VIER MANIEREN OM SECURITY-RESULTAAT TE VERKNALLEN!

In de aanloop naar het Oud en Nieuw vuurwerk 2018 noem ik vier manieren om security-resultaat te verknallen:

1. **Onderschat de aanvalskracht van je tegenstander.**
2. **Overschat de kracht van je eigen verdediging.**
3. **Denk te makkelijk over security als vak.**
4. **Doe te moeilijk richting je security-personeel.**

Bij elke manier doe ik een suggestie voor een "goed voornemen" voor het komende jaar 2019 (en verder natuurlijk).

1. Onderschat de aanvalskracht van de tegenstander

De cybercriminelen hebben als aanvallers hun duistere zaakjes beter georganiseerd dan de verdedigers aan de security-kant. De boeven werken onderling meer samen, ook wereldwijd, en hebben meer en betere kennis die ze vaker met elkaar delen. Gratis of in ruil weggeven via dark web fora, of zelfs verkopen aan elkaar via CAAS (Crime As A Service). Er wordt ook verkocht aan of geruild met zeer ruimdenkende veiligheidsdiensten van nation states (black hat hacking as a service). Als je vandaag als security-specialist denkt: "Deze encryptie is weliswaar te kraken, maar alleen door veiligheidsdiensten en daarvan hebben we niets te vrezen", dan sus je jezelf in slaap. Want die kraaktechniek is morgen – of hooguit overmorgen – ook beschikbaar voor criminelen. Geheime diensten passen overigens ook steeds vaker technieken toe die eerder alleen door criminelen werden gebruikt.
En hackingtechnieken uit andere landen of continenten zijn veel gemakkelijker te exporteren en elders te implementeren dan security-maatregelen. De criminelen voelen zich immers in hun werkwijze, organisatie en informatie-uitwisseling niet gehinderd door zoiets als privacy-wetgeving. En doordat criminele bendes het begrip 'deadline' soms letterlijk toepassen, motiveert dit hun betaalde (of gedwongen) leveranciers in hevige mate om de toegezegde deliverables op tijd en binnen alle verwachte kwaliteitseisen op te leveren. Verder zijn aan de misdaadkant de beschikbare budgetten in het algemeen hoog, want voor de aanvallers is een zwakke security bij hun tegenstander een bron van opbrengsten. Hun investering in een aanval levert vrijwel zeker meer geld op. De cybercriminelen hadden het in eerste instantie gemunt op bijvoorbeeld banken om daar geld te stelen, als in een digitale bankroof. Maar via inzet van ransomware worden door middel van chantage of afpersing ook andere bedrijven, organisaties of zelfs particulieren slachtoffer. Via phishing-mails of misbruik van websites voor dating en vacatures worden met behulp van social engineering mensen overgehaald om 'vrijwillig' geld over te boeken aan de criminelen. Oplichting dus. En ook afdelingen die gewend zijn aan uitbetalen, zoals salarisadministraties en crediteurenafdelingen, zijn in elke organisatie een (theoretisch) interessant doelwit omdat ze nu eenmaal een uitgaande geldstroom hebben. Door de grote en groeiende groep aanvallers, die onderling samenwerken, groeit het risico voor een organisatie, zeker als die slechts beducht is voor één aanvallersoort.

Advies: *probeer voortdurend de TTP (tools, techniques, procedures) van de groep tegenstanders zo goed mogelijk in kaart te brengen en wapen je daartegen.*

2. Overschat je eigen verdedigingskracht

"Ken de vijand en ken uzelf, en u kunt 100 slagen vechten zonder nederlaag", zei Sun Tzu en hij kon het weten, want hij was een succesvolle Chinese militaire strateeg. Het gaat er dus niet alleen om threat intelligence (inlichtingen) over de vijand te hebben, maar ook informatie over jezelf en je eigen verdediging is noodzakelijk om de oorlog niet te verliezen. En die informatie moet volledig en juist zijn. Helaas schort het daar in security-land een enkele keer aan. Je weet dan niet alle zaken die je eigenlijk wel zou moeten weten, en wat je wel 'weet', is niet altijd juist. Thuis heb ik onder andere twee Windows 10 computers en eentje met Windows 7 die vrijwel de hele maand ongebruikt en uitgeschakeld in de kast staan. Elke maand ben ik op Patch Tuesday een groot deel van de dag (weliswaar naast andere activiteiten) bezig met het downloaden en installeren van patches en tussendoor

Robert Metsemakers is als ervaren IT auditor en informatiebeveiliging expert beschikbaar voor security advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

opnieuw starten van die computers. Aan het eind van zo'n dinsdag kan ik dan wel naar waarheid zeggen: "mijn machinepark is 100% gepatcht en up-to-date". Maar als je in je organisatie 400, 4.000 of nog meer machines hebt, krijg je dat natuurlijk niet in één dag af. En dan is het, op een moment dat malware zoals Petya (klinkt als 'patched', want voor de daar misbruikte kwetsbaarheid was al lang een patch beschikbaar) uitbreekt, jammer genoeg niet meteen duidelijk hoeveel nog-niet-gepatchte machines in je organisatie in potentie gevaar lopen. Bovendien, als je heel veel machines in gebruik hebt, zijn er altijd wel bijzondere projecten zoals pilots, waarin de betreffende gebruikers reeds Windows 10 hebben, terwijl de rest van de organisatie nog op Windows 8 zit. Of dat op een klein aantal servers Windows XP 'moet' blijven draaien vanwege bepaalde onmisbare legacy-software die alleen op dat oudere operating system werkt. Of de organisatie staat toe dat gebruikers hun eigen telefoon of tablet mogen gebruiken om bedrijfsinformatie te benaderen, maar het is lastig af te dwingen dat ze die eigen machines voortdurend bijwerken met (security) patches. Wanneer ze het niet bijhouden, kun je dat weliswaar bij het verbinden zien en hen daarom de toegang tot die data ontzeggen. Maar dan kunnen ze hun werk niet doen en geef je als werkgever nutteloos hun salaris weg. Je hebt daarom bij een groter machinepark misschien wel vier of vijf verschillende patch-percentages tegelijk nodig, namelijk voor elke omgeving of netwerkdeel apart. Ze zullen trouwens waarschijnlijk ook nog onderling verschillen en elk in een ander tempo veranderen.

Je weet met andere woorden als aangevallen of – als collatoral damage – kwetsbare partij in de meeste gevallen niet volledig over je eigen situatie wat je eigenlijk wel zou moeten weten voor een totaalbeeld. En dat totaalbeeld is nodig om de juiste tegenacties te bepalen en in die verzameling vervolgens hun onderlinge prioriteit en volgorde als verdedigingsmaatregelen te bepalen. Bijvoorbeeld: wat is het patch-niveau van software op onze werkplekken, op de servers, op de laptops en op de BYOD-apparaten die in eigen beheer van de medewerkers zijn? Deels is dit een probleem van alle tijden, want je kunt nu eenmaal niet alles weten. Of: het is te duur om alle denkbare informatie te registreren en verzamelen, dus wordt er een keuze gemaakt.

'Meten is weten', maar aan de andere kant: je krijgt (alleen) wat je meet! Zeker wanneer je het meten beperkt tot enkele KPI's (Key Performance Indicator). De mens is nu eenmaal een economisch wezen en streeft dus naar maximalisatie van de opbrengst bij een bepaalde inspanning, of naar minimalisatie van de inspanning om het vooraf bepaalde doel te bereiken. Dit economische uitgangspunt gebruiken veel mensen die geld willen verdienen bij het bedenken wat ze nou vandaag weer eens zullen gaan doen op het werk. Als je de beloning voor je medewerkers bijvoorbeeld afhankelijk maakt van het aantal in een periode opgeloste IT audit issues, is er een tendens om veel kleine issues op de actielijst te plaatsen. Waarvan dan een hoog percentage in korte tijd wordt opgelost. Wordt men aan de andere kant afgerekend op een laag aantal openstaande IT audit issues aan het eind van een periode, is de neiging juist om een beperkt aantal grote issues te formuleren. Die dan vaak bestaan uit meerdere onderling afhankelijke issues, welke uit de aard der zaak slechts zeer langzaam (of zelfs nooit) volledig worden opgelost.

Sinds mijn eerste college Administratieve Organisatie, waar het ook ging over de zojuist genoemde (menselijke) tendensen, ben ik daarom een enthousiast voorstander van functiescheiding. Dat wil zeggen dat degene die registreert wat de status van bijvoorbeeld het patchen is, een andere persoon is dan degene die verantwoordelijk is voor het uitvoeren van de activiteit (het patchen zelf). Functiescheiding verbetert de betrouwbaarheid van de gerapporteerde gegevens. Organisaties die – om wat voor reden dan ook – meerdere taken bij één functionaris beleggen, lopen een risico dat die persoon de bereikte status of uitgevoerde activiteiten te rooskleurig (of op een andere manier foutief) presenteert. Ik heb het hier natuurlijk niet over uw organisatie beste lezer, maar bedoel alle andere bedrijven en organisaties in de wereld.

Een te sterke focus op slechts een beperkt aantal KPI's kan er naar mijn mening toe leiden dat de andere zaken onvoldoende aandacht krijgen van de medewerkers. Daardoor kan de informatie over de verdedigingskracht onvolledig zijn. Op het marineschip is dan het dek blinkend gepoetst en de ankerketting is voortreffelijk opgerold, zodat niemand erover kan struikelen. Het vaartuig is op tijd feestelijk gepavoiseerd (= met seinvlaggen versierd), maar onderdeks is er van alles loos omdat de bemanning daar niet óók nog tijd en aandacht aan heeft besteed.

Wanneer een organisatie zoals dat in georganiseerde bendes gebeurt (zie paragraaf 1) heel letterlijk 'afrekent' met onvoldoende presteerders door ze met veel spektakel uit de organisatie te verwijderen, versterkt dit de tendens van 'zaken te rooskleurig weergeven'. Naar mijn idee is dit ingebakken in het menselijke DNA en wordt dit ongewenste gedrag onder druk alleen maar erger. Daar waar je dus in de meeste gevallen onvolledig bent in alle informatie die je over je eigen situatie zou moeten hebben voor een goede verdediging, is dan wat je wel meet helaas ook nog eens onjuist voorgesteld. Vaak te positief, al helpt het principe van functiescheiding tussen beschikken, uitvoeren, bewaren, registreren en controleren overigens óók bij het vermijden van een te negatieve weergave, zoals dat optreedt bij zwart geld betalingen of een 'zaak-in-de-zaak'. Als voorbeeld: een barkeeper

Security als vak is moeilijker dan je denkt en dat geldt op strategisch, tactisch en operationeel niveau

brengt een zelfgekochte fles whisky mee naar zijn werk, die hij per glas voor normale prijzen verkoopt aan uw klanten – terwijl ze genieten van de barkrukken, toog, muziek, verlichting en verwarming die u als café-eigenaar heeft betaald – en steekt daarbij de opbrengst in eigen zak. Die omzet had u liever zelf in de boeken gehad!

Advies: *laat de kwaliteit van de eigen verdediging breed, frequent en door onafhankelijke personen meten om zo volledig en juist mogelijk te zijn.*

3. Denk te gemakkelijk over het vakgebied security

Security als vak is moeilijker dan je denkt en dat geldt op strategisch, tactisch en operationeel niveau.
Op strategisch niveau noemt de Amerikaanse security specialist Dan Geer in zijn lezingen security het moeilijkste vak ter wereld, terwijl men meestal rocket science en hersenchirurgie als bijzonder moeilijk en ingewikkeld ziet. Maar daar zijn de te behandelen onderwerpen al miljoenen of honderdduizenden jaren hetzelfde! De zon heeft er verder geen financieel belang bij om de onderzoeker voor de gek te houden. De natuurwetten gaan zich niet anders gedragen doordat een wetenschapper er naar kijkt. Een patiënt kan niet snel zijn bloedgroep veranderen terwijl er bij hem/haar een bloedproef wordt genomen. Een cybercrimineel kan dat allemaal wel en heeft er ook een groot belang bij, omdat hij/zij wil doorgaan met de illegale activiteiten. Een patiënt wil snel genezen. De ontwikkelingen in de IT gaan bovendien vele malen sneller dan de ontwikkelingen in het heelal (een nieuwe planeet of ster is er niet zomaar 1-2-3) of in het menselijk lichaam. Security moet als vakgebied dus veel sneller mee ontwikkelen met die IT dan dat chirurgen moeten meebewegen met ontwikkelingen in de menselijke hersenen.
Tactisch niveau zie ik als het vertalen van het security-beleid naar concrete maatregelen en projecten. Daarbij is het lastig dat veel security-beleid, vanwege de eraan verbonden risico's, bepaalde handelingen of gedrag compleet verbiedt of ze alleen toestaat onder strenge, beperkende voorwaarden. Geen onversleutelde USB-stick of webmail gebruiken om vertrouwelijke bedrijfsinformatie het pand uit te krijgen. Parkeren van meegebrachte auto's alleen in de op de grond geschilderde parkeervakken. Roken mag, maar alleen buiten en het telt niet als arbeidstijd. Op zich zijn dat begrijpelijke, duidelijke en te verdedigen voorschriften, maar het is toch goed om periodiek te controleren of de medewerkers zich er inderdaad aan houden. Of tenminste, welk percentage van de medewerkers dat wel doet! Dat blijkt in de praktijk nog best veel (extra) werk, zo precies bijhouden hoeveel medewerkers zich aan de redelijke afspraken houden…
Een ander voorbeeld: toegang verlenen tot een mobiele app met een wachtwoord (dus zonder tweede factor zoals een token) mag, maar alleen als dat wachtwoord, door de lengte en ingewikkeldheid ervan, voldoende moeilijk via een brute force aanval te raden is. Dit terwijl de business juist vraagt om een gemakkelijke oplossing. Ja, ze weten nu wel dat cloudgebruik security-risico's in zich draagt, maar ze willen die 'computer van iemand anders' toch gebruiken, soms zelfs als 'shadow IT'dus geheel buiten het medeweten of de bemoeienis van de IT-afdeling om. Ze zijn wel bereid om klanten een wachtwoord te laten gebruiken, maar dan wel een simpele. Eentje van vier cijfers en de klant hoeft deze slechts één keer per jaar te veranderen en mag deze ook op 9999 zetten en een minuut later weer de oude code instellen. Toegegeven: niet alle gebruikers zoeken zo de rand en de mazen van het security-beleidsnet op, maar sommige helaas wel en daar ben je dan de hele dag mooi druk mee als security officer annex business-enabler.
Op operationeel niveau is security moeilijk omdat de verdediger nu eenmaal altijd in het nadeel is. Per definitie kan hij/zij alleen reageren op het initiatief (de aanval) van de aanvaller. De verdediger moet in de spreekwoordelijke voetbalwedstrijd voortdurend waakzaam zijn en de aanvaller hoeft slechts kort te pieken. Want in één qua aandacht gemiste minuut kan de verdediger (zoals een keeper) de voetbalwedstrijd verliezen, en een aanvaller (zoals de spits van de tegenpartij) kan in slechts één geslaagde minuut de voetbalwedstrijd winnen. Verder is de operationele laag veel breder en er zijn dus meer mensen betrokken dan in de strategische en tactische laag. Dus moeten er ook meer mensen gemotiveerd en gestimuleerd worden om tot gedragsverandering te komen. In veel organisaties is het zo, heb ik gehoord en gelezen, dat een beperkt deel van de medewerkers security héél belangrijk en interessant vinden: de leden van die groep werken allemaal op de afdeling Security. Dan is er een groep medewerkers die security ook tamelijk belangrijk en

Men kan ze 'nerds' noemen en dat vinden ze niet eens een scheldnaam

interessant vinden: dit zijn de personen die erover praten bij de koffie-automaat en die met mails en posts op intranet reageren op de security awareness posters gericht op infomatiebeveiligingsbewustzijnsverhoging (te lang voor Scrabble). En dan is er nog een grote groep medewerkers die security juist onbelangrijk vindt, die er mogelijk zelfs een hekel aan heeft en nog belangrijker, er nauwelijks iets aan doet. Dit maakt het inherent moeilijk om de door de kleine groep 1 bedachte maatregelen door de grote groep 3 uitgevoerd te krijgen. Hoe goed groep 2 als 'leading coalition' daarbij ook meehelpt door het geven van positief commentaar of hoe welwillend zij de security-acties 'gedoogt' door juist geen negatief commentaar te geven.
Naarmate security stap voor stap, van beleid via maatregelen naar concrete acties, de operationele laag bereikt, wordt het dus veel meer werk en dat maakt het ook moeilijker uit te voeren. Denk aan wat je na een (bijvoorbeeld CISSP) examen zegt: "Het was niet moeilijk, maar vooral véél". Ook dijt het werkveld nog steeds uit. De oude security-risico's gaan niet weg en behoeven nog steeds tijd en aandacht. Zoals 'social engineering', gericht op het hacken van de mens als zwakste schakel in de totale security-keten. Of 'dumpster diving', gericht op het door de aanvaller verzamelen van onnadenkend door medewerkers weggegooide maar nog steeds leesbare informatie. Maar er komen wel steeds nieuwe risico's en nieuwe soorten en nieuwe voorbeelden van bestaande soorten malware bij, die allemaal óók aangepakt zullen moeten worden. Het speelveld wordt dus steeds breder. En de security-professional die de mogelijke risico's van nieuwe activiteiten in kaart moet brengen, heeft daarmee een steeds langere lijst van zaken die in het verleden al zijn gebeurd, in de eigen organisatie of elders, om uit te kiezen en dus aan te vinken op de security-checklist. Zodat het speelveld ook langer wordt. Met – in veel organisaties – een gelijkblijvend of zelfs dalend aantal spelers in het team dat het spel moet spelen.

Advies: *bedenk bij het vaststellen van plannen, ambities en doelen in security dat Keulen en Aken ook niet in één dag zijn gebouwd.*

4. Doe te moeilijk richting je security-personeel

Managen van personeel vraagt altijd tijd en aandacht. Echter, het managen van security-personeel is misschien wel moeilijker dan van 'gewoon'(u snapt wat ik bedoel) personeel. Goed security-personeel binnenhalen en tevreden houden is lastig.

In de groep IT-personeel zie ik meer introverten of autisten dan op andere afdelingen. Ook meer hoogbegaafden (Bill Gates, Steve Jobs), met bijzondere hobby's (bergbeklimmen en dat als Nederlander!), afwijkende favoriete muzieksoorten (schlagers, hardrock), excentrieke kledingstijlen (zwarte T-shirts, vaak met prikkelende teksten) en opvallende haardrachten (schouderlang, dreadlocks of ingeschoren Mickey Mouse figuren). Bij security-afdelingen is dat percentage soms zelfs nog hoger dan op andere IT-afdelingen. Men kan ze 'nerds' noemen en dat vinden ze niet eens een scheldnaam. Ze werken met passie in een voor de buitenwereld onduidelijk en vaak ook oninteressant werkgebied. Onder voortdurende tijdsdruk, altijd reagerend op onverwachte aanvallen, datalekken, responsible disclosure meldingen, bedieningsfouten van andere medewerkers en achteraf ontdekte fouten in software die met grote spoed, maar wel foutloos moeten worden gepatcht (zie paragraaf 2).
Voor zover security-specialisten (of generalisten) niet al vanaf de wieg 'anders' zijn, beïnvloeden deze omstandigheden op den duur hun manier van werken. Met andere woorden: deze 'nerds' moeten op een andere manier gemanaged worden, dat vergt maatwerk en is dus tijdrovend voor leidinggevers. 'Micromanagement', zoals het zeer strikt laten naleven van 'regeltjes' waarvan het nut door de nerds in twijfel wordt getrokken, werkt hier vaak averechts. In het algemeen zijn het gemotiveerde professionals, met een passie (of zelfs roeping) voor het vak, die vanuit zichzelf hun werk zo goed mogelijk willen doen, aldus Mathieu Weggeman, die zijn interessante managementboek samenvat in de titel.

Advies: l*ees daarom, als leidinggevende of leidingontvanger, Mathieu Weggeman - "Leidinggeven aan professionals? Niet doen!".*