Drs. Vincent Hoek
Enterprise Architect (EA), I-Interimrijk.nl, onderdeel van de Uitvoeringsorganisatie Bedrijfsvoering Rijk

NOG NET NIET WAAR GEBEURD...

EERSTE HULP BIJ AURA-LEKKAGE

“Je aura lekt!” Ze zei het echt. De hele coupé luisterde licht geamuseerd naar hun gesprek. Zou je echt kunnen zien hoe het met de gezondheid van een organisme gaat, door uit te gaan van onzichtbare indicaties buiten het lichaam? Aura’s en vibraties zijn dan wel vaag, maar het is een feit dat honden ziekte bij mensen kunnen ruiken. Je immuunsysteem dat ziekte bestrijdt zich uit in chemische veranderingen die leiden tot de uitstoot van andere geurmoleculen.

Je kunt het horen als je auto of wasmachine begint te overlijden, dankzij verontrustende geluidjes of een weeë rubbergeur. Nog voor de vonken in je datacentrum in het rond vliegen, waarschuwen feromoonsensoren zodra de moleculen van isolatiemateriaal worden gemeten. Websites scannen ongewild wat voor computer en welke software versies jij gebruikt. Er bestaan algoritmen die sensorinformatie van het geluid van passerende treinen vergelijken met een databank, zodat je met een griezelige precisie kunt voorspellen welk reserve-onderdeel je maar het best alvast in huis kunt halen. Digitale aura’s lekken wel degelijk!

De westelijke wereld functioneert tegenwoordig bij de gratie van real-time datastromen. Die datastromen maken deel uit van grensoverschrijdende, samenwerkende ecosystemen van bedrijven en sociale relaties tussen mensen en machines. Steeds meer producten zijn daardoor cybernetisch verbonden multipurpose producten geworden.

Na de eerste industriële revolutie van stoom, doorliep onze samenleving een tweede industriële revolutie van elektriciteit en daarna een derde industriële revolutie van communicatie, waarin mensen, machines en mediabeelden elkaar op gingen roepen. Dit leidde binnen één generatie tot een vierde industriële revolutie ‘of Things’, waarin meer apparaten onderling digitaal ‘praten’ dan mensen. Vandaag staat onze samenleving aan het begin van een vijfde industriële revolutie. Konden we de vierde industriële revolutie nog beschouwen als een voortbouwen op de digitale com-

municatie revolutie, gekenmerkt door de vervaging van de grenzen tussen de fysieke, de digitale en de biologische wereld; de vijfde industriële revolutie gaat veel verder. Onze samenleving kan de borst nat maken voor robotisering en automatisering (kantelpunt volgens het World Economic Forum in 2021), het Internet of Anything (IoX), het Wearable Internet (denk aan Augmented en Mixed Reality 'brillen'), 3D/4D printing and manufacturing (kantelpunt in 2022); supercomputers in de broekzak (kantelpunt 2023); bestuurderloze voertuigen (kantelpunt 2026) en nog wat kleinigheden rondom blockchain, nanotechnologie, genetisch onderzoek en quantum computing. Het fysieke wordt informatie in de vorm van cybernetische logica; de realiteit van onze voorouders versmelt met een computerspelletje. Dit vraagt om een aanpassing aan de manier waarop we risico's beheersen. Niet achteraf checken, maar vooraf doordenken. Niet van buiten naar binnen beschermen, zoals een harnas, een slotgracht, een firewall of een Intrusion Detection System, maar van binnen naar buiten beschermen, zoals een immuunsysteem. Niet risico's mitigeren, maar managen. Niet afzonderlijke apparaten en systemen 'applicatiecentrisch' beveiligen, maar niet naïef meer zijn over 'supply chain' attacks die juist inspelen op de digitale relaties.

'Risk-based security' is daarom een term die steeds vaker gebruikt wordt. Een risk-based cybersecurity-aanpak betekent dat bedrijven bij het maken van security-beslissingen 'risico' als belangrijkste factor beschouwen. Een risk-based aanpak wordt vaak neergezet als het tegenovergestelde van een compliance-gedreven aanpak. Risk-based security-teams richten zich vooral op het verminderen van de daadwerkelijke blootstelling aan cyberaanvallen en datalekken. Zij richten zich niet zozeer op het afvinken van compliance spreadsheets en het behalen van audits. Hoewel belangrijk, toch een vorm van check-in-the-box zelfhypnose.
Een risk-based aanpak is proactief en

kijkt naar het hele ecosysteem waar de organisatie op draait: de assets, de resources, de sociale en digitale relaties. Als jouw organisatie een schip is, dan is het internet het water. Jouw mensen bellen (VoiP), mailen, bezoeken websites en jouw software en sensoren wisselen data uit. Externen met mobiele devices lopen in en om jouw gebouwen, appen, bevragen en besnuffelen de softwarediensten van jou, je toeleveranciers en afnemers. In plaats van zich te richten op incident response, investeert een CIO die de Risk-Based Security aanpak hanteert daarom veel meer in testen, threat intelligence en preventie. Net zoals een immuunsysteem plakt hij geen pleisters meer als het fout gaat, maar is hij realistisch dat risico's hooguit te reduceren zijn en dan nog alleen als je ze tijdig onderkent.

Honderd procent veiligheid is niet te realiseren en hij wil pragmatisch kunnen beslissen over budget en resources. Bij 100% security drive worden geen kosten bespaard, ook niet wanneer investeringen minder opleveren. Een security-programma dat uitgaat van een risk-based aanpak levert daarentegen meer op dan veiligheid, namelijk ook een strak (licentie)portfolio. Dit komt door het vervangen van compliance checklists door continue monitoring. De CISO wil tenslotte een gedegen kennis van risico's hebben en risico inschatting moet worden gebaseerd op feiten in plaats van meningen, trends en krantenkoppen. Dankzij de datificerende samenleving kan IT-security plaatsvinden op basis van actuele data. Continue monitoring is hierbij essentieel. Aangezien blinde vlekken funest zijn voor deze aanpak, moeten kwetsbaarheidsbeoordelingen en penetratietesten, die normaal twee keer per jaar plaatsvinden, worden aangevuld met andere soorten beoordelingen. Security-ratings bijvoorbeeld. Ratings bieden inzicht in gecompromitteerde systemen, configuratie-processen, gebruikersgedrag en andere factoren die bijdragen aan risico's. Deze inzichten worden gebundeld in beoordelingen voor individuele risico-vectoren en uiteindelijk samengevat in één cijfer dat dagelijks wordt geüpdatet en wordt gerapporteerd aan de verantwoordelijken. Hierdoor kan prioritering plaats vinden. Proactief. Als je hond je vreemd aan begint te kijken, moet je toch misschien eens naar de dokter.

Risk-based cybersecurity omvat een systeem dat security-behoeften prioriteert op basis van gepercipieerde blootstelling aan actuele risico's. Effectieve prioritering vraagt daarom twee zaken: kennis van de dreiging en kennis van het target.

De traditionele CISO bewaakt het auditeerbaar houden van zijn compliance. De moderne CISO is een teamspeler die samen met zijn CIO Office voortdurend op de hoogte moet zijn van de laatste en belangrijkste cyberdreigingen voor hun organisatie, sector en regio. Een actueel kennisniveau dat menselijkerwijs niet te verwachten is in het hoofd van één functionaris (de CISO), maar wel in een geautomatiseerd wereldwijd netwerk. Net zoals een viruskiller elke paar seconden wordt opgewaardeerd met de laatste mogelijkheden, kun je op afstand specifieke vragen pingen of bijvoorbeeld een patch achterhaald is. Het is vervolgens aan de CISO om te weten welke systemen en data kwetsbaar zijn voor de dreigingen waarvoor het Systeem hem waarschuwt, zoals het aan de besnuffelde persoon is om vervolgstappen richting arts te nemen. Zo kan hij/zij op elk moment bepalen welke projecten de meeste resources vereisen en met zekerheid zeggen dat bijvoorbeeld het pauzeren van de implementatie van software voor geautomatiseerd incidentenbeheer ten behoeve van het updaten van gebruikersgegevens het risico op blootstelling van de organisatie op dat moment verkleint. Prioriteren zelf moet ook dynamisch en kort-cyclisch zijn.

Niet langer (drie)maandelijks, maar doorlopend. Het dynamisch complexe risicolandschap muteert zich daar te snel voor. Tools voor continue monitoring, zoals security ratings, zijn daarom van groot belang geworden voor het bepalen van prioriteiten. Naast continue risicomonitoring, kunnen cyberrisico's pas echt begrepen worden als niet meer alleen naar de eigen organisatie wordt gekeken. Risico is relatief en vereist daarom de context van historische prestaties en de prestaties van collega's, concurrenten en sectoren. Of jij ziek bent kan je hond alleen ruiken als hij weet waar hij op moet letten.

Security ratings worden gebaseerd op openbare informatie, waardoor elk bedrijf kan worden beoordeeld en niet alleen jouw eigen organisatie.

Zo wordt inzicht verkregen in de security-prestaties van concurrenten; in bovengemiddeld presterende organisaties en in de algemene stand van zaken in een sector. Cybersecurity benchmarking geeft security-professionals de benodigde context om te bepalen hoe zij er zelf voor staan. Het is ook mogelijk om te kijken naar een specifieke organisatie, om zo een beeld te krijgen welke security-onderdelen bij die club de meeste aandacht krijgen. Moderne verzekeraars krijgen zo gevoel voor de kwaliteit van een nieuwe klant en daarmee voor het te verzekeren risico. Investeerders krijgen een indicatie voor de gevoeligheid voor datalekkage van

"Cybersecurity benchmarking geeft security-professionals de benodigde context om te bepalen hoe zij er zelf voor staan."

hun acquisitie target en daarmee voor de kwetsbaarheid van het intellectueel eigendom. Vergeleken met compliance-gedreven organisaties bespaart een organisatie met een risk-based aanpak veel tijd en geld. Niet alleen kunnen de cybersecurityproducten die zij al hebben, zoals SIEMs, veel strakker worden geconfigureerd; zij hoeven ook geen geld meer uit te geven aan overtollige tools en systemen die feitelijk niets opleveren, of die de organisatie onbewust bloot stellen aan risico's bij derden. Een risk-based aanpak vermindert de noodzaak voor dure security-consultants en grootschalige assessments. Het portfolio-inzicht wordt beter en gebruiksprocessen worden veel helderder gerelateerd aan specifieke datastromen, waardoor de kansen op datalekken verminderen. Dit alles maakt het verschil tussen winst en faillissement; tussen vertrouwen en imagoverlies. Als je aura lekt, kun je het maar beter weten.