we de wapenwedloop die nu gaande is.

Een cybercrimineel heeft maar één backdoor nodig om binnen te komen. En aanvallen is daarmee makkelijker dan verdedigen, ofwel alle gaten zien te dichten. Toch is betere bescherming mogelijk. Ik vind dat naast het bedrijfsleven ook de overheid hier een taak heeft. De taak om de regie over het gehele landschap te voeren. Problemen te onderkennen. Wetgeving te maken die de hele keten raakt. Certificeringen te helpen ontwikkelen. Informatie te delen. Als je krachten bundelt, overheid en bedrijfsleven bij elkaar brengt en de samenwerking verbetert, komen we een heel eind.'

Alla Ponkina, ICT Security Manager bij Meander MC

Meander MC loopt binnen de zorgsector mede voorop als het gaat om cybersecurity. Het ziekenhuis was de eerste klant die een plek kreeg in het SOC van Pinewood. Alla Ponkina is ICT Security Manager bij dit topklinisch ziekenhuis in Amersfoort en weet dat cybercriminelen de weg naar de medische zorg steeds beter weten te vinden. 'Ransomware is een wurggreep die ook óns kan treffen.'

'Cybercriminelen gaan over lijken. In ons geval helaas letterlijk, want terwijl bij ransomware-aanvallen in andere sectoren grote geldbedragen gemoeid zijn, gaat het bij ons om leven en dood. Het voorbeeld van de patiënt in Duitsland die overleed nadat zijn ambulance moest uitwijken vanwege een hack, is schrijnend én dichtbij. Of ik me zorgen maak? Dat is te groot aangezet maar ik denk wel dat het een kwestie van tijd is voordat het onheil ook ons treft.' Alla Ponkina komt uit het bedrijfsleven en ziet dat in vergelijking daarmee de systeembeheerders van het Meander MC extra gemotiveerd zijn om cybercrime aan te pakken. 'Het is een heel ander soort motivatie dan ik in het bedrijfsleven gewend ben, een meer intrinsieke motivatie. De zorg gaat onze mensen aan het hart. Iedereen hier heeft patiëntveiligheid hoog in het vaandel en weet dat cybercrime daar directe afbreuk aan doet.'

eHealth en slimme koelkasten

De pogingen tot cybercrime in de zorg zijn tegenwoordig helaas aan de orde van de dag, weet Ponkina. 'Dat heeft verschillende oorzaken. Criminelen bereiden zich beter voor en vallen niet meer lukraak aan, maar met een duidelijk target en een glashelder doel voor ogen. Het is een zeer lucratieve business. Het ziekenhuis is een data gedreven organisatie geworden en gezondheidsdata zijn véél waard op de zwarte markt. Dit vraagt om non-stop alertheid en monitoring. Daarnaast zijn ziekenhuizen in toenemende mate afhankelijk van externe leveranciers voor hun IT-systemen. Ligt de IT plat, dan ligt het ziekenhuis plat. Natuurlijk zijn er dan noodprocedures, maar je kunt geen volwaardige zorg blijven leveren als je geen IT hebt. Door Corona heeft eHealth een vlucht genomen en is de afhankelijkheid alleen maar groter geworden. Wat ik ook zie, is dat alle medische techniek binnen een ziekenhuis, meer dan voorheen, onderdeel van het netwerk is. Hartmonitoring, de infuuspomp, maar ook het gebouwbeheersysteem, slimme koelkasten en voorraadsystemen; alles is met elkaar verbonden. Raak één onderdeel, en je kan het gehele systeem raken.'

> 'De zorg wordt zéker niet ontzien door cybercriminelen'

Cyber security structureel op de kalender

Meander MC zet – in samenwerking met Pinewood – stevig in op detectie en respons. 'Dat helpt enorm. Maar wat minstens zo helpt, is awareness. Daarmee zit het binnen onze ziekenhuismuren wel goed en daar ben ik best trots op. We werken er ook hard voor. In overleg met teammanagers en medische staf wordt regelmatig aandacht besteed aan het belang van cybersecurity. Steeds wisselende artsen zijn onze ambassadeurs en gaan binnen het ziekenhuis de boer op om te hameren op het belang van het beschermen van onze patiënten en onszelf. Op onze kwaliteitskalender wordt elke maand een veiligheidsaspect ingepland, cybersecurity en privacy hebben hun eigen themamaand in november. De voorzitter van onze Raad van Bestuur is ook voorzitter van de Stuurgroep Informatiebeveiliging & Privacy. Niet alleen bij ons, maar bij steeds meer ziekenhuizen zie ik het thema op de bestuurlijke agenda staan, en wordt het als een strategisch risico. Dat is zeker geen overbodige luxe. Het zorgt ervoor dat cybersecurity meer wordt dan een nice-to-have; het wordt een integrale built-in.'

Middelen en mankracht

'De grootste uitdaging voor cybersecurity in ziekenhuizen is meestal om het rond te krijgen op financieel en bezettingsvlak,' vervolgt Ponkina. 'Het budget voor IT en cybersecurity moet drastisch omhoog om de dreigingen het hoofd te kunnen blijven bieden. Voor middelen maar ook voor mankracht, want de arbeidsmarkt is krap en het bedrijfsleven betaalt nou eenmaal beter. Het budget bij Meander is gegroeid én wordt goed besteed. Dat komt voornamelijk doordat onze RvB de urgentie ziet. Tijdens een cyberoefening met ransomware lieten we een klok aflopen, net als bij een echte ransomware aanval. Losgeld; dat is de nachtmerrie van iedere bestuurder. Dus dát kwam wel aan!'

Organisatie	Impact
ERP-clouddienst	Twee zorginstellingen hadden enkele dagen geen toegang tot het ERP-systeem (Enterprise Resoucre Planning). Hierdoor moesten bestellingen via een omweg worden gedaan. Ook kon het voorraadbeheer en de logistieke afhandeling niet worden ingezien.
Subverwerker van een data-analysebedrijf	Patiëntendata van vier laboratoria waren ontoegangkelijk
Leverancier medische apparaten	Leverancier kon bepaalde onderhoudstaken niet uitvoeren doordat het ziekenhuis uit voorzorg de VPN-verbinding dichtzette.
Organisatie voor professionele ontwikkeling	Niet-gevoelige data van meer dan twintig zorgorganisaties werden versleuteld.
Toeleverancier kantoorartikelen	Nihil, alleen vertragingen van leveringen.
Ziekenhuizen en GGZ-instellingen	Verschillende leveranciers en zorginstellingen namen met spoed preventieve maatregelen, omdat er een kwetsbaarheid was in Kaseya VSA die op grote schaal werd misbruikt door een ransomware-groep.

Bron: Cybersecurity Dreigingsbeeld Zorg van Z-Cert
Toelichting tabel: uit deze data blijkt dat de meeste ransomware-incidenten zijn gestart bij de leveranciers van de keten.

Tips van Alla Ponkina

- Uit eigen ervaring weet ik: wil je cybersecurity aanpakken, dan is het van cruciaal belang dat de RvB het uitdraagt. Dat is dus de eerste stap!
- Zorg ook voor draagvlak op andere niveaus; van management tot medische en verpleegkundige staf.
- De markt van cybersecurity-talent is krap en uitdagend maar laat dit geen risico's opleveren; zorg dat je ook kunt terugvallen op externe expertise.
- Iets met een kalf en een put: bereid het incidentresponsplan en de responsstructuur al voor in de koude fase en niet pas als de dreiging zich aandient.
- Oefenen, oefenen, oefenen: wij doen het periodiek en binnen álle lagen van onze organisatie.

Fotografie: Joke Schut

Wim Hafkamp, Managing Director Z-CERT

De teller op onze website onthult dé grootste bedreiging die de zorgsector op dit moment kent: ransomware. Steeds vaker en steeds gerichter zetten cybercriminelen gijzelsoftware in om slachtoffers te maken. En steeds vaker treffen hun pijlen ook de zorg. Tot nu toe zijn met name buitenlandse zorginstellingen doelwit - onder meer in de VS, Ierland en Duitsland. Maar ook in Nederland zijn de eerste voorbeelden de revue gepasseerd.

Ransomware leidt direct tot 'onbeschikbaarheid' in allerlei verschijningsvormen. Het beïnvloedt mogelijk het zorgproces en doet sterke afbreuk aan de patiëntveiligheid. Een schrijnend voorbeeld van de impact komt uit Duitsland, waar in 2021 een deel van een Duits ziekenhuis plat lag door een ransomware-aanval. Een ambulance moest uitwijken naar een ander ziekenhuis en de patiënt die erin vervoerd werd, overleed onderweg. Natuurlijk valt niet 100% hard te maken dat de cybercriminelen hier bloed aan hun handen hebben maar wie logisch nadenkt, zal geen andere conclusie kunnen trekken dan dat het niet beschikbaar zijn van het ziekenhuis een rol heeft gespeeld.

Een andere trend die ik zie is dat steeds vaker leveranciers geraakt worden. En juist leveranciers worden steeds belangrijker voor zorginstellingen. Hun kwetsbaarheid wordt daarmee de kwetsbaarheid van de zorg. De eerste voorbeelden van extern ingekochte, door cybercriminaliteit aangevallen voorraadbeheersystemen hebben we al gezien. De impact: geen zicht op de voorraad van medische hulpmiddelen waardoor een middel mogelijk niet voorhanden is wanneer de nood hoog is.

> 'Geen zorgorganisatie kan nog zonder eigen CISO'

Wat kun je doen als zorgorganisatie? Met de 10 gouden tips tegen ransomware die wij opstelden, voorkom je op voorhand al heel wat ellende. Zorg bijvoorbeeld dat de afspraken die je met een leverancier maakt, hard en dichtgetimmerd zijn. Houd toezicht op deze afspraken en voer controle uit. Het is allang niet meer voldoende als een leverancier NEN7510 gecertificeerd is. Zo vereist deze certificering een back-up maar als je dat alleen online doet en gehackt wordt, ben je nergens meer. Spreek dus met een leverancier af dat er naast een online back-up ook fysieke data behouden worden. Zorg daarnaast dat je een 24/7 crisisorganisatie achter de hand hebt, die klaar staat wanneer het fout gaat en die

exact weet welke stappen gezet moeten worden om schade te beperken. Cybercriminelen slaan 'toevalligerwijs' meestal toe op vrijdagmiddag, als onze eigen aandacht – met het weekend in zicht - enigszins begint te verslappen.

Een onafhankelijke partij die niet alleen audits uitvoert op het certificaat maar ook checkt of verder alles op orde is, die toezicht houdt, penetratietesten uitvoert en een controlerende rol heeft, zou uitkomst bieden. Of wij die rol op ons moeten nemen? We denken erover na. Vooralsnog zien wij onszelf vooral als expert-adviseur en niet als controleur. En daarnaast: zorgbestuurders hebben ook een verantwoordelijkheid om zich te verdiepen in de risico's. Als je digitaliseert binnen je organisatie, dan moet je snappen wat dat betekent. Je hoeft natuurlijk niet zelf de security officer te worden maar je moet als bestuurder wel de juiste prioriteiten stellen en weten waar je je geld in stopt. Voor veel bestuurders is cybersecurity een ver-van-hun-bed-show, een van de aandachtsgebieden van de CFO, met niet altijd voldoende urgentie. Maar dat moet écht veranderen. Benoem een aparte CISO en geef hem of haar een podium in het bestuur. Cybersecurity is té belangrijk om er 'even bij te doen'.

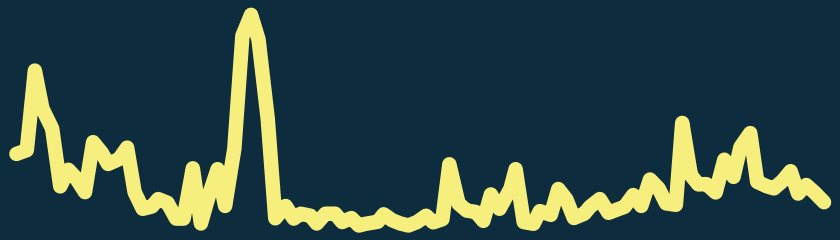
10 gouden tips tegen ransomware

1. Implementeer Applicatiewhitelisting
2. Stop of reguleer Office macro's
3. Patch applicaties en gebruik de laatste versies
4. Beveilig afstandswerkoplossingen
5. Scan de buitenkant van uw IT-infrastructuur
6. Beveilig uw applicaties
7. Pas least privilege principes toe
8. Maak regelmatig back-ups van belangrijke data
9. Patch de Operating Systems van uw apparaten
10. Implementeer multifactor authenticatie

Bron: Z-Cert, Cybersecurity Dreigingsbeeld Zorg 2021

Over Z-CERT

Z-CERT is het onafhankelijk expertisecentrum voor cybersecurity in de zorg. Z-CERT ontvangt informatie van het Nationaal Cyber Security Centrum en andere (inter)nationale CERTS en partners en vertaalt deze informatie naar producten en diensten, zoals het ZorgDetectieNetwerk (ZDN). Ook het SOC van Pinewood levert een bijdrage aan het ZDN. Ruim 190 ziekenhuizen en andere zorginstellingen maken momenteel gebruik van de diensten van Z-CERT.



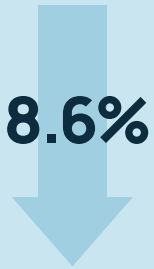
Misbruik Log4j-kwetsbaarheid leeft op

Eind **december 2021** kwam de kwetsbaarheid in de Apache library Log4j naar buiten. Op **8 januari 2022** is er een duidelijke piek in het aantal pogingen om die uit te buiten. Opvallend is dat de pogingen daarna flink afnemen tot **begin februari**. Vanaf dat moment zien we juist weer een toename en een licht stijgende lijn gedurende meerdere weken.

De speld in de hooiberg

Er vinden miljoenen events plaats in een gemiddeld netwerk van een bedrijf. Deze kun je onmogelijk allemaal stuk voor stuk nalopen op mogelijk malafide eigenschappen; het geeft de noodzaak van een SOC aan. De verhouding staat gemiddeld op **364 miljoen ruwe events,** tot **105 alarmen** in het SIEM, tot **1 incidentmelding** richting klant. Kortom, de speld in de hooiberg is lastig te vinden, maar gelukkig wordt hij wel gevonden.

Ruwe events.....364.702.187
Alarmen 105
Incidentmeldingen 1

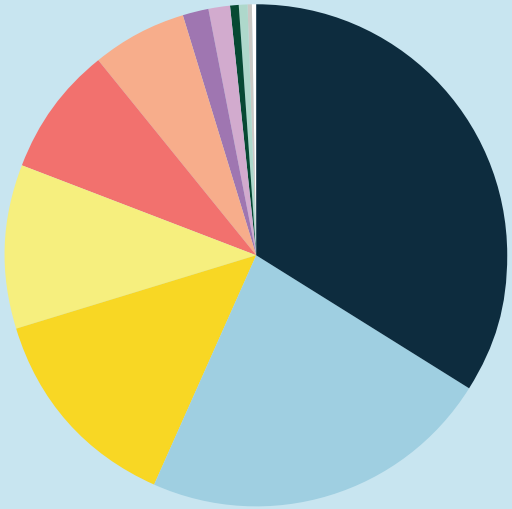


Cybersecurity-inbreuken verminderen de waarde van openbare bedrijven met naar schatting 8.6%
Bron: Compitech

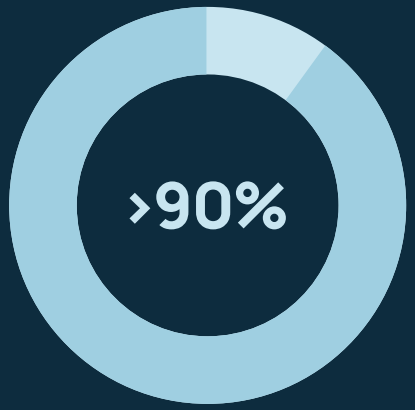
85% van de cybersecurity-inbreuken wordt veroorzaakt door menselijke fouten.
Bron: Verizon

Van de ransomware-incidenten in 2021 had 40 procent voorkomen kunnen worden als de RDP niet was ontsloten via internet.
Bron: Z-Cert, D

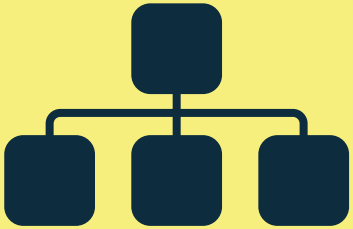
Aanvallen gericht op oudere kwetsbaarheden



- IDS/IPS/EDR event - 34,1%
- Suspicious login - 22,6%
- Device health - 13,6%
- Indicator hit - 10,6%
- Suspicious network connection - 8,3%
- Malware event - 6,1%
- Suspicious Windows event- 1,7%
- Other - 1,6%
- App consent - 0,5%
- Suspicious file - 0,5%
- Anomaly - 0,2%
- Suspicious account actions - 0,2%



Meer dan 90% van de malware komt via e-mail
Bron: CSO Online



43% van het midden- en kleinbedrijf (MKB) heeft nog geen plannen voor cybersecurity
Bron: Bull Guard

Farida, Chief Information Security Officer

Farida is al zestien jaar werkzaam in uiteenlopende functies binnen cybersecurity. Ze begaf zich in verschillende sectoren: industrie, logistiek, telecom, publieke sector en op dit moment zet ze haar ervaring in als CISO binnen de advocatuur. Farida signaleert dat de toenemende afhankelijkheid van externe software-leveranciers vraagt om een organisatorische herstructurering. Ook aan de respons-kant is winst te behalen.

'Log4j heeft ons weer eens met de neus op de feiten gedrukt: de grootste dreiging van dit moment is de kwetsbaarheid die organisaties krijgen als ze softwaresystemen van externe leveranciers inkopen,' stelt Farida. 'De kwestie Log4j is een tekenend voorbeeld van hoe een kwetsbaarheid ergens in de keten ontdekt wordt door hackers, en vervolgens een aanval uitvoeren met een gigantisch bereik.'

Compliance dichttimmeren

Die afhankelijkheid is niet te voorkomen, vindt Farida. 'Je kunt niet alles zelf ontwikkelen. De wereldeconomie is ook ingericht om samen te werken en te specialiseren. Je wilt nu eenmaal gebruikmaken van de dienstverlening van experts. Maar deze impactvolle trend vraagt wel om een stevig antwoord op het vlak van preventie, detectie en respons. Het begint met het dichttimmeren van controle en compliance. Organisaties toetsen hun leveranciers nauwelijks. Ook ontbreken vaak goede afspraken met leveranciers over privacy. Het is de waan van de dag die deze blind spot veroorzaakt.'

> 'Informatiebeveiliging hoort thuis bij compliance, niet bij IT'

Organisatorische change

Farida pleit voor een organisatorische herindeling. 'Richt een gedegen procurement-afdeling in en laat het niet over aan willekeurige medewerkers. Plaats informatiebeveiliging niet onder IT maar onder compliance; dat is waar het thuishoort. IT richt de techniek in, compliance doet de controle. Anders keurt de slager zijn eigen vlees. Richt je SOC goed in en werk er ook echt mee samen. Deel de bedrijfsrisico's met de analisten van het SOC zodat ze hun detectie gericht kunnen inrichten. Alleen als een SOC wordt meegenomen in alles wat je als bedrijf doet, kan 't zijn werk goed en effectief uitvoeren.'

Respons als integraal bedrijfsonderdeel

Een goed antwoord op deze actuele dreiging is mede afhankelijk van de reactiesnelheid, het soort respons en hoe dit is ingebed in de organisatie. 'Die respons moet onderdeel zijn van het crisismanagementplan. Alleen door deze integratie kun je respons-maatregelen goed inrichten. De respons hoort ook thuis in het bedrijfs-communicatieplan, zowel als het gaat om interne als om externe communicatie. Wanneer de hack naar buiten komt, moet je ook weten wat je de media gaat vertellen. Het lijkt voor veel bedrijven misschien overdreven om op deze manier je responsplan klaar te hebben liggen, maar het is bittere noodzaak. Het is namelijk niet meer de vraag óf je wordt gehackt maar wanneer ben je gehackt.'

Farida's aanbevelingen voor CISO's

1. Zorg voor een goede governance-structuur waarmee je controle kunt uitvoeren op je leveranciers.
2. Maak van afspraken over privacy en security een vast onderdeel van elk leverancierscontract.
3. Onderschat nooit het belang van detectie: neem je SOC mee in alles wat er in het bedrijf gebeurt.
4. Neem iedereen binnen je organisatie mee in jouw dagelijkse kost: laat in hack-simulaties zien dat de risico's voor iedereen gelden en niet alleen een 'IT-dingetje' zijn en vertaal externe nieuwsberichten naar risico's binnen de eigen organisatie.
5. Reken de directie voor wat de potentiële business impact is van een aanval en zorg zo dat er voldoende aandacht (en budget!) is voor de juiste respons.

Samuel Bergmann, Security Business Consultant bij Pinewood

Samuel Bergmann houdt zich als Security Business Consultant bezig met de beleidskant van cybersecurity. Op zijn bord ligt een belangrijke maar niet eenvoudige taak, want bedrijven zien nog altijd te weinig in dat cybersecurity niet alleen maar gaat over technische maatregelen maar ook om menselijke zaken zoals beleid en organisatie. Vijf vragen aan Bergmann.

Welke trends zie jij op het gebied cybersecurity?

'De rol van systeembeheerder is langzaamaan aan het verdwijnen uit de bedrijfsorganogrammen. We zien IT in toenemende mate als een dienst die je inkoopt bij externe partijen. Zo wordt Microsoft, Amazon of Google je systeembeheerder. Het personeelsdossier zit niet meer in de map bij HR maar staat online. Een begrijpelijke trend, want het voelt goed om dingen uit te besteden. Bedrijven kopen op die manier gemak en tijd. Anderzijds geeft het bedrijven ook een vals gevoel van veiligheid. Er zijn simpelweg zaken die je niet uit handen kunt geven. HR moet bepalen wie toegang mag hebben tot personeelsdossiers, niet de software. Gaat een medewerker uit dienst, dan moet HR ervoor zorgen dat hij of zij niet langer toegang heeft tot gevoelige bedrijfsinformatie. Je mag dus nooit uit het oog verliezen dat je als bedrijf zelf moet meedenken en maatregelen moet nemen. Het is de mens die het (ook) moet doen, niet (alleen) de technologie.'

Wat moet er gebeuren om bedrijven hiervan te overtuigen?

'Awareness is key. Wie de risico's niet kent en de impact van cyber-aanvallen niet ziet, zal niet begrijpen dat cybersecurity iets is waar iedereen binnen een bedrijf mee bezig moet zijn. Gelukkig groeit dit bewustzijn. De olietanker is aan het keren. In mijn werk als Business Consultant zie ik dat de risico's steeds meer gevoeld worden. Dat komt ook door de harde realiteit: ransomware heeft een flinke vlucht genomen en raakt steeds meer organisaties. Bedrijven vragen zich massaal hardop af: kan dit ook bij ons gebeuren, hoe krijgen we grip en controle en hoe vinden we de balans tussen uitbesteden aan externe leveranciers en zelf vinger aan de pols houden? Vanuit Pinewood helpen we ze met de antwoorden. We doen een security review, brengen risicomanagement in kaart en adviseren. Met die aanpak geven we bedrijven een stuk grip terug.'

Welk misverstand over cybersecurity kom je het meest tegen bij jullie klanten?

'Het grootste misverstand is dat, als je de juiste preventieve maatregelen hebt genomen, je veilig bent. Het security-landschap wordt steeds

complexer. Detectie is belangrijker dan ooit. Als je gaat monitoren, zie je meer en kun je meer voorkomen.'

Wat is er nog te doen?
'Van alles. Vanuit de overheid komt er steeds meer druk op het bedrijfsleven om cybersecurity inzichtelijk én op orde te hebben. Maar in feite stuurt de overheid bedrijven het bos in. Veel bedrijven missen de kennis en kunde om écht goed te weten wat van ze verlangd wordt. Er is winst te behalen als we kijken naar het gat tussen wat overheid en wetgeving eisen en wat bedrijven weten.'

> 'De awareness groeit, nu nog zorgen voor verankering in de bedrijfsprocessen!'

Wat kunnen bedrijven zelf doen?
'Naast hulp inschakelen kunnen bedrijven inderdaad zelf ook wat zaken aanpakken. Voor het levend houden van informatiebeveiliging is nog altijd geen standaard onderdeel van bedrijfsprocessen. Het ligt vaak alleen nog bij IT. Bij bijvoorbeeld BHV krijgt iedereen uitleg over waar de nooduitgangen zijn. En iedereen doet verplicht mee met de brandoefening. Maar op het moment van een security-incident, zit iedereen naar elkaar te kijken. Wat moeten we doen en wie mag op welke knop drukken? Door cybersecurity stevig in te bedden in je bedrijfsprocessen en draaiboeken klaar te leggen, geef je het de aandacht die het verdient en die noodzakelijk is om dreigingen het hoofd te bieden. Kortom: de awareness groeit, nu nog verankeren in de processen!'

Joost Gijzel, Head of Incident Response bij DataExpert

Joost Gijzel helpt samen met zijn collega's organisaties die getroffen zijn door een cyberincident. Als een soort digitale brandweer zoals Gijzel het zelf noemt, zorgt het DataExpert Cyber Emergency Response Team dat deze organisaties – van overheid tot maakindustrie - zo snel mogelijk weer back in business zijn. Alles om de schade zoveel mogelijk te beperken. 'Het begint bij een nieuwe mindset.'

'Een cyberincident is een bedrijfscrisis. Eentje waarbij ontzettend veel aspecten een rol spelen. Hoe communiceren we intern en extern wat er aan de hand is? Hoe houden we het hoofd koel en de business draaiende? Hoe kunnen we de schade beperken? Het gaat om meer dan alleen techniek; ook bedrijfscultuur en -processen spelen een rol.'

Ketenaanvallen

'Waar voorheen heel gericht werd getarget op een bank of een KLM, kan nu in feite iedereen slachtoffer worden, ziet Gijzel. 'Van kleine ondernemer tot MKB+ tot grote corporate. Dat komt doordat de aanvalsstructuur beter georganiseerd is. Er vinden steeds meer ketenaanvallen plaats, waarbij degene die de achterdeur openzet niet dezelfde is die de aanval uitvoert. Criminelen maken bovendien gretig gebruik van bestaande lekken. Er wordt dus gezocht naar generieke zwaktes in systemen en daarmee wordt de bandbreedte van potentiële slachtoffers enorm.'

Nieuwe mindset

Dit betekent natuurlijk dat iedereen zijn systemen zodanig moet inrichten dat hij geen slachtoffer wordt. Maar het betekent vooral dat meer dan ooit tevoren respons iets is waar de volle aandacht naartoe moet. Gijzel: 'Voorbereid zijn. Dat begint bij een nieuwe mindset: het gaat namelijk gebeuren. Die aanval gaat er komen. Vroeg of laat. Het is, met de kaders die ik net schetste, een voldongen feit. Heb je dat eenmaal erkend, dan heb je als organisatie de belangrijkste stap gezet.'

Draaiboek

'Daarna volgt de volgende essentiële stap, vervolgt Gijzel. 'Want je bent er niet met het inzetten van de juiste techniek om cybercrime te voorkomen. Natuurlijk moet er gedetecteerd en geanalyseerd worden maar als je uitgangspunt is dat je op een dag aan de beurt bent, is het minstens zo belangrijk om te bepalen welk proces in werking treedt na een aanval, als ieder uur telt. Hoe ziet het draaiboek eruit? Wie is waarvoor verantwoordelijk? Wat zijn de succes- en kritieke factoren? Pas als je het proces goed op orde hebt, kan techniek iets oplossen.'

Van voorkomen naar voorbereid zijn

Je voorbereiden kan klein beginnen, aldus Gijzel. 'Een uurtje met de directie om de tafel en bespreken wat cyberveiligheid voor jouw organisatie betekent, kan al winst betekenen. Mijn advies is: begin morgen en niet overmorgen. Een cyberaanval zit in een klein hoekje.'

Voorbereiding in 6 stappen

1. Creëer een team: verzamel intern en extern de belangrijkste stakeholders om tafel om na te gaan wie bij een cyberincident welke verantwoordelijkheid heeft en kan/wil nemen.
2. Creëer inzicht en adresseer risico's: welke systemen zijn er, welke data wordt waar bewaard en wie kan daar bij? Wat zijn de risico's en wat is kritiek voor de bedrijfscontinuïteit?
3. Bepaal de gevolgschade: wat zijn de gevolgen op korte en op lange termijn bij een cyberincident? Hoelang kunt u niet operationeel zijn? Wat is de impact op medewerkers, (keten)partners en imago?
4. Bepaal partners en expertise: welke expertise is er al in huis, welke expertise mist er nog en welke partners moet je op voorhand benaderen?
5. Bepaal rollen en scenario. Wie doet wat en wanneer? Wat is de besluitvorming? Werk pragmatisch uit hoe de organisatie van plan is om te handelen bij een cyberincident.
6. Zorg dat de basishygiëne op het gebied van security-maatregelen en interne informatievoorziening op orde is.

Arjan Aelmans, Enterprise Systems Engineer bij Fortinet

'Herinnert u zich de torens van opgestapelde containers in de Rotterdamse haven nog, toen de computers van Maersk vergrendeld werden door de malware NotPetya en de hele chain van vrachtverkeer piepend en krakend tot stilstand kwam? Indrukwekkende beelden die de hele wereld overgingen. En – recenter – weet u nog dat de kaas schappen van Albert Heijn dagenlang leeg bleven na een ransomware-aanval waardoor zo'n 250 vrachtwagens van het transportbedrijf geen kant meer op konden? De impact was zichtbaar en merkbaar voor het dagelijks winkelende publiek. Het zijn precies dit soort incidenten die er dankzij de omvang, grootsheid of juist alledaagsheid voor zorgen dat de publieke aandacht voor ransomware is gegroeid. De awareness groeit recht evenredig mee en dat is een goede zaak. Ik stam uit de tijd dat geld uitgeven aan cybersecurity gezien werd als het afsluiten van een brandverzekering: het werd pas relevant als je de ellende zelf een keer ervaren had.

Meer aandacht voor ransomware dus. Door het soort aanvallen, het publieke karakter ervan en de media die het steeds meer oppikken. Maar ook: meer aandacht doordat simpelweg het aantal gevallen toeneemt, vooral als we kijken naar bedrijven in de logistieke sector en just-in-time-delivery. En dát is natuurlijk allesbehalve positief. Ransomware is een waar verdienmodel geworden. Op het dark web is een aanval zó besteld. In landen als China, Rusland, Noord-Korea en Iran zijn gebouwen vol mensen 24/7 bezig met het opzetten, voorbereiden en uitvoeren van cyber attacks. Ze zijn uit op geld, hebben politieke motieven of opereren vaak als statelijke actoren om bijvoorbeeld kritische infrastructuur lam te leggen.

We horen onze klanten regelmatig zeggen: 'Bij mij valt niks te halen, mijn bedrijf maakt niks bijzonders'. Een misvatting. Er wordt door cybercriminelen hard gewerkt om kennis en data uit landen zoals dat van ons te verzamelen. Vooral toeleveranciers zijn populair: zij voelen zich minder bewust van hun kwetsbaarheid – ze maken immers maar een stukje van een eindproduct – en hebben hun security-zaakjes doorgaans minder goed op orde. In werkelijkheid zijn ze net zo kwetsbaar als degenen die een eindproduct maken; leg hen lam en je legt de eindproducent lam.

> 'Een goede aanpak is een verzameling van hardware, software, kennis en mensen'

Wat is er nodig? Detectie en preventie. Het is een misverstand om te denken dat het aanschaffen van één oplossing je vrijwaart van ransomware. Een goede anti-ransomware-aanpak is een verzameling van hardware, software, kennis, mensen en (micro)segmentatie van netwerk-infrastructuren. Je kunt je security en back-up policy prima op orde hebben en een stevige firewall bij de voordeur zetten, maar er hoeft maar één medewerker op een verkeerde link te klikken en hij of zij omzeilt alle maatregelen.

Door meerdere drempels na elkaar op te werpen, verklein je je kwetsbaarheid.

Wat nog veel belangrijker is, is dat de snelheid waarmee malware zich verspreidt vraagt om een minstens zo snelle aanpak. En dat past niet bepaald bij de traditionele zienswijze van veel bedrijven. Het beeld van 'er dringt iemand binnen, er gaat een alarm af en de beheerder gaat morgenvroeg eens even kijken wat er loos is' is nog te vaak realiteit maar past allang niet meer bij de cybercriminaliteit van tegenwoordig. De oplossing is het automatiseren van je security-aanpak. Zorgen dat je infrastructuur zelf direct ingrijpt op het moment dat er een aanval plaatsvindt en niet pas als de security officer zijn computer aanzet. En dat alle informatie rondom een lek of aanval verzameld en gedeeld wordt met het SOC. Alleen op deze manier ontstaat er een integrale aanpak die hout snijdt. Wij noemen dit een Security Fabric; technologie met een multi-layered benadering, die het gehele netwerk van een bedrijf segmenteert en beveiligt, van het Internet of Things tot de cloud. Ook externe oplossingen kunnen met de Fabric worden verbonden en informatie wordt uitgewisseld, waardoor de dekking binnen het netwerk verder wordt vergroot. De Fabric automatiseert detectie en preventie binnen het netwerk en rekent af met de risico's van endpoints.

Groeiende stapels containers, kaastekorten; we zullen dit soort 'fotogenieke' incidenten nog vaak terugzien in de media. Maar ik denk echt dat – als we slimmer drempels opwerpen en detectie en preventie niet alleen maar overlaten aan mensen maar ook aan technologie – we een vuist kunnen maken tegen die massa's cybercriminelen die nu soms wel héél makkelijk een weg naar binnen vinden.'

FORTINET

Tips van Arjan Aelmans:

- Is er geen budget voor een brede uitrol van EDR, zorg er dan in ieder geval voor dat je belangrijkste servers ermee zijn uitgerust.
- Spendeer je budget naast preventie en detectie ook aan recovery! Ja, dit kost tijd en geld maar juist het verloop van de recovery-fase heeft ontzettend veel impact op je business. Hoe langer deze fase duurt, hoe langer je uit de running bent, hoe langer je business stilligt. En tijd is geld.
- Zorg voor een respond-strategie met waterdichte back-ups. Veel getroffen bedrijven hebben een te makkelijk benaderbare back-up. Een goede back-up staat in de cold storage, blijft onbeschadigd tijdens een aanval en bespaart tijd bij de recovery na een ransomware-aanval.
- En design to fail: zorg ervoor dat - als het ergens misgaat – je weet wat je moet doen en wie je kunt bellen voor hulp. Als je nog offertes moet gaan opvragen, ligt je business onnodig lang stil.

Column

Peter Lahouse, cybercrime en dark web trendwatcher bij cybercrimeinfo.nl

'Om maar meteen met de deur in huis te vallen: ik maak me zorgen. In Nederland vinden we vrijheid heel belangrijk – of het nu gaat over onze nationale vrijheid of over alledaagse vrijheid ten tijde van een pandemie - maar we hebben het te weinig over digitale vrijheid. Op internet maken steeds meer grote, criminele spelers de dienst uit. Ze belemmeren ons om ons vrij en veilig te bewegen over het web. Ze persen ons af, bestelen en manipuleren ons.

Niet gek dat dit ze veelvuldig lukt: overheid, bedrijven en burgers zijn vaak te naïef. We zijn met zijn allen in hoge mate afhankelijk geworden van onze digitale infrastructuur maar zetten onze voordeuren te makkelijk wijd open. Maar liefst 80% van de hacks wordt veroorzaakt door iets simpels als een slecht wachtwoord!
De grootste bedreiging van dit moment is dus onze eigen onwetendheid. Wat is er nodig om het tij te keren? Om het belang van cybersecurity in de haarvaten van alle lagen van de overheid, van elke grote corporate en iedere mkb'er, van de politie en van elke burger te krijgen?

> 'De grootste bedreiging van dit moment is onze eigen onwetendheid'

We moeten ons allereerst beter bewust worden van de gevaren. Dat gaat alleen maar als we de gevaren en impact van cybercrime daadwerkelijk zien. Lastig, want deze vorm van criminaliteit is niet zo zichtbaar als andere vormen. Wordt er een pinautomaat leeggehaald, dan zie je vier

politiewagens met zwaailichten voorbijkomen. Voor een cyberaanval wordt de sirene niet aangezet. Je moet er dus bewust aandacht voor vragen. Dat kan bijvoorbeeld door het beestje bij de naam te noemen. Een hack is een cyberaanval, geen 'storing', zoals een getroffen bedrijf het in zijn externe communicatie vaak noemt.

Ten tweede moeten uiteraard de deuren dicht. Elk bedrijf - groot of klein -, iedere burger en elk overheidsorgaan moet zijn cybersecurity piekfijn op orde hebben. Met slimme wachtwoorden, gedegen beveiliging en de juiste experts op de juiste plek.

Daarna is het een kwestie van zorgen dat je klaar bent voor het moment dat het tóch verkeerd gaat. Oefenen dus, zoals we ook doen met een brandoefening. Ga tijdens zo'n oefening tot het gaatje: laat de monitor op de OK van een ziekenhuis ook écht uitvallen, dan wordt de impact tastbaar en vallen de kwartjes.

Het begint te komen. Heel geleidelijk begint het bewustzijn te groeien. Steeds vaker haalt een cyberaanval het nieuws. De overheid begrijpt steeds beter hoe belangrijk dit is. Bij de log4j-aanval kwam het nationale SOC - het NCSC - bij elkaar. Een goede zet: als je samenwerkt en krachten bundelt, kun je een vuist vormen en voorkom je dat iedere cybersecurity-partner het wiel zelf moet uitvinden.

We maken stappen. Maar criminelen maken grotere stappen. Zij kennen geen vertragende regels en taaie wetten. Werk aan de winkel dus, om ervoor te zorgen dat onze kleine stapjes grote sprongen worden.'

Fotografie: Marike van Pagee

Michel van Eeten, hoogleraar Governance of Cybersecurity (TU Delft)

Michel van Eeten is hoogleraar Governance of Cybersecurity aan de TU Delft en lid van de Cyber Security Raad, een adviesorgaan van de Nederlandse overheid. Hij ziet dat het verschil tussen ongericht en gericht aanvallen aan het vervagen is. En hij ergert zich. Want waarom doen we in Nederland niet meer met die gouden berg aan informatie over datalekken die nutteloos ligt te zijn in een kluis van de Autoriteit Persoonsgegevens?

'Tot een paar jaar geleden waren cyberaanvallen grofweg te verdelen in twee soorten: ongerichte aanvallen - ofwel het met hagel schieten en kijken waar je binnenkomt - en gerichte aanvallen – op heel specifieke doelwitten waarvan heel duidelijk was wat er te halen viel. Dat onderscheid is aan het vervagen. We zien steeds vaker de ultieme mix van de twee aanvalssoorten; aanvallers die vrij ongericht zoeken naar kwetsbaarheden bij random slachtoffers en hier vervolgens – eenmaal binnen – heel nauwkeurig en gericht te werk gaan.'

Bottleneck

'Het ongerichte gedeelte wordt steeds makkelijker. Onderzoek laat zien dat binnenkomen eigenlijk nagenoeg geen uitdaging meer is voor cybercriminelen. Ieder bedrijf, elke organisatie heeft kwetsbaarheden die te benutten zijn. De bottleneck zit 'm in de vraag hoe intensief het is om – eenmaal binnen - een bedrijf écht te raken. Het bereiken van de juiste systemen vereist tijd en geduld. Wil je je als organisatie anno 2022 wapenen tegen cybercrime, dan heeft het dus meer nut om te werken aan monitoring en respons dan aan predictie en preventie.'

> 'Nederland is wereldkampioen datalek melden maar doet niks met die waardevolle info'

Wikken en wegen

'Je netwerk segmenteren en scherp monitoren zijn belangrijke zaken waarmee je binnengekomen criminelen ontmoedigt. Hoe langer ze in je netwerk zitten, hoe groter de kans op ontdekking. Een crimineel zal dus een deurtje verder gaan als het allemaal te lang duurt of als hij merkt dat hij in de gaten wordt gehouden. Ze moeten wikken en wegen; wat is lucratief, zijn de risico's het waard? Cybercriminelen zijn eigenlijk nèt mensen.'

Game over

'Dankzij de steeds gerichtere en zorgvuldige aanpak wanneer criminelen de poort eenmaal

door zijn, worden steeds vaker IT-beheerders zelf slachtoffer van cyberaanvallen. Een zorgelijke trend want zij loggen in op allerlei systemen waar gebruikers ook komen. Hack een beheerder en je hebt kilo's bijvangst. Bovendien zijn met de credentials van IT-beheerders zelfs back-ups te benaderen. Game over. De klassieke fout die veel bedrijven maken – back-ups die hangen aan één en dezelfde IT'er – is koren op de molen van criminelen. Mijn advies? Richt verschillende soorten beheerdersrollen in en blijf deze zeer gedisciplineerd beheren. Delete rollen als iemand uit dienst gaat. En zorg dat niemand het ooit in zijn hoofd haalt om met dezelfde credentials in te loggen op een andere server.'

Nietszeggend taartdiagram

'De trends die ik noem, hebben impact op de groep bedrijven en organisaties die zich bevinden tussen heel kleine MKB'ers en grootbedrijven. Ongeacht sector, ongeacht product of dienstverlening. Dat zijn er dus gigantisch veel. We weten nog niet eens alles; lang niet alle aanvallen komen in de pers. En ondanks de meldplicht kiezen veel bedrijven er nog steeds voor om een aanval niet te melden. Toch is Nederland wereldkampioen datalek melden; we melden ongeveer 250 keer meer datalekken per hoofd van de bevolking dan de Verenigde Staten, waar de meldplicht al zo'n vijftien jaar bestaat. En dat brengt me op mijn grootste ergernis in de categorie 'aanpak van cybercrime': we dóen niks met al die meldingen! Ze worden in een grote kluis gestopt bij de Autoriteit Persoonsgegevens en een keer per jaar wordt er een nietszeggend taartdiagram over gepubliceerd. Punt. We zouden met deze gegevens zóveel meer kunnen.'

Weeffout in de wet

'Kijk naar de VS, waar data over lekken grotendeels openbaar gemaakt worden en er hele markten zijn ontstaan die organisaties diensten op maat bieden om hun cybersecurity op orde te maken. Dát is oplossingsgericht denken. In Nederland hebben we de slechtst denkbare combinatie; hoge administratieve lasten door al die meldingen maar geen enkel rendement op al die kostbare data. Het komt door een weeffout in de wet; daarin staat dat we meldingen vertrouwelijk moeten behandelen. En we vinden hier – heel behoudend – dat openbaar maken van deze data te veel reputatieschade zou veroorzaken. Maar in de Verenigde Staten blijkt dat die reputatieschade eigenlijk niet bestaat. Het is ronduit zonde om als samenleving miljoenen te spenderen aan het verzamelen van meldingen maar hier vervolgens niks mee te doen.'

Edwin Tump, Senior Analist Pinewood

Edwin Tump ziet vanuit het SOC van Pinewood dat ransomware-aanvallen steeds gerichter worden en dat de uitbuiting van kwetsbaarheden in systemen die op internet zijn aangesloten steviger zijn dan ooit. Drie vragen aan deze senior analist die ook tien jaar bij het NCSC werkte.

Welke trends in bedreigingen signaleer jij?
'Ransomware als trend lijkt een open deur en is niet nieuw maar toch zien we ontwikkelingen die het vermelden waard zijn. Waar aanvallers voorheen met hagel schoten, gaan ze gefaseerder te werk. Ze komen binnen, kijken rustig rond, prikken hier en daar wat en onderzoeken waar ze maximale schade kunnen berokkenen. Pas dan vallen ze echt aan.

Ik zie daarnaast ook de toename van uitbuiting van de kwetsbaarheden in systemen die op internet zijn aangesloten; firewalls, VPN-oplossingen, web servers, Citrix. Met als belangrijkste voorbeeld de recente Log4j-kwestie. Hierbij hoeft het systeem dat als eerste geraakt wordt zich niet eens binnen het bedrijf te bevinden dat slachtoffer wordt. Verderop in de keten kan het misgaan, terwijl de gevolgen van zo'n supply chain attack elders te merken zijn.'

Wat zijn de risico's van deze threats?
'Door de stap-voor-stap aanpak dringen criminelen door tot persoonlijkere of gevoeligere informatie, en is de kans groter dat hun slachtoffer geen andere uitweg ziet dan te betalen. Maar betalen is natuurlijk nooit een optie; je voedt er criminelen mee en bovendien is betalen geen garantie voor een oplossing. Wat je wel moet doen, is maatregelen treffen om voorbereid te zijn. Bijvoorbeeld door een draaiboek klaar te hebben liggen, regelmatig te oefenen en je aanvalsoppervlak te minimaliseren. Maar er zijn natuurlijk nog veel meer dingen die je kunt doen*. Het valt me overigens op dat bedrijven nog steeds moeite hebben met het in kaart brengen van de risico's. Het lukt ze niet om net zo inventief en adaptief te zijn als de cybercriminelen. Veel bedrijven zijn vooral gericht op preventie en niet in staat om goed mee te bewegen.'

> 'Losgeld betalen is nooit een optie, voorbereid zijn is altijd een must'

Wat is jullie antwoord op deze bedreigingen?
'In ons SOC passen we ons constant aan op trends in bedreigingen. We brengen tactieken van criminelen in kaart en richten daar onze detectie op in. Als een aanvaller in een netwerk zit, zal hij een reconnaissance doen, om zich heen kijken, een netwerkscan doen. Zo'n scan kunnen wij detecteren. Een ander voorbeeld: criminelen achter ransomware proberen altijd zoveel mogelijk rechten te krijgen. Ze gaan daarom op zoek naar accounts van beheerders en dat kunnen wij terugzien in de Active Directory. Je begrijpt dat we daar een specifiek alarm op hebben gezet. We zetten ook steeds meer in op threat intel. We verzamelen - geautomatiseerd - allerlei technische dreigingsinformatie en passen dit toe op de logging die we van onze klanten

krijgen. Het kan gaan om url's, ip-adressen of mailadressen waarvan bekend is dat ze voor aanvallen misbruikt zijn. Ook zijn we - speciaal voor onze zorgklanten - aangesloten op het landelijke ZorgDetectieNetwerk en op een van de channels van het NCSC. Via dit soort kanalen wisselen we waardevolle informatie uit met vakgenoten. Dankzij onze intelligence-inspanningen zitten we altijd bovenop de nieuwste ontwikkelingen en hebben we de knowledge om vervolgstappen zoals detectie nóg slimmer en effectiever in te richten.'

Tumps tips voor organisaties

1. Zorg voor een gelaagde beveiliging en vertrouw niet op één beveiliging.
2. Stel een goed patch-beleid op. Ga niet ad hoc dingen patchen maar breng de risico's in kaart en richt een plan voor structureel patchen in.
3. Besteed aandacht aan de hardening van je systemen; draai geen dingen die je niet nodig hebt. Hoe minder je gebruikt, hoe minder kwetsbaar je bent. Opschonen dus en verwijder functionaliteiten die je niet nodig hebt.
4. Leg een draaiboek klaar voor als het misgaat. En: oefen regelmatig!!
5. Zet in op detectie en werk minstens zo hard aan de awareness van je medewerkers.
6. Start vandaag nog met vulnerability scanning.
7. Minimaliseer je aanvalsoppervlak: hoe smaller, hoe minder kwetsbaar je bent.
8. Zorg voor goede en up-to-date backups. Als je bestanden versleuteld zijn, wil je kunnen terugvallen op recente onversleutelde kopieën daarvan. En heel belangrijk: vergeet niet je backups onbereikbaar te maken voor ransomware!
9. Segmenteer het netwerk. Maak het een aanvaller niet gemakkelijk om vanaf een geïnfecteerd systeem door te hoppen naar andere systemen binnen je netwerk.

Samenvatting

Ransomware als verdienmodel
Ramsomware staat prominent op de kaart, met steeds meer aanvallen. Cybercriminelen zijn professioneler dan ooit, beschouwen ransomware 'as a service' en zien een steeds grotere return on investment op hun activiteiten. Bekende namen in de logistieke sector en just-in-timedelivery, maar ook de zorgsector worden niet gespaard en dat vergroot het publieke karakter van deze digitale gijzelingen. Ransomware is een verdienmodel geworden waarmee een steeds grotere groep criminelen succesvol aan de slag gaat. Vrijwel alle geïnterviewden in dit rapport zijn eenduidig: preventie alleen is niet genoeg. Predictie-, detectie- en responsmaatregelen zijn essentieel. We moeten begrijpen hoe cybercriminelen werken en deze informatie gebruiken om onze gegevens te beveiligen. Door duidelijk te hebben uit welke fases een ransomware-aanval is opgebouwd en hoe je deze fases detecteert, kun je eenvoudig en vanuit de bestaande infrastructuur detectie opbouwen.

Ongerichte en gerichte aanvallen worden één
We zien steeds vaker een aanval waarin twee aanvalssoorten worden gecombineerd; aanvallers die vrij ongericht zoeken naar kwetsbaarheden bij random slachtoffers en hier vervolgens – eenmaal binnen – heel nauwkeurig en gericht te werk gaan. Binnenkomen wordt steeds eenvoudiger. De uitdaging zit 'm er tegenwoordig in om – eenmaal binnen – een slachtoffer zo hard mogelijk te raken. Wil je je als organisatie anno 2022 wapenen tegen cybercrime, dan heeft het dus meer nut om te werken aan monitoring en respons dan aan predictie en preventie.

Ketenaanvallen vergen ketenbeveiliging
De aanvalsstructuur van cybercrime is steeds beter georganiseerd. Er vinden meer en meer ketenaanvallen plaats, waarbij cybercriminelen ieder een stukje uit een langere aanvalsketen op zich nemen. Zo worden aanvallen ongrijpbaarder en criminelen steeds minder goed te traceren. Preventief beveiligen is niet meer genoeg; bedrijven en overheden moeten beter acteren en samenwerken op de gebieden predictie, detectie en respons zodat een ketenaanval in iedere fase kan worden gestopt. Maar dat lukt alleen als we het ook echt doén en daar ontbreekt het nog weleens aan. Zoals hoogleraar Michel van Eeten in dit rapport stelt: "Nederland is een kei in het melden van datalekken, maar zet de gouden berg aan informatie die uit deze meldplicht komt niet om in adequate preventie en detectie."

Toeleveranciers in de supply-chain een gewilde prooi
"Bij mij valt niks te halen, mijn bedrijf maakt niks bijzonders". Deze vlieger gaat niet meer op. Datacriminelen zijn drukdoende om kennis en data uit allerlei landen – en niet in de minste plaats Nederland – te verzamelen. Vooral toeleveranciers zijn een gewilde prooi; zij zijn zich maar beperkt bewust van hun kwetsbaarheid en hebben hun cybersecurity minder strak geregeld. Val hen aan en de impact is enorm. Ons advies is om koppelingen met leveranciers goed te borgen door bijvoorbeeld certificerings-eisen of een minimale set aan beveiligingsmaatregelen (en deze te testen!).

Externe leveranciers maken organisaties kwetsbaarder
Organisaties zijn in toenemende afhankelijk van externe softwareleveranciers, die Cloud- en andere services bieden. We zijn met zijn allen steeds afhankelijker van deze digitale infrastructuur. Tegelijkertijd anticiperen we te weinig op deze ontwikkeling. We zetten onze voordeuren te makkelijk open, wapenen ons niet voldoende tegen de risico's die externe

leveranciers met zich meebrengen. En criminelen? Die maken intussen gretig gebruik van generieke zwakten in systemen, waardoor ze met één druk op de knop een enorme hoeveelheid slachtoffers maken. Goede borging van security en maatregelen bij leveranciers is dus essentieel voor veiligheid.

De basis laat te wensen over

Ondanks dat grootschalige incidenten aan de orde van de dag zijn, is de basis bij veel organisaties niet op orde. Voor security experts een frustrerende bevinding. Deels heeft dat te maken met onwetendheid van gebruikers en deels met gebrek aan maatregelen. Zo zijn eenvoudig te raden wachtwoorden en niet gepatchte systemen nog aan de orde van de dag. Zorg dus dat de basis goed op orde is en er werk wordt gemaakt van bewustwording van de risico's. En oefen. Crisisoefeningen zijn essentieel voor de continuïteit van je organisatie. Zonder testen weet je niet wat je moet doen als er zich echt een ramp voordoet.

Cybersecurity is geen 'IT feestje''

Een cyberincident kan een groot bedrijfsrisico vormen. Nog al te vaak is cybersecurity een 'IT feestje'. Dat zou niet moeten. Het gaat om meer dan alleen techniek; ook bedrijfscultuur en -processen spelen een rol. Een duidelijke structuur met verantwoordelijkheden is broodnodig. Een structuur die wordt gedragen door de business en de bestuurders. Dat geldt ook voor de respons als het mis gaat. Responsmaatregelen verdienen een vaste plek in het bedrijfs-communicatieplan.

Toets de basishygiëne

Tot slot, maar zeker niet onbelangrijk: er zijn vele standaarden in securityland, denk aan NIST, ISO, NEN of CIS . Gebruik deze standaarden om je basiscyberhygiëne te toetsen. Als deze zaken op orde zijn, is de kans op een malware- of ransomware-besmetting kleiner en wordt het eenvoudiger om detectie op de gekozen maatregelen in te richten.

Het Cybersecurity Dreigingsbeeld en Adviesrapport NL 2022 is een uitgave van Pinewood.

Delftechpark 57
2628 XJ Delft
T 015 251 36 36
info@pinewood.nl
www.pinewood.nl

Redactie: ItsaRep en Pinewood
Vormgeving: BOS Reclame

pinewood