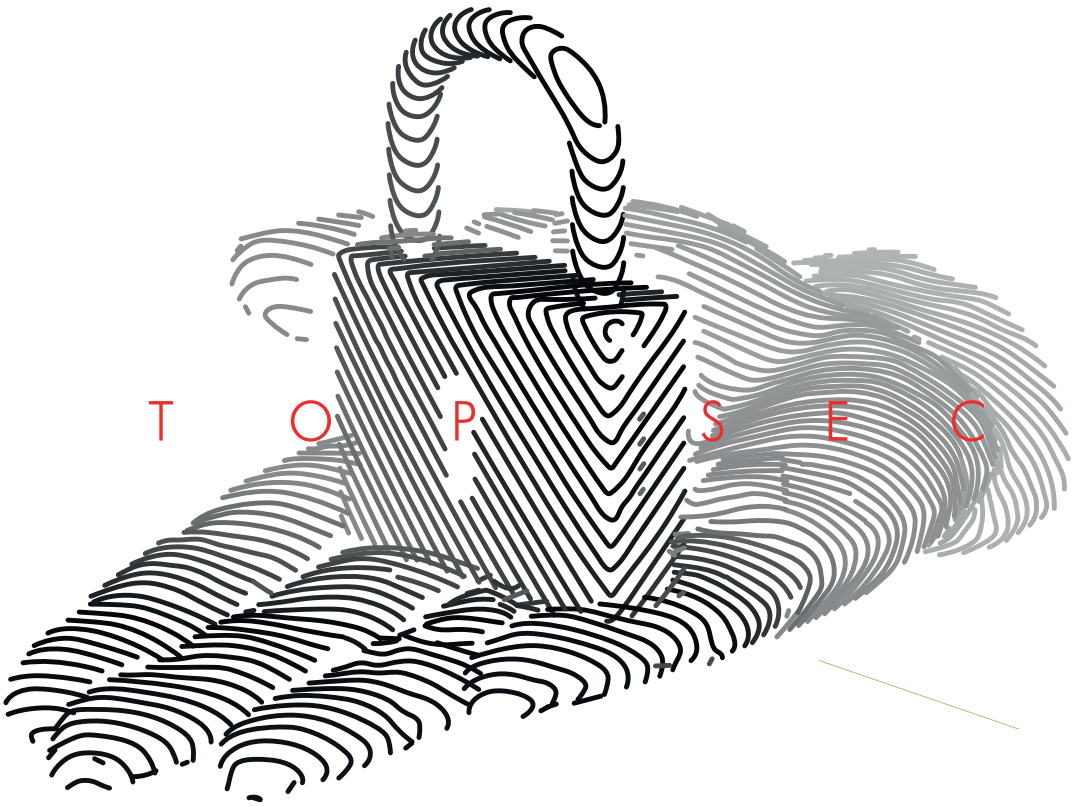
INFORMATIEBEVEILIGING
MAGAZINE



T O P S E C R E T

- Interview Martijn Jonk: is het NCSC er ook voor niet-vitale organisaties?
- Zie dataprivacybescherming als kans in plaats van verplichting
- Column: SyRi dood? Welnee, het heet nu alleen anders

JAARGANG 21 - 2021 - EDITIE 4

In de prijzen

Nicole van Deursen

De artikelen in iB-magazine worden geschreven door en voor PvIB-leden en de auteurs steken daar veel tijd en energie in. Het is dan ook ieder jaar weer leuk dat een onafhankelijke jury, buiten de ogen en oren van de redactie, het beste artikel uit iB-magazine kiest. De top 4 auteurs en de winnaar van 'Artikel van het jaar' worden op pagina 32 in het zonnetje gezet! Proficiat aan de winnaars en namens iedereen veel dank aan alle auteurs.

In deze uitgave legt TNO uit waar het Europese innovatieproject SOCCRATES aan werkt. In dit consortium ontwikkelt men een platform voor het automatisch detecteren, analyseren en reageren op dreigingen, aanvallen, kwetsbaarheden, changes en nieuwe systemen. Totdat zo'n alles-in-een-platform bestaat moeten we ons werk nog doen met mensen en met de informatie die we krijgen uit onze bestaande professionele groepen voor informatiedeling. In het interview met het NCSC wordt daarom ingegaan op de bestaande en toekomstige mogelijkheden voor het delen van dreigingsinformatie met vitale en niet-vitale organisaties. Maar ons eigen magazine is ook een goede bron voor waarschuwingen en handelingsperspectief. We kunnen bijvoorbeeld leren hoe we onze website kunnen beschermen tegen java-script aanvallen door derden (p. 8) of hoe we access management kunnen inrichten (p. 12).

Privacy vraagstukken komen ook in deze uitgave aan de orde. De redactie gaat in op de privacy problemen met Google Workspace Education in Achter het Nieuws. Hopelijk leest dat bedrijf ook het artikel over kijken naar privacy als een kans om grotere klanttevredenheid en vertrouwen op te leveren. Deze artikelen warmen ons alvast op voor het volgende iB-magazine (iB-5) dat weer een privacy themanummer wordt.

Nicole

IN DIT NUMMER

Auteur: Sandra Kagie, freelance tekstschrijver (Sanscript Tekstproducties). Sandra is bereikbaar via info@sanscriptproducties.nl

INTERVIEW

Nationaal Cyber Security Centrum: ook voor niet-vitale organisaties?

`Oproep na kaas-hack: Bestempel voedselvoorziening als vitale infrastructuur', kopte de NOS op maandag 12 april. Bedrijven die het stempel 'vitaal' hebben gekregen kunnen voor hulp na bijvoorbeeld een hack immers aankloppen bij het Nationaal Cyber Security Centrum (NCSC). Waar anderen dat niet kunnen. In het kort de teneur van het artikel. Klopt dat echter wel? Ben je als niet-vitale organisatie op jezelf aangewezen als het gaat om je digitale weerbaarheid? We vragen het Martijn Jonk, teamleider bij het Nationaal Cyber Security Centrum.

"Zoals onder meer blijkt uit het Cyber Security Beeld Nederland 2020, is de digitale dreiging op ons land permanent. Alle reden dus om er gezamenlijk voor te zorgen dat onze digitale weerbaarheid niet langer achterblijft bij deze dreiging", trapt Jonk af. "Verhoging van de digitale weerbaarheid blijft de belangrijkste maatregel om deze risico's te beheersen. Als NCSC zien we dit als een gedeelde verantwoordelijkheid. Publiek-private samenwerking is en blijft daarom noodzakelijk."

"Op basis van de Wbni (red. - Wet beveiliging netwerk- en informatiesystemen, ook wel Cybersecuritywet genoemd) is het de primaire taak van het NCSC om vitale aanbieders en Rijksoverheidsorganisaties in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen te informeren, adviseren en indien nodig bijstand te verlenen", schrijft het NCSC in februari nog in een nieuwsbericht. Voor de helderheid: onder vitale organisaties worden producten, diensten en onderliggende processen verstaan die van essentieel belang zijn voor het dagelijkse leven van de meeste mensen in Nederland. Zoals toegang tot drinkwater, elektriciteit, internet en betalingsverkeer. "Uiteraard is digitale veiligheid ook voor organisaties die geen vitale aanbieder of Rijksoverheid zijn van belang", stelt het NCSC in hetzelfde bericht.

Landelijk Dekkend Stelsel (LDS)

"Precies de reden waarom we als NCSC in opdracht van het kabinet sinds 2018 inzetten op de ontwikkeling van het Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden", betoogt Jonk. "Zodat we ook niet-vitale organisaties zo goed mogelijk kunnen voorzien van relevante dreigingsinformatie."

Dat niet-vitale organisaties niet zouden kunnen aankloppen bij het NCSC is volgens Jonk dus niet waar. "Zo communiceert het NCSC via de website (red - ncsc.nl) bijvoorbeeld beveiligingsadviezen die voor iedereen, organisaties en particulieren, toegankelijk zijn", gaat hij verder. "Zo'n advies publiceren we naar aanleiding van een recent gevonden kwetsbaarheid of geconstateerde dreiging. We beschrijven de dreiging en de mogelijke gevolgen en we geven ook de mogelijke oplossingen."

"Met het Digital Trust Center dat in 2018 door ministerie van Economische Zaken en Klimaat (EZK) is opgericht werken we bovendien nauw samen om relevante informatie waarover wij beschikken naar een breder publiek, zzp'ers en mkb'ers, weg te zetten. En via het LDS delen we dus ook informatie met niet-vitale organisaties." Dit laatste gebeurt via schakelorganisaties als CERTs, Computer Emergency Response Teams, en zogenoemde OKTTs. Instellingen die 'objectief kenbaar tot taak' (OKTT) hebben andere organisaties, hun achterban, te informeren wanneer deze niet tot de vitale infrastructuur behoren.

"Via deze schakelorganisaties kunnen we als NCSC informatie waarover we beschikken op een efficiënte en effectieve manier delen met een brede groep van bedrijven en organisaties. Schakelen met een beperkt aantal partijen om via hen een grote groep te bereiken", legt Jonk het principe achter het LDS uit.

Op dit moment zijn de onderstaande organisaties als schakelorganisatie aangesloten op het LDS:

CERTs

- IBD, de InformatieBeveiligingsDienst is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten
- Z-CERT, het expertisecentrum voor cybersecurity in de zorg
- WM-CERT, het Computer Emergency Response Team Water Management
- SURF-CERT, het crisisteam van ict-onderwijsstichting SURF

OKTTs

- Vereniging Abuse Information Exchange
- Stichting Nationale Beheersorganisatie Internetproviders (NBIP)
- Stichting Cyber Weerbaarheidscentrum Brainport (CWB)
- Cyberveilig Nederland
- Connect2Trust
- Stichting FERM, onderdeel van het Port Cyber Resilience Programma

Wet als obstakel

Toch komt veel informatie die binnen het NCSC aanwezig is niet breed beschikbaar. Een constatering die Jonk beaamt: "De wet, onder meer de Algemene verordening gegevensbescherming (AVG), staat het delen van bepaalde privacygevoelige informatie met niet-vitale organisaties door het NCSC namelijk in de weg." Een constatering die minister van Justitie, Ferd Grapperhaus, begin februari ook deed in een brief die hij schreef aan de Tweede Kamer. "Voor het goed functioneren van het cybersecuritystelsel is een optimale uitwisseling van informatie over digitale dreigingen, kwetsbaarheden en incidenten tussen de overheid, vitale organisaties en niet-vitale organisaties van groot belang", schrijft de minister. Obstakels bij deze informatiedeling door het NCSC zijn 'onwenselijk'.

(Noot van de redactie: een IP-adres wordt door de AP als persoonsgegeven gezien en mag daarom niet zonder wettelijke grondslag worden gedeeld).
In de brief kondigt hij aan te willen komen met een wetsvoorstel om de mogelijkheden voor het NCSC om informatie te delen, juist ook met niet-vitale bedrijven, verder te verruimen. Hiervoor zou de Wbni op een aantal punten moeten worden gewijzigd.
Het gaat dan om de volgende aanpassingen:

1. Het mogelijk maken dat het NCSC in bijzondere gevallen informatie rechtstreeks aan individuele organisaties kan verstrekken die geen deel uitmaken van de Rijksoverheid of van de vitale infrastructuur in Nederland.
2. Het mogelijk maken dat het NCSC vertrouwelijk herleidbare informatie over aanbieders, bijvoorbeeld over kwetsbare IP-adressen, kan delen met OKTTs. Zodat zij als schakelorganisaties de betreffende aanbieders in hun achterban hierover kunnen informeren.

De eventuele aanpassing van de Wbni moet volgens het voorstel van de minister met voorrang worden opgepakt. Jonk hoopt dan ook dat het 'AVG-probleem', zoals hij het noemt, deze zomer is opgelost. De verwachting is dat de wet dan in internetconsultatie gaat.

Nationaal Detectie Netwerk

"Partners van het NCSC worden 24 uur per dag, 7 dagen per week gewaarschuwd in het geval van ernstige kwetsbaarheden (zogenaamde High/High-meldingen). Daarnaast delen we dreigingsbeelden en informatie over weerbaarheidsmaatregelen", legt Jonk uit. "Ook kunnen we onze partners aansluiten op het Nationaal Detectie Netwerk. Een samenwerking tussen ons, inlichtingen- en veiligheidsdiensten, organisaties binnen de Rijksoverheid, vitale organisaties en partners binnen het Landelijk Dekkend Stelsel."
"Via het NDN delen we dreigingsinformatie met elkaar. Informatie die gebruikt kan worden voor detectie. Deze informatie kunnen schakelorganisaties dan weer delen met hun achterban." De waarde die samenwerkingspartners kunnen halen uit aansluiting op het NDN 'is afhankelijk van de mate van volwassenheid van hun achterban op het gebied van cybersecurity', benadrukt hij. Of organisaties wanneer ze samenwerken met het NCSC ook verplicht zijn informatie terug te delen, ligt wat Jonk betreft genuanceerd. "Op grond van de Wbni hebben vitale aanbieders en aanbieders van essentiële diensten (AED's) in geval van ernstige incidenten een meldplicht bij het NCSC. Voor andere organisaties geldt dat op dit moment niet."
"Wanneer ons doel als Nederland echter is: sámen digitaal weerbaarder te worden dan is het in mijn ogen altijd nuttig om wanneer je met elkaar samenwerkt, informatie over dreigingen en incidenten te delen", gaat Jonk verder. "Ik zie het als een collectieve verantwoordelijkheid, een morele plicht zelfs. Door als organisatie een melding te doen, kun je het verschil maken voor een ander. Omgekeerd zou je van een ander hetzelfde willen."

Sámen een muur optrekken

Waar veel organisaties in Nederland volgens Jonk nu als het gaat om digitale veiligheid nog zijn gericht op het individueel een zo sterk mogelijke muur optrekken, hoopt hij dat dit mede door een steeds nauwere publiek-private samenwerking zal groeien naar het sámen een zo sterk mogelijke muur optrekken. Dat betekent volgens hem 'bouwen aan een sterk NCSC en een sterk DTC. Én bouwen aan 'sterke schakelorganisaties en daarmee aan een steeds sterker LDS'.

"Denk je nu als niet-vitale organisatie baat te hebben óf een bijdrage te kunnen leveren aan het bouwen van die collectieve muur, waardoor Nederland als geheel en daarmee ook iedere organisatie individueel digitaal weerbaarder wordt, onderneem dan actie", adviseert hij. "Bekijk met ketenpartners, sectorgenoten of bijvoorbeeld met een aantal regionale partners naar de mogelijkheid om schakelorganisatie binnen het LDS te worden. We hebben als NCSC verschillende handreikingen om zo'n samenwerking op te zetten."

Tot slot de minister

"De informatie-uitwisseling binnen het LDS is niet enkel de verantwoordelijkheid van de overheid. Het stelsel werkt alleen effectief en efficiënt als bedrijven zichzelf organiseren in samenwerkingsverbanden, die beeld hebben van wat er speelt binnen een sector en kunnen inschatten welke informatie relevant voor hen is en hoe deze informatie kan worden vertaald naar concreet handelingsperspectief", schreef minister Grapperhaus in februari aan de Kamer.
Een pleidooi waar Jonk zich graag bij aansluit. "In beginsel is elke organisatie, vitaal of niet-vitaal, verantwoordelijk voor zijn eigen digitale veiligheid. Maar wij zijn er als NCSC om collectieve weerbaarheid te faciliteren", vat hij samen.

Meer informatie over het NCSC en het samenwerken met het NCSC als schakelorganisatie is te vinden op de website ncsc.nl. Contact opnemen via samenwerken@ncsc.nl kan ook.
Cybersecuritybeeld Nederland 2021:
https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

SyRi dood? Welnee, het heet nu alleen anders

Wie denkt dat de overheid leert van haar fouten, komt ook op het gebied van privacy bedrogen uit. De inkt op het rapport uit Omtzigt-gate is amper droog en ondertussen gaat politiek Den Haag vrolijk verder met het ontwerpen van wetten die automatisering van besluitvorming en data-analyse met profilering van burgers mogelijk maakt. Op de valreep voor het nieuwe jaar werd in december 2020 door de Tweede Kamer het wetsvoorstel 'Wet gegevensverwerking door samenwerkingsverbanden' (WGS) aangenomen.

Een wet die zeer vergaande bevoegdheden moet inregelen waardoor private en publieke partijen kunnen samenwerken om criminaliteit aan te pakken. Dat aanpakken gebeurt dan door middel van het analyseren van enorme bakken data uit diverse bronnen. De Raad van State maakte eind april al gehakt van het voorstel in haar adviesrapport. Ze noemde de wet niet effectief, veel te breed en vaag in scope en te weinig specifiek. Ook maakt de wet een te grote inbreuk op het grondrecht op privacy en stelt: 'Omdat het voorstel vergaande beperkingen van het recht op bescherming van de persoonlijke levenssfeer mogelijk wil maken en tegelijkertijd niet de wezenlijke elementen en begrenzingen bevat, voldoet het in deze vorm niet aan de eisen van artikel 10 Grondwet.'

De Autoriteit Persoonsgegevens werd pas afgelopen april om een mening gevraagd en heeft deze nog niet kunnen geven, maar ik kan me niet voorstellen dat zij een andere mening zullen zijn toegedaan dan de Raad van State. Sterker nog, AP heeft het werken met Artificial Intelligence en slimme data-analyses opgepakt als een van de speerpunten van haar handhavende toezicht. Zo deed AP in 2020 uitgebreid onderzoek naar de misstanden bij de Belastingdienst in het toeslagenschandaal. De verwerkingen waren onrechtmatig, discriminerend en onbehoorlijk, oordeelde de toezichthouder.

In hetzelfde jaar dat de WGS werd aangenomen door de Tweede Kamer, werd SyRI (Systeem Risico Indicatie) verworpen door de rechter. Over SyRI oordeelde de rechter dat het een te grote inbreuk maakte op het grondrecht op privacy en het onvoldoende inzichtelijk en controleerbaar was. De wet werd onrechtmatig geacht en onverbindend verklaard. SyRI was een wettelijk instrument dat de overheid gebruikte voor de bestrijding van fraude op bijvoorbeeld het terrein van uitkeringen, toeslagen en belastingen. Alles door middel van eenzelfde soort data-analyses en profilering van burgers als de WGS nu voorstelt.

SyRI, de toeslagenaffaire en de WGS zijn slechts recente voorbeelden van extreem privacy inbreukmakende systematieken. In het iets verdere verleden vinden we de discriminerende Verwijsindex Antillianen, een kentekenregistratiesysteem (ANPR) dat voor allerhande doeleinden werd ingezet waarvoor het niet bedoeld was en niet te vergeten de corona noodwetgeving, die forse beperkingen op grondrechten mogelijk maakt. Keer op keer laat de overheid zien niet volwassen genoeg te zijn om op een ethisch verantwoorde manier met de gegevens van burgers om te gaan. Wat mij betreft is het tijd voor een pas op de plaats. Want als de schandalen met gegevens van burgers een ding duidelijk maken, dan is het dat burgers hierin telkens het onderspit delven en slachtoffer worden van onkunde en geblunder. Het gaat over mensen en over overheidsbesluitvorming met grote levensveranderende gevolgen. Daar past niets anders dan zeer grote terughoudendheid.

Rachel

Auteur: Drs. ing. William Breuer schrijft op persoonlijke titel en is als Ethisch Hacker werkzaam bij het Cyber Defense Center van de Volksbank. Hij is bereikbaar via William.Breuer@deVolksbank.nl. Dit artikel is mede tot stand gekomen met hulp, allen op persoonlijke titel, van Kim Gunnink en Roy Huijts (de Volksbank) en Yorick Koster (Securify).

Bescherm je websitebezoekers:

Voorkom JavaScript-aanvallen via derden

Er is geen bedrijf ter wereld dat graag ongevraagd een stukje cryptominingcode geïnjecteerd krijgt op zijn website. Toch duikt zo af en toe een nieuwsbericht op dat een website via een derde partij is gecompromitteerd. Hoe? Via extern ingeladen JavaScripts. Een kwaadwillende past het JavaScript bij de externe derde aan en in plaats van een nuttige feature is het JavaScript ineens malware worden. Hoe kun je dit voorkomen?

Als je wilt weten hoe het gesteld is met de beveiligingsmaatregelen rondom JavaScripts op jouw website kun je gebruikmaken van security-checkers zoals Mozilla's Observatory (1). Daar leg je jouw eigen site als het ware langs de meetlat: heb je alle beveiligingsmaatregelen geactiveerd die de test adviseert? Maak je bijvoorbeeld al gebruik van `Subresource Integrity' (SRI)? Grote kans dat je nu met gefronste wenkbrauwen zit te lezen. Geen nood: dit artikel vertelt je meer over mogelijke kwetsbaarheden van extern ingeladen JavaScripts en het nut van oplossingen, zoals SRI.

Gebruikt jouw website JavaScripts die niet op je eigen webserver gehost worden? Dan maakt de site gebruik van externe scripts, ook wel derde partij scripts genoemd. Als je geen maatregelen treft die misbruik voorkomen, ben je kwetsbaar voor wat je JavaScript supply-chain-aanvallen kunt noemen: het door een kwaadwillende naar believen kunnen aanpassen van die JavaScripts. Tijdens dit type aanval op de externe partij wordt ook jouw website een gecompromitteerde website. Zo kan jouw website ineens malware gaan verspreiden, jouw bezoeker cryptomining laten uitvoeren of kan de bestemming waar een (contact- of bestel)formulier naar wordt verzonden worden aangepast (zogenaamde `FormJacking' (2)). De kans dat dit met één van de op jouw website ingeladen scripts gebeurt lijkt misschien klein, maar de potentiële impact is hoog. Omdat elk ingeladen JavaScript standaard alle rechten heeft in de browser van de bezoeker, wordt iedere bezoeker namelijk direct geraakt door de aanval.

Vele aanvalsscenario's leiden tot dezelfde uitkomst

Het is nog niet zo simpel om een extern gehost JavaScript aan te passen. Zeker niet als die server bij de derde partij goed is beveiligd. Maar onmogelijk is het zeker niet. Drie voorbeeldscenario's van hoe het toch mis zou kunnen gaan:

1. JavaScript als direct doelwit

Ondanks goede afspraken die je met derden kunt maken, kan er altijd iets gebeuren waardoor een kwaadwillende toch het externe JavaScript kan aanpassen. Bijvoorbeeld doordat een kwaadwillende ineens gebruik kan maken van bewerk-functionaliteiten, zoals Tag Managers die vaak aanbieden. Bestaan ingeladen JavaScripts uit vele onderdelen en wordt een stuk van het ingeladen JavaScript uit andere projecten gehaald? Dan kan dat een risico vormen als er niet goed genoeg gescreend wordt welke code wordt toegevoegd. Denk hierbij bijvoorbeeld aan code uit een open-source project dat in het JavaScript wordt ingeladen zonder dat de ontwikkelaars echt kijken naar wat de code doet (bijvoorbeeld bij een update).
Ook insider threats kunnen een risico zijn. Een ontevreden ontwikkelaar kan bijvoorbeeld proberen een aanpassing door te voeren in het (versiebeheersysteem van het) JavaScript dat uiteindelijk op jouw website staat. Of denk aan een ontslagen systeembeheerder die zijn voormalige werkgever – jouw leverancier – een ha(c)k wil zetten.

2. Via de webserver bij de derde partij

Ook door een hack of een misconfiguratie van de webserver van de derde partij, waar het JavaScript wordt gehost, kan een probleem ontstaan. Immers kan een kwaadwillende die op de een of andere manier (schrijf)toegang krijgt tot de webserver het JavaScript bestand aanpassen.
Dankzij goede beschrijvingen van praktijkvoorbeelden, zoals bijvoorbeeld door het NCSC UK (3) en RiskIQ (4), kunnen we kennis opdoen van dit soort scenario's. Eén voorbeeld betrof een extern JavaScript dat op vele websites actief bleek, waar bezoekers van de gecompromitteerde websites waarop het javascript draaide de kwaadwillende hielpen met crytocurrencymining. Het andere voorbeeld was een extern JavaScript dat op specifieke webpagina's stond en uiteindelijk resulteerde in onder andere een datalek.

3. Via netwerkaanvallen

Kan de kwaadwillende het script niet direct aanpassen en de webserver niet hacken? Dan kan hij of zij kwaadwillende nog rigoureuzer te werk gaan.
In 2016 werden de `Domain Name System' (DNS) instellingen van (kwetsbare) thuisrouters zo aangepast om het IP-adres van het domein waarop specifieke JavaScripts stonden te laten verwijzen naar de webserver van de kwaadwillende (5). Zo konden kwaadwillenden het JavaScript dat werd ingeladen aanpassen en konden de vele websites die het script inlaadde

Ingeladen externe scripts weten wellicht meer van uw bezoekers dan u wilt meegeven aan de derde partij. Een browser deelt, standaard en zonder dat er in het script code voor aanwezig is, het volledige adres van de webpagina met de server waar het JavaScript wordt opgevraagd. Dit gebeurt via de 'referral header'. Bij situaties waar in het webadres herleidbare informatie staat, kan dat zelfs leiden tot datalekken. Denk hierbij bijvoorbeeld aan het lekken van de postcode van de klant op een webadres zoals https://example.nl/winkel-zoeker?postcode=1234AB. Het zetten van een 'referrer-policy header' (10) en het maken van afspraken over het verwerken van dergelijke informatie is, zelfs bij het gebruik van SRI, dus vrijwel altijd aan te bevelen.

worden voorzien van advertenties. Zolang die eerste router-hack maar niet opviel kon er dus geld worden verdiend. Destijds kon deze aanval plaatsvinden omdat er nog veel gebruik werd gemaakt van onversleutelde (http-)verbindingen. Dat is anno 2021 wat lastiger voor een kwaadwillende, omdat inmiddels vrijwel elke website versleutelde (https-)verbindingen gebruikt. Doordat de kwaadwillende op het andere IP geen geldig https-certificaat kan aanbieden zal de verbinding met de server niet worden opgebouwd en zal het JavaScript niet worden geladen.

Het is echter mogelijk varianten te bedenken die nog wel werken. Kan de kwaadwillende aanpassingen doorvoeren in de DNS van de externe partij zelf of hun leverancier (6)? Of kan het zelfs, als het JavaScript op een ander topleveldomein staat, het complete topleveldomein (7) overnemen? Dan kan de kwaadwillende, mits goed voorbereid én ondanks de (zeer) opvallende werkwijze van zo'n aanval, in korte tijd veel slachtoffers maken ver buiten het aangepaste DNS-domein zelf. Wordt er immers een JavaScript van een gecompromitteerd domein ingeladen, dan is jouw website ook gecompromitteerd. JavaScript supply-chain-aanvallen hoeven dus niet gericht te zijn op jouw bedrijf, maar jouw website en jouw klanten kunnen alsnog slachtoffer worden.

De integriteit van JavaScript verbeteren

Bij het op betrouwbare wijze in gebruik nemen van extern gehoste JavaScript bestanden is het belangrijk om vast te stellen dat de door de websitebezoeker ingeladen JavaScriptcode nog gelijk is aan de versie die de programmeur op de website plaatste. Met andere woorden: de integriteit zal moeten worden vastgesteld.

Een eerste gedachte kan wellicht zijn om alle scripts van derden van de website te weren of alles lokaal op eigen server te plaatsen. Dat lost het probleem op, immers je weet als bedrijf wel wanneer je eigen servers onder aanval liggen. Toch is het weren van dit soort scripts in de praktijk vaak onhaalbaar, omdat er dan functionaliteiten van de website verloren gaan. En alles lokaal plaatsen kost onderhoud en wordt niet altijd door een leverancier mogelijk gemaakt.

Een andere optie is om JavaScripts om te bouwen naar Application Programming Interface (API) calls. Stel dat er bijvoorbeeld een extern JavaScript wordt geladen dat als functie heeft om een postcode om te zetten naar een adres, dan kan dit ook zo worden omgebouwd dat de website zelf de logica bevat en alleen de gegevens ophaalt bij de leverancier. Hier is echter vaak wel (veel) ontwikkeltijd aan verbonden en het onderhoud kan lastiger worden. Ook kan het niet in alle situaties goed worden toegepast.

Subresource Integrity: de integriteit-hash toepassen

Het toepassen van Subresource Integrity (SRI) kan een praktische oplossing zijn. SRI is ooit bedacht om de integriteit van scripts (en stylesheets) die je inlaadt van Content Delivery Networks (CDN) te garanderen. CDNs bieden veelgebruikte JavaScripts aan, waarmee schaalvoordelen kunnen optreden op bijvoorbeeld snelheid en benodigd dataverkeer.

Sinds 2016 is SRI een aanbeveling van het World Wide Web Consortium (W3C) (8). Elke moderne browser ondersteunt het inmiddels. Het leunt op het principe dat we ook kennen bij het downloaden van software: 'controleer de hash'. De programmeur stuurt na het opleveren van de software de hash van die versie mee en deze wordt gepubliceerd in de website,

Het is niet simpel om een extern gehost JavaScript aan te passen. Maar onmogelijk is het zeker niet

als 'integrity'-parameter van het 'script'-tag. Die waarde is dan uniek voor de inhoud van dat JavaScript. Het is (nagenoeg) onmogelijk om dezelfde waarde te maken voor een andere inhoud.

```
<script
        src="https://example.nl/javascript.js"
        integrity="(berekende-SHA384-hash-in—base64)"
        crossorigin="anonymous"
        nonce="(willekeurige-SHA-hash-in-base64-vanuit-CSP-header)"
>
```

Klopt de hash niet op het moment dat de browser het script downloadt en de hash nogmaals berekend wordt? Dan wordt het script niet uitgevoerd.
Enkele investeringen bij zowel de leverancier als de website-bouwer zijn helaas wel nodig: een goed versiebeheer en een gedegen patch-proces zijn ineens van groot belang. Er kan dus niet meer worden geleund op een 'altijd up-to-date live'-versie van een JavaScript, waar de leverancier zonder medeweten zomaar updates kan doorvoeren. Tegelijkertijd is dit voor een securityafdeling waardevol, omdat er zo meer controle is op wat de scripts doen. Immers kan er, na een pen-test bij een eerste livegang van het script, zeer makkelijk naar de verschillen worden gezocht in de code die elke keer live gaat. Bij elke livegang moet een nieuwe hash worden opgevoerd, dus niets gaat zonder het te weten live. Maar het betekent wel meer onderhoud, initieel om die codes makkelijk te kunnen opvoeren en vervolgens omdat elke update idealiter gecontroleerd moet worden doorgevoerd.

De aan/uit knop

Is het gebruik van SRI (nog) niet mogelijk, is de verversingsfrequentie (nog) dermate hoog dat het beheer onmogelijk zou worden of wil je nog een extra beveiligingsmaatregel toevoegen voor gebruikers van oude browsers zoals Internet Explorer 11? Kies dan voor een 'aan/uit' knop voor elk extern ingeladen JavaScript. Dit zorgt ervoor dat een script meteen uitgeschakeld kan worden in het geval van een gecompromitteerde situatie. De website dient dan wel zo te zijn ontwikkeld dat deze zonder het script functioneel goed blijft werken, bijvoorbeeld door de gebruiker het adres zelf te laten invoeren in het voorbeeld van een postcode-omzetter JavaScript. Omdat snelheid dan de sleutel tot mitigatie is kunnen we gerust stellen dat je eigenlijk altijd te laat bent voor de eerste paar slachtoffers, maar hierdoor wel erger kunt voorkomen. De gehele site offline halen is niet meer nodig om te voorkomen dat nog meer klanten worden blootgesteld. Wel is het dan van belang om met de leverancier afspraken te hebben over de snelheid waarmee zij een gecompromitteerde situatie opmerken en melden. Het restrisico dat zo overblijft is duidelijk en kan door de eigenaar van de website goed worden overwogen en geaccepteerd in acceptatie-trajecten, totdat het JavaScript zo wordt aangepast dat het wel SRI kan ondersteunen, lokaal kan draaien of de functionaliteit als API kan worden aangeroepen. Tenslotte kan het bij specifieke aanvallen ook helpen om een Content Security Policy (CSP) (9) actief te hebben, bij voorkeur inclusief de rapportage optie. Mocht een kwaadwillende in het JavaScript slechts een korte instructie hebben toegevoegd om een JavaScript elders op te halen dan zal CSP dit al snel blokkeren en hierover alarmeren. Het moment om de 'uit' knop vervolgens snel in te zetten.

Referenties

(1) https://observatory.mozilla.org/

(2) https://www.digitaltrustcenter.nl/informatie-advies/formjacking

(3) https://www.ncsc.gov.uk/guidance/ncsc-advice-malicious-software-used-illegally-mine-cryptocurrency

(4) https://www.riskiq.com/what-is-magecart/

(5) Ad-Fraud Malware Hijacks Router DNS, Sergei Frankoff, 25 maart 2015, https://sentrant.com/2015/03/25/

(6) https://blog.fox-it.com/2017/12/14/lessons-learned-from-a-man-in-the-middle-attack/

(7) https://thehackerblog.com/tags/#tld hijacking

(8) https://www.w3.org/TR/SRI/

(9) https://www.w3.org/TR/CSP2/

(10) https://www.w3.org/TR/referrer-policy/

Authors: Andres Maurer and Robert Metsemakers have extensive security experience in respectively Swiss and Dutch financial services. They wrote this article together in a personal capacity. They can be reached on andres-maurer@hotmail.com and robert.metsemakers@gmail.com.

Best practices in access managament (part 1 of 2)

The purpose of this article is to provide best practices for the different processes in a generic access management process landscape. They are based on 'lessons learned' and experience gained by the authors in various implementation projects for access management and through regular line activities.

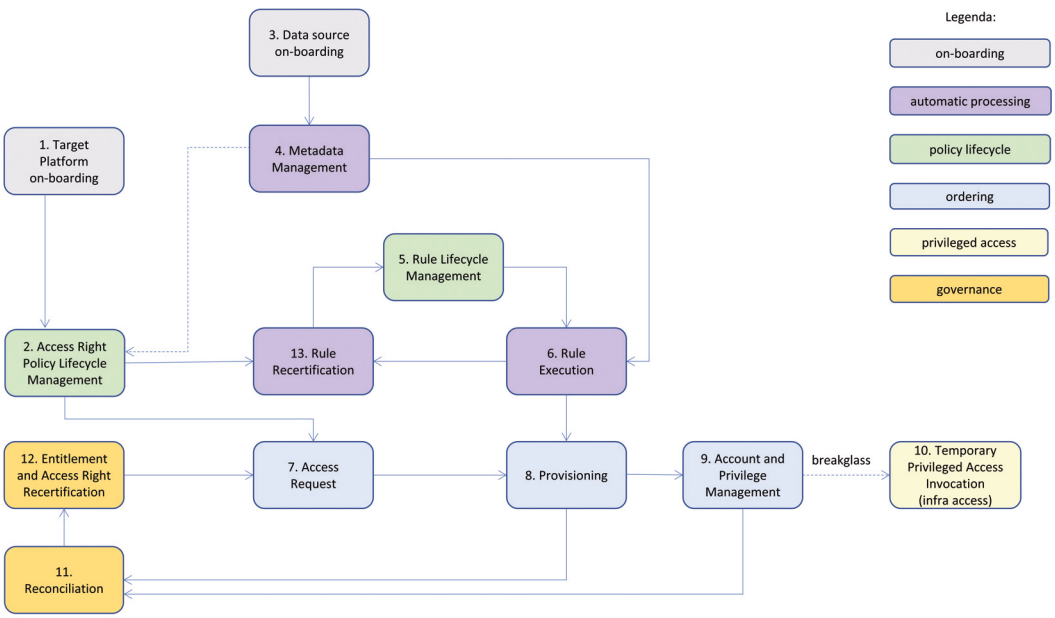


Figure 1 - Steps in Acces Management.

Access management, as an 'existing discipline', might not always receive the same attention as the latest and greatest next generation firewall or an 'artificial intelligence enhanced automatic anomaly analysis remediation device'. Whatever new security technology the future brings, the topic access management will remain an important basic building block of security. It will always be essential to give users exactly the right level of privileges in the various information systems. Not too much, to prevent misuse and abuse. And also not too little, because employees need access to the right information to be able to work.

The best way to do that is to:

- Have an enterprise-wide access model that defines what access rights and (high) privileges are needed for different

functions/roles in the organization.
- Stick to that access model during deployment.
- Use a centralized access management repository for the whole organization. And ensure that the whole process is traceable end-to-end (provide an 'audit trail').
- Make sure that the 'Joiner-Mover-Leaver' process functions end-to-end and that access rights can be revoked quickly when required (for example: terminated employees).
- Automate, automate, automate where possible, but have a manual handbrake/'break-glass' to stop 'escalations' when things are getting out of hand (like removal of existing rights).
- Understand that these different steps take time to do them right and accept that access management is a full-time job (for maybe even more than one person in larger organizations).

We assume you already know an abbreviation or two (like RBAC, SoD, SSO) about Identity and Access Management. If not, please check Wikipedia (1). The first part explains steps 1 to as shown in figure 1.

Section 1 – Process Landscape

1. Target Platform on-boarding

Description

It is important to ensure that a new platform (e.g. Linux/Unix, Windows, etc.) or an update to an existing one are always compatible with the corporate IAM environment, ensuring that accounts and rights on this platform can be provisioned by this IAM system. This process provides the basic integration patterns to both identity and access management systems (including 'Privileged access' for system administrators) for the whole enterprise. Note: identity management needs to be implemented together with access management but is outside of the scope of this article.

Best Practices

- Communicate the IAM protocols that are in use in your organization and include them already as requirements during purchase/ Request for Quotation/Request for Information to suppliers of IAM systems. Integrating the new asset would then only require configuration work instead of having to develop specialized interfaces.
- Ensure that architecture includes a definition of IAM strategy according to your corporate strategy (for example – Need to know, information barriers, etc.).
- Maintain a Standard or Inventory of all IAM-protocols that can be used in your organization and by that, also a list of protocols that are not supported. Correspondingly, an exception process has to be in place to allow special cases to be implemented. However, roles and responsibilities have to be clearly delegated and adequately covered.
- Provide, for example in the form of a detailed whitepaper, an 'on-boarding guide' on how to integrate new and changed information systems and platforms with the corporate IAM services.

2. Access Right Policy Lifecycle Management

Description

The process to define access rights and roles for an application becomes more consistent when using the same access concept for the whole enterprise (note: in this article, access rights are granted on application level - the applications run on platforms). This includes managing changes to the rights and roles of users (including developers) during the development or extension of a new information system. Additionally, there is often no proper decommissioning of rights/roles when they are no longer needed. The leftover privileges may grant users an unintended access level that is not readily visible. Therefore, the decommissioning of rights/roles should be done consequently when the application is decommissioned to prevent this accidental side-access to other applications.

Best Practices

- Development and procurement of applications based on the list of supported IAM protocols.
- Provide a clear application access concept, to help definition of access roles and rights at the 'right' granularity level that complies with the Enterprise access structure (RBAM/Role Based Access Management concept, etc.).
- Provide an analysis tool to help identify clusters of user rights and track risks (like violations of Segregation of Duties or missing 'four eyes' checks).
- Clearly define the different cases where and how Segregation of Duty (SoD) should be enforced. In some cases, this can be enforced by defining this through different access rights. Otherwise, this needs to be part of the application logic.

3. Data source on-boarding

Description

This process on-boards the metadata source (for instance, the database with personnel records from Human Resources

department providing personnel numbers, names and departments) for use in the IAM processes.

Best Practices

- Develop a clear understanding of the data source's life cycle and frequency of update that is to be expected in the future.
- Provide a clear (and as complete as possible) Corporate Data Dictionary, so that roles and rights are understandable for non-experts.
- Ensure that a field's taxonomy (like numbers only, capitals only, maximum length) is consistent across different systems.
- Identify the fields in the data source that can be used for plausibility checks or manual verification threshold.

4. Metadata Management

Description

The activity to process metadata from the different data sources that are used to trigger access management rules has to be properly defined and thought through to prevent any unplanned side-effects of edge cases of unforeseen constellations. Proper handling of the metadata's lifecycle is key to automation.

Best Practices

- Have a clear understanding of the volatility of the content of each field. Fields that change too often may not be suitable as a parameter for automation (of deployment of IAM rights).
- Clearly define the data source of 'enriched fields', to prevent having to do redundant maintenance of the same data in both source and IAM system.
- Ensure transactional completeness of an import run from the data source into the IAM system.
- Ability to (manually) stop the propagation if the data provided by the source is found to be corrupt/incomplete. Should there be a data issue from a critical data source, this might trigger removal of automated access rights and handicap the organization.

5. Rule Lifecycle Management

Description

This process creates, updates or decommissions automated grants and Segregation of Duty/ Information Barrier rules for an application.

Automation can massively reduce Access Management overhead if a proper IAM Concept is in place and fit for daily use. A key function is the analysis impact of the changes to the rules in the event that metadata content changes in a way that impacts the rule execution. Reorganizations are especially challenging, as they may need to be kept confidential and the rules have to be changed to reflect this in a short timeframe. Otherwise, rules that depend on the Organizational Unit may suddenly not be consistent after the OU change, leading to certain employees not having proper access after the reorganization. Analog to access rights, it is important to keep the rules up to date and decommission rules that are no longer needed.

Best Practices

- Automatically applied rules where feasible to reduce manual overhead.
- Determine a clear ownership of the Rule (every rule should have one owner). Rules will experience entropy, which means that rules' exactness degrades over time and needs to be updated occasionally.
- Have a clear and complete understanding of (external) regulatory and internal control requirements, as they are fundamental for the rules.
- Have a clear and documented understanding of the volatility (lifecycle) of the underlying metadata when defining rules. Highly volatile metadata will trigger rule execution more often, and this may not be necessary nor efficient.
- Define and test the rules on a (test) system separate from the live IAM-system.
- Implement both automated and manual execution of the rules. During manual execution, the rule owner needs to verify the result of the rule before triggering the execution. This allows the rule owner to gain confidence on the rule accuracy before switching to automated execution.
- Define a threshold, for instances on amounts of changed accounts or user rights, to determine when automation of rules should revert back to manual. For instance, it is very unusual that more than 100 users need to be stripped of all their access rights at once. An input error in the department number seems more likely.

6. Rule Execution

Description

This process controls the execution of the rules that are defined in the step 'Rule Lifecycle Management'. Unforeseen events

can happen that may decapitate the Access Management policies. Therefore, it is highly recommended to provide an option to manually validate the rule results before the actual deployment.

Once in full automation mode, a circuit-breaker mechanism is highly recommended that will trip the automation into the manual confirmation mode if the threshold is surpassed. This can often be caused by metadata problems and could - in the worst case - lead to widespread access removals.

Best Practices

- The IAM-system needs to be able to fully execute all the rules within the designated time window, so performance testing is needed to assure this.
- Clear behavior of rules in conflict situations (grant and block) is needed (for instance: if conflict exists, then no rule action).
- You need to have the ability to pause an automatic rule until discovered issues are fixed.
- Provide traceability of automatic rule actions (like a date time stamp, rule number etc.).
- The purpose and expected results of the (automatic) rule should be documented clearly.
- A 'Deputy' (= the person allowed to intervene) is needed for cases of manual intervention.

7. Access Request

Description

Even if there is an automated access granting process in place, there will still be a need for an end user or representative to manually request for addition, change or removal of access rights for specific account(s).

All access requests should be checked for any violation of policies (both IB and SoD).

Example for Information Barrier: employees from Division South should not be able to view (bank) client records from Division North.
Example for Segregation of Duties: an employee that puts in a new salary level, should not be able to validate that request him/herself.

To ensure an efficient execution, the approval of the access requests by the relevant Line Manager (of the requestor) and designated approver groups (like system or application 'owner') should be time-boxed so that there is a planned amount of time before the request is completed.
Rights that are automatically granted via access roles or automatic rules should be clearly designated. Rights granted through such mechanism cannot be changed or updated.

Best Practices

- User (requestor) must be able to quickly find the desired access rights/roles in the full list.
- Provide good navigation, clear structure and an efficient search engine to help the requestor find the 'right' access rights.
- Description and metadata of the roles and rights need to be clear and precise.
- Approval process should match (in speed and number of controls) the criticality of the access (for instance: being able to book a parking space is less critical than access to a banking system).
- Duration of the approval of the access request needs to be time-boxed, as soon as possible but with the necessary controls.
- Provide clear feedback to both requestor and security officer should there be a violation in the request.
- In some cases, a violation may have a time-limited exemption where the extra rights are granted, but only with additional management approval.
- Define a clear approval deputyship, make sure there is no single point of blockage (for instance: security officer is on holiday and because she cannot approve, 'nobody' can work in the system).

Part 2 of this article will be published in iB5 and will address steps 8 to 13 as shown in figure 1.

Reference

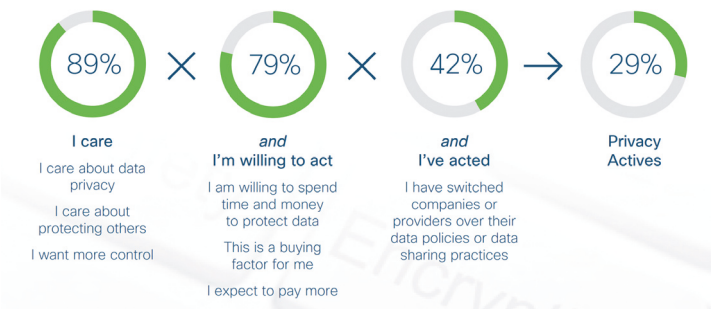
(1) For instance, https://en.wikipedia.org/wiki/Identity_management

Auteur: Enrico van de Laar is data privacy expert bij Dataheroes en helpt organisaties om dataprivacy van hun klanten, medewerkers, cliënten en burgers op innovatieve wijze te beschermen. Enrico is bereikbaar via enrico@dataheroes.nl.

Zie dataprivacybescherming als kans in plaats van verplichting

Veel organisaties zien het beschermen van dataprivacy van hun klanten, medewerkers, burgers of cliënten als een verplichting die door wet- en regelgeving opgelegd wordt. Nog meer organisaties voelen zich (nog) niet geroepen om überhaupt privacygevoelige data optimaal te beschermen. Het bewijs hiervan zien we de laatste tijd regelmatig terug in nieuwsberichten over datalekken en het onrechtmatig gebruik van privacygevoelige gegevens.

Uitgezonderd de organisaties die dataprivacy wel serieus nemen, simpelweg omdat ze het belangrijk genoeg vinden, maakt het merendeel zich niet zo druk. De Autoriteit Persoonsgegevens heeft veel meer op haar bordje dan ze aankan en dat lijkt de komende tijd alleen nog maar erger te worden. Waarom zou je als organisatie zoveel tijd, geld en moeite stoppen om aan wet- en regelgeving te voldoen als er nauwelijks gehandhaafd wordt?
Het antwoord op deze vraag komt uit een andere hoek dan de wet- en regelgeving, namelijk de personen van wie privacygevoelige informatie wordt verwerkt. Er is al een tijd een beweging actief die de term dataprivacy langzaamaan beter begrijpt. Stonden we jaren geleden nauwelijks stil bij hoe organisaties met onze gegevens omgingen – vooral omdat we eigenlijk geen idee hadden wat we weggaven – inmiddels zijn we aanzienlijk kritischer geworden over hoe er met onze privacygevoelige data omgegaan wordt. Hierbij spelen de publieke discussies rondom corona apps, de vele datalekken in het nieuws en onze persoonlijk online veiligheid een grote rol.
We eisen steeds vaker dat organisaties op een goede manier met onze privacygevoelige gegevens omgaan. Verschillende



Figuur 1 – Het aantal personen dat zijn of haar privacy van groot belang vindt neemt toe. Bron: Cisco Consumer Privacy Study 2020.

onderzoeken bevestigen dit. Zo liet een onderzoek van Cisco in 2020 (1) zien dat meer en meer consumenten het heft in eigen hand nemen op het gebied van dataprivacy. Deze groep – door Cisco 'Privacy Actives' genaamd, zijn kritisch over hoe organisaties met hun gegevens omgaan en zijn bereid actie te ondernemen op het moment dat ze het gevoel hebben dat er niet goed met hun digitale gegevens omgegaan wordt. Zo geeft 42% van de Privacy Actives aan dat ze zelfs van

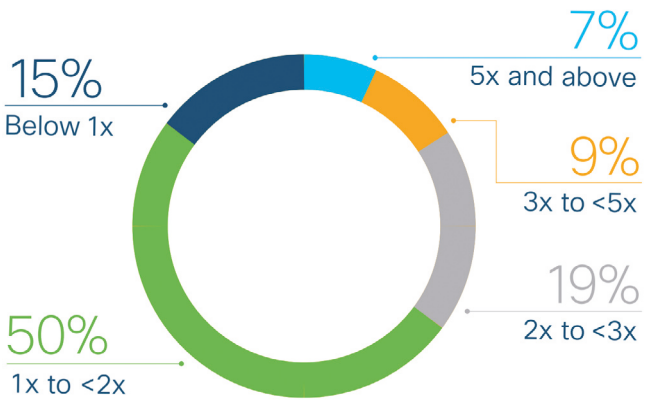
leverancier zouden wisselen op het moment dat hun dataprivacy niet goed beschermt wordt.

Mocht je dus als organisatie nog niet veel aandacht hebben gegeven aan dataprivacybescherming, dan zou dit dus zeker een signaal kunnen zijn hier iets mee te gaan doen. Door de impact van o.a. social media kan één fout op het gebied van dataprivacybescherming enorme impact hebben op je organisatie, haar imago en het vertrouwen van de consument.

Dataprivacy als unique selling point

Toch pleit ik liever voor een compleet andere aanpak. De groter wordende groep Privacy Actives zou je namelijk als een nieuwe doelgroep kunnen aantrekken door te laten zien dat jij het als organisatie wél goed voor elkaar hebt. Dataprivacy als unique selling point! De impact van dataprivacybescherming voor organisaties is al door verschillende onderzoeken in kaart gebracht. Een onderzoek van Capgemini in 2019 (2) liet zien dat het voor organisaties veel voordelen kan hebben om dataprivacybescherming als een kans te zien in plaats van een verplichting. Zo gaf 92% van de ondervraagde organisaties aan dat ze door aan de AVG te voldoen voordeel hebben behaald ten opzichte van hun concurrenten die hier nog niet aan voldoen. Dit uit zich onder andere in een stijging van klanttevredenheid, beoordelingen en – misschien nog wel belangrijker – vertrouwen. Ook op financieel gebied heeft het voldoen aan privacywet- en regelgeving voordelen. Uit de Data Privacy Benchmark van Cisco van 2021 (3) wordt duidelijk dat investeringen in dataprivacybescherming bijna twee keer terugverdiend worden. In sommige gevallen zien organisaties zelfs een return on investment van vijf keer het geïnvesteerde bedrag.

Vanuit deze onderzoeken en cijfers kunnen we denk ik wel concluderen dat de tijd dat je als organisatie dataprivacy kon negeren is gepasseerd. Maar hoe pak je dat als organisatie aan en waar liggen de grootste kansen? Eén van de belangrijkste gebieden waarin je als organisatie kunt investeren op dataprivacyvlak zijn privacycertificeringen. Dergelijke onafhankelijke certificeringen – zoals bijvoorbeeld ISO 27001/27701 – hebben een bewezen positief effect met name voor organisaties die zich op business-to-business diensten en producten richten. Een ander belangrijk gebied is de dataprivacy awareness van medewerkers. Door medewerkers te trainen op het gebied van dataprivacybescherming stijgt de bewustwording dat zich weer uit in kwaliteitsverbetering. Daarnaast



Figuur 2 – Organisaties verdienen hun investeringen in dataprivacy in de meeste gevallen meer dan terug. Bron: Cisco Data Privacy Benchmark Study 2021.

dient er ook aan bewustwording gewerkt te worden bij het bestuur van een organisatie zodat dataprivacybescherming op de agenda komt en blijft staan. Belangrijk is ook transparantie naar diegenen van wie je de privacygevoelige gegevens verwerkt. Dit kan door open te zijn over de maatregelen die je neemt om de privacy van die personen te beschermen en ze daar zelfs actief in te betrekken. Hierdoor draag je positief bij aan de ervaringen die een persoon heeft op het moment dat ze hun data bij je achter laten wat vervolgens weer kan bijdragen in het vertrouwen in je organisatie.

Kortom, er zijn redenen genoeg om serieus met dataprivacy aan de slag te gaan. Het zal zich zeker niet alleen terugbetalen, maar ook een positief effect hebben op het vertrouwen dat mensen in je organisatie hebben. En naast deze effecten is het simpelweg ook het juiste om te doen, want zeg nou zelf, in deze tijd waar we meer dan ooit privacygevoelige gegevens delen wil je er zelf toch ook op kunnen vertrouwen dat er veilig met je gegevens omgegaan wordt?

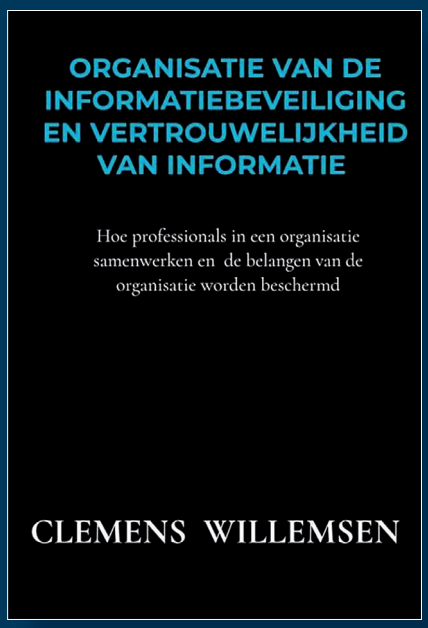
Referenties

(1) https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf

(2) https://www.capgemini.com/wp-content/uploads/2019/09/Report_Championing-Data-Protection-and-Privacy.pdf

(3) https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf

Auteur: Chris de Vries is redacteur en zelfstandig professional onder de naam Chris de Vries Impuls Management. Chris is bereikbaar via: impuls@euronet.nl.



Titel	: Organisatie van de informatiebeveiliging en vertrouwelijkheid van informatie
Auteur	: Dr. Clemens H.J. Willemsen
Taal	: Nederlands, Engels, Frans, Spaans
Aantal pagina's	: 87
ISBN	: 978-94-0360-917-1
Uitgever	: Managementboek

BOEKREVIEW

Organisatie van de informatiebeveiliging en vertrouwelijkheid van informatie

Het oogmerk van dit boek is een handreiking te geven voor een praktische invulling van de taak als (deeltijd) informatiebeveiliger (geen hoofdtaak) op het terrein van informatiebeveiliging en bedrijfsproceskennis, wetende dat de rol een grote vakinhoudelijke deskundigheid vereist.

“Was rubricering vroeger vooral het classificeren van afzonderlijke documenten, nu is het meer en meer het classificeren van een informatiesysteem als verzameling van documenten waarover dan in één keer een uitspraak over het niveau wordt gedaan.”

Daarbij besteedt de auteur aandacht aan de volgende zaken:
- organisatie en rolverdeling;
- relatie vertrouwelijkheid en rubricering en
- (data)classificatie in relatie tot risico- alsook incidentmanagement.

Verbanden & verschillen worden daarbij in beeld gebracht. In dit boek volgt de auteur vooral een procedurele benadering. Daarbij streeft hij naar een helicopterview, wat hij dan ook bereikt door middel van vergelijking van de gehanteerde begrippen bij de verschillende standaarden.
De auteur geeft als beperkingen aan dat het boek niet ingaat op privacyvraagstukken, aangezien het niet gaat om indirecte belanghebbenden, de burger, maar wel om de direct belanghebbenden te weten de overheid. Ook de maatregelen die genomen kunnen worden om de impact (van de schade) te beperken komen niet aan de orde.
Wat uit dit boekwerk blijkt is dat er vrijheid bestaat tot persoonlijke interpretatie, logisch beredeneerbaar vanuit het vertrekpunt dat belanghebbenden daar zelf niet éénduidig over zijn en de lezer niet per se een voltijds informatiebeveiliger is. Persoonlijke interpretatie van (onbepaalde (1)) termen/begrippen lijkt daarnaast inherent te zijn aan de rubricering (Staatsgeheim) en de positie van belanghebbenden (Staat en zijn bondgenoten). Zou wellicht ook afhangen van de situatie omtrent het te beschermen belang.
De auteur verduidelijkt ook het standpunt hoe bijvoorbeeld de Wet Openbaarheid Bestuur zijn beperkingen kent als gevolg van het wegen van het belang van het verstrekken van informatie versus de belangen van Nederland, haar publiekrechtelijke lichamen en bestuursorganen en andere staten en/of internationale organisaties.

Het boek gaat verder in op onder andere:
- een verbeterd begrippenkader;
- de relatie tussen dataclassificatie en risicomanagement en
- subtiele verschillen in definities en begrippen.

De tabellen, figuren en bijlagen geven een verhelderend overzicht. De auteur geeft voorts een handreiking aan de lezer door de beschikbaarstelling van een goed overzicht in de vorm van een spreadsheet met betrekking tot de bescherming van de belangen (2).

Persoonlijke beleving

Aanvankelijk is het boek wat moeizaam leesbaar, mede omdat bekendheid wordt verondersteld met het (overheids)begrippenkader. Later las het een stuk vlotter ook door een vlottere schrijfstijl. Inderdaad bereikt het boek dat een deeltijd informatiebeveiliger een helder overzicht wint aangaande de (gewenste) organisatie en de rubricering (vertrouwelijkheid) van informatie. Echter, het is niet direct een boek voor de beginner in het vak, terecht dat de auteur als subtitel vermeldt: ‘Hoe professionals in een organisatie samenwerken en de belangen van de organisatie worden beschermd’. Jammer is enkel dat de uitgever niet meer tijd heeft gestoken in de redactie van het boekwerk, nu bleven er storende tik-, taal- en grammaticafouten achter.

Referenties

1) Zie uitspraak van de HR der Nederlanden: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2016:168&showbutton=true&keyword=ECLI%3aNL%3aHR%3a2016%3a168

(2) Aanzet ‘spreadsheet’ bescherming van de belangen (afgeschermd, maar wel vrijelijk beschik- en aanpasbaar) onder:
http://www.researchgate.net/profile/Clemens_Willemsen

Auteur: Arash Rahmani helpt organisaties als externe adviseur of als ad interimmanager bij het ontwikkelen, beoordelen en implementeren van hun informatiebeveiligingsbeleid en -programma's. Arash is bereikbaar via arash@rahmani.nl.

De menselijke factor in informatiebeveiliging

In mijn vorige artikel (`Organisatiecultuur is essentieel voor informatiebeveiliging', iB-Magazine 2021 nummer 2), legde ik uit waarom organisatiecultuur essentieel is voor informatiebeveiliging. Informatiebeveiliging is niet alleen een technische kwestie, maar processen, mensen en cultuur spelen ook een belangrijke rol. In dit artikel geef ik een paar praktische tips om de digitale weerbaarheid van een organisatie te versterken.

"Wij zijn een organisatie die bestaat uit professionals en daarom is het bij ons niet nodig om aandacht te besteden aan mensen. Awareness is voor ons niet relevant omdat onze medewerkers professionals zijn." Dit zei de Chief Information Security Officer (CISO) van een groot technologie consultancybureau tegen mij. Een CISO met meer dan 15 jaar ervaring en die als techneut een tunnelvisie heeft met betrekking tot techniek en zeer weinig waarde hecht aan processen, mensen en cultuur. Zijn organisatie kwam in de media omdat medewerkers gevoelige gegevens van tientallen klanten online hadden gezet zonder enige vorm van een wachtwoord, encryptie of andere veiligheidsmaatregel. Deze gegevens waren in een openbare database voor iedereen toegankelijk. Een organisatie die alle technische mogelijkheden heeft om gegevens in een beveiligde omgeving op te slaan, met encryptie, access control en andere veiligheidsmaatregelen en tóch kozen de medewerkers desondanks voor een ongecontroleerde onbeveiligde online omgeving.

Vergeet mensen en cultuur niet

Als CISO is het jouw verantwoordelijkheid onder andere om de organisatie te beschermen tegen informatiebeveiligingsdreigingen en om een team neer te zetten dat in staat is om zo snel mogelijk de schade te beperken. Gelukkig hoef je

het wiel niet opnieuw uit te vinden en werken we in een branche waar een aantal tools bestaan om ons hierbij te helpen. Een dergelijke tool is het NIST Cybersecurity Framework (kort: NIST CSF). Een voordeel van de NIST CSF is dat het de flexibiliteit en mogelijkheden biedt om een Tiers-focus area te definiëren dat het beste past bij de behoeften van een organisatie. Het raamwerk kan worden aangepast aan de organisatie door het toevoegen, wijzigen of veranderen van categorieën en subcategorieën. Dat zorgt voor waardevolle discussies en inzichten, waar de organisatie en haar teamleden baat bij hebben. Hieronder een basisvoorbeeld van een implementation tier met als focus area mensen.

Framework Implementation Tiers

Focus Area: Mensen

Tier 1 Partial Implementation

- Het bewustzijn van informatiebeveiliging van medewerkers is zeer beperkt;
- De informatiebeveiligingsmedewerkers hebben beperkte cybersecuritytraining;
- Medewerkers zijn zich niet of nauwelijks bewust van de beveiligingsmiddelen en escalatiepaden van de organisatie;
- De CISO heeft geen training gevolgd op het gebied van governance en business.

Tier 2 Risk Informed

- Er is een bewustzijn van informatiebeveiligingsrisico's op organisatieniveau;
- De informatiebeveiligingsmedewerkers hebben cybersecuritytrainingen gevolgd;
- Medewerkers zijn zich in het algemeen bewust van de beveiligingsmiddelen en escalatiepaden van de organisatie;
- De CISO heeft trainingen gevolgd op het gebied van governance en business.

Tier 3 Repeatable

- Medewerkers krijgen regelmatig informatiebeveiliging gerelateerde trainingen, briefings en toetsingen;
- De informatiebeveiligingsmedewerkers beschikken over de kennis en vaardigheden om de aan hun toegewezen rollen en verantwoordelijkheden te vervullen;
- De organisatie en de afdelingen hebben toegewijde informatiebeveiligingsmedewerkers;
- De CISO volgt regelmatig governance en business gerelateerde trainingen.

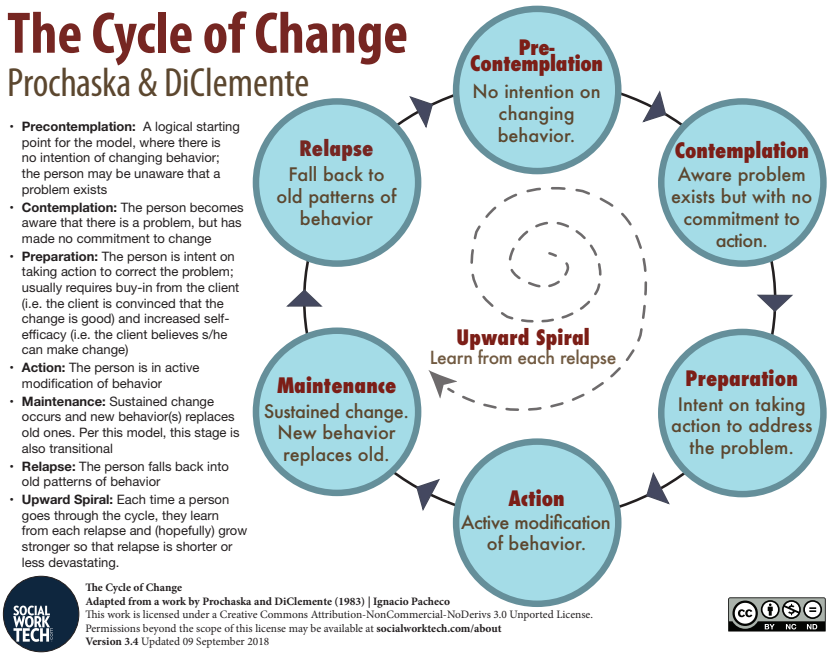
Tier 4 Adaptive

- Medewerkers krijgen regelmatig informatiebeveiliging trainingen, briefings en toetsingen over relevante en opkomende beveiligingsonderwerpen;
- De kennis en vaardigheden van de informatiebeveiligingsmedewerkers worden regelmatig getoetst op actualiteit en toepasbaarheid, en nieuwe vaardigheden en kennisbehoeften worden geïdentificeerd en aangepakt;
- Medewerkers zijn actief in overleg met toegewijde informatiebeveiligingsmedewerkers;
- De CISO heeft kennis en vaardigheden op het gebied van governance en business en volgt regelmatig interne en externe trainingen op deze gebieden.

Zorg voor een flexibel team en juiste houding

Incidenten zijn onvermijdelijk. Daarom is het belangrijk om maatregelen te nemen en een team te trainen voor voortijdige detectie en reactie. Zijn de incident response teamleden zich bewust van hun eigen specifieke rollen en verantwoordelijkheden en dat van hun teamleden? Zijn ze gedrild om te reageren op een incident? Hoe vaak heeft een organisatie een incident response simulatie? Wanneer was het de laatste keer dat het geen geplande simulatie was, maar een spontane? Hoe snel kan het team reageren tijdens vakanties en feestdagen of als er teamleden ziek zijn? Zijn de teamleden hiervoor getraind en worden ze hiervoor gecompenseerd? Is er binnen de organisatie bewustzijn, begrip en waardering voor de keren dat het team incidenten oploste voordat ze een probleem werden voor de organisatie? Of krijgt het team voornamelijk negatieve aandacht wanneer ze niet voldoen aan de verwachtingen of wanneer er schade is?

De houding van de organisatie, CISO, managers en teamleden zijn cruciaal. Beton is een geweldige uitvinding in de bouw, maar je hebt er weinig aan als het in de betonmolen of -wagen lang stilstaat en uitdroogt. Datzelfde geldt voor een CISO en zijn of haar team. Ongeacht je functie, is het voor een organisatie vaak ongezond wanneer medewerkers al tientallen jaren bij dezelfde organisatie werken en vastgeroest zitten in een tunnelvisie. Die tunnelvisie en gebrek aan flexibiliteit en juiste houding zorgen vaak voor een onbewuste toename van risico's.



Figuur 1 – The cycle of change. Licentie: Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. Bron: SocialWorkTech.com

Awareness is geen synoniem voor gedragsverandering

Uit verschillende onderzoeken, waaronder die van IBM (1), Kaspersky (2) en Proofpoint (3), blijkt dat de menselijke factor, veelal van interne medewerkers, de belangrijkste oorzaak zijn van informatiebeveiliging incidenten. Het is steeds vaker, sneller en gemakkelijker om met social engineering of menselijke fouten toegang te krijgen tot gevoelige en betrouwbare informatie. Social engineering gaat een nog grotere rol spelen bij security incidenten die impact hebben op de business. Neem bijvoorbeeld CEO-fraude, waarbij een medewerker op de financiële administratie van een bedrijf een e-mail van een directielid ontvangt om geld over te maken. Dankzij de steeds betere neurale netwerkarchitectuur voor spraaksynthese is het mogelijk om een organisatie te bellen en verzoeken in te dienen met een vertrouwde stem, zoals 'de stem' van de financieel directeur. De medewerker denkt dan dat het de financieel directeur is die belt met een dringend verzoek. Bij hoeveel organisaties is dit mogelijk omdat medewerkers onvoldoende controle hebben of de controles niet volgen? Vooral in coronatijd, wanneer mensen vanuit huis werken en fysieke conformatie niet mogelijk is, of wanneer een kwaadwillende weet dat de financiële directeur op vakantie is. Spraaksynthese en andere social engineering technieken gaan naar verwachting de komende jaren een veel grotere rol spelen dan organisaties beseffen.

Bewustzijn is maar één van de fases van gedragsverandering, met alleen bewustzijn kom je niet ver. De meeste mensen zijn zich er al jaren van bewust dat gezond eten en sporten gezondheidsvoordelen hebben. Een feit waar in de media veel aandacht voor is. Toch heeft, gebaseerd op cijfers van het RIVM (4), 1 op de 6 volwassenen in Nederland ernstig overgewicht (obesitas), terwijl dat 10 jaar geleden 1 op de 9 was en 30 jaar geleden 1 op de 16. Als je gedragsverandering wilt, focus dan daadwerkelijk op gedragsverandering in plaats van alleen awareness. Zorg dat medewerkers vanaf onboarding tot offboarding continu getraind worden om hun gedrag te veranderen. Doe dit in alle lagen van de organisatie en maak de training op maat voor de verschillende rollen en risico's. Er zijn meerdere gespecialiseerde bureaus die je hierbij kunnen helpen. Je hoeft dit niet alleen te doen.

Referenties

(1) IBM Cyber Security Intelligence Index - https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

(2) The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within https://www.kaspersky.com/blog/the-human-factor-in-it-security/

(3) Threat Report: The Human Factor Report - https://www.proofpoint.com/us/resources/threat-reports/human-factor

(4) https://www.volksgezondheidenzorg.info/onderwerp/overgewicht/cijfers-context/trends#node-trend-obesitas-volwassenen

Awarenesstest: kennis- of gedragsmeting?

Stel: je helpt een bekende Nederlander inchecken bij het hotel waar je werkt. Wat doe je?
a. Ik maak meteen een screenshot van zijn telefoonnummer
b. Ik maak stiekem een foto van hem en die app ik naar mijn vrienden
c. Ik check hem in net als alle andere gasten en doe verder niets
Beste securitywereld, hoeveel procent van de mensen zou op deze vraag níet antwoord c invullen?

Awarenessstests. Vaak uitgestuurd als goedbedoeld initiatief, maar ze dienen helaas lang niet altijd het beoogde doel. Het is interessant om zaken te meten, zonder twijfel. Alleen in het geval van mensen en menselijk gedrag is dat nog niet zo simpel. Mensen hebben namelijk de natuurlijke neiging tot het geven van 'het juiste antwoord'. We zien bovenstaande vraag en we weten wat het goede antwoord is. Dus dat klikken we aan. Dat betekent niet dat het ook iets zegt over het daadwerkelijke gedrag. De psychologie legt uit waarom:
Mensen zijn geen rationele wezens. Het kennen van de regel is niet hetzelfde als je eraan houden. Kijk naar het dagelijks leven; iedereen wéét inmiddels echt wel dat we geen telefoon mogen vasthouden in de auto, dat we anderhalve meter afstand moeten houden van anderen en dat je niet in het donker mag fietsen zonder licht. Maar laten we eens kijken naar daadwerkelijk gedrag: er worden nog steeds veel boetes uitgedeeld voor het 'vasthouden van een mobiel elektrisch apparaat tijdens het rijden', we krijgen continu berichten over handhaving van situaties waarin mensen te weinig onderlinge afstand houden, en de fietsers die ik 's avonds zie rijden, hebben helaas lang niet allemaal verlichting.

Als we deze zaken zouden uitvragen in een awarenesstest, is het dus maar de vraag of mensen het eerlijke antwoord geven, óf het antwoord waarvan zij denken dat het het juiste is. De psychologie leert dat het laatste vaker het geval is. Omdat we het graag goed willen doen, willen laten zien dat we het weten én omdat we de neiging hebben om sociaal wenselijke antwoorden te geven. Het is nou eenmaal lastiger om te zeggen dat je regelmatig appt in de auto dan om te zeggen dat je dat nooit doet (lijkt mij dan, maar ja, ik doe het natuurlijk nooit 😉).

Een awarenesstest is dus voornamelijk een kennismeting, geen gedragsmeting. En als we het als zodanig waarderen, is dat prima. Maar we moeten los van het feit dat we doen alsof een dergelijke vragenlijst weergeeft hoe de mensen in je organisatie zich daadwerkelijk gedragen. De test meet of mensen weten wat ze zóuden moeten doen. Niet wat ze doen. Overigens wel een belangrijk handvat voor verandering, want als jouw organisatie hoog scoort op een awarenesstest, dan weet je dus dat het aan kennis niet ontbreekt. Als je dan toch het gewenste gedrag niet terugziet, zit de oplossing dus ook in iets anders dan kennis zenden! Dat scheelt een hoop moeite die veel effectiever ingezet kan worden. Bijvoorbeeld door mensen te motiveren of faciliteren.
Ingewikkeld, de psychologie. Wel boeiend. En effectief!

Inge

Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.

Auteur: Robert Metsemakers schrijft op persoonlijke titel en is als ervaren IT-auditor en informatiebeveiligings-expert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

BLOG

Misplaatste metaforen van securitymanagers

Met metaforen kun je dingen aan managers uitleggen, projectmedewerkers motiveren en gedrag van eindgebruikers beïnvloeden, ook op het gebied van security. Maar het geeft alleen het beoogde resultaat als het bij de ontvanger opgeroepen beeld precies is wat jij als zender bedoelt.

It ain't over till the fat lady sings – Deze uitdrukking wordt vaak gebruikt om aan te geven dat de race nog niet gelopen is, omdat een bepaald iemand nog zijn/haar zegje erover moet doen. Of omdat de communicatie-campagne rondom het securityproject dat dreigt te mislukken, nog moet starten. Het eindresultaat van de audit, de nulmeting of de security self assessment kan nog alle kanten op, zeg maar.

Het is (a) een onheuse manier om over een zwaar gebouwde vrouwelijke collega of ariazangeres te spreken en (b) in een opera is een aria wel een belangrijk moment, maar niet het slotnummer van de voorstelling. De echte uitdrukking is 'it ain't over till the fat lady sinks' (met een letter k) en komt uit het 8-ball spel bij poolbiljart. Daar moet speler A met de witte speelbal de hele ballen (effen gekleurd, met nummers 2 t/m 7) in de putjes in de biljartrand spelen. Speler B doet dat met de halve ballen (met streep, nummers 9 t/m 16). Beide spelers moeten als laatste bal de zwarte '8' putten en die lijkt stilistisch een beetje op een dikke dame. Ook Britse bingomasters noemen het cijfer 8 zo – althans die enige keer dat ik in Blackpool op de boulevard was. De '88' heet daar 'two fat ladies' en de '22' 'two sitting ducks'.

Het gaat hier dus niet om communicatie of uitstel van een oordeel, maar om een duidelijke, onbetwistbare spelregel.

Zoals dat een kwetsbaarheid in software binnen je organisatie pas volledig is uitgebannen als alle apparaten, dus de eigen en BYOD, met die kwetsbaarheid zijn voorzien van de patch.

Van scratch af

Projectleiders beginnen in de kick-off vaak 'van scratch af' om te laten zien dat er een verse start wordt gemaakt en dat alles van de grond af moet worden opgebouwd. Soms zelfs opnieuw. Het lijkt op het 'om krediet vragen' bij een presentatie die je onverwacht van iemand moet overnemen: 'Het is mij een eer als vervanger deze presentatie aan u te geven, maar ik heb vanochtend pas gehoord dat ik'... Deze uitdrukking komt uit het golfspel. Daar moet de speler de eigen bal op elk van de 18 holes in zo weinig mogelijk slagen in het putje bij de vlag slaan. Na het aanleggen van de golfbaan speelt een aantal geoefende (professionele) spelers daar. Hun benodigde aantallen slagen worden gemiddeld en per hole berekent men zo de PAR (Professional Average Result). Heb je zelf minder slagen nodig, dan speel je onder PAR. Hoe méér minder slagen je nodig hebt, des te zeldzamer is de vogelnaam voor je bijzondere prestatie:

1. birdie
2. eagle
3. albatross (of double-eagle)
4. condor

De meeste amateurspelers hebben echter meer slagen dan PAR nodig. Om een wedstrijd tussen een beginnende en ervaren golfspeler toch spannend te maken, is de handicap bedacht. Dat zijn 36 slagen die je op 18 holes extra mag maken - zolang je nog niet zo goed bent in golf. Die handicap wordt van je score afgetrokken om een netto score te berekenen. Je kunt die handicap verlagen door een aantal Qualifying Scorecards (door je tegenspeler voor akkoord getekend) in te leveren. Je kunt een 'single digit' speler worden, met een handicap van 1 tot 9. Heel goede spelers komen zelfs op nul uit en spelen dus op professioneel niveau. Zij starten dan hun wedstrijden 'vanaf nul' en in golf noemen ze dat 'from scratch'. Deze uitdrukking betekent dus dat je héél goed bent in wat je doet en dat je juist niet vanuit een achterstandspositie vertrekt.

De meeste holes zijn PAR4. Langere zijn PAR5, kortere PAR3. Daarvan zijn twee slagen gereserveerd voor het eindspel op de green (het kort gemaaide gras rondom het putje). Eentje om bij het putje in de buurt te komen en de tweede om de bal er volledig in te tikken. Tip van mij: doe dit niet nonchalant met één hand en achterstevoren. Op een PAR3 hole houd je één slag over om vanaf de tee (de afslagplaats) op de green te komen. Reserveer ook in elk securityproject aan het eind voldoende tijd voor het evalueren van je fouten, delen van lessons learned en het schrijven van een leuk stukje op de intranetsite over de nieuwe USB-dongle.

Op zijn elfendertigst

Meestal krijgen de uitvoerders van een project te horen dat iets door hen niet 'op zijn elfendertigst' moet worden uitgevoerd. De projectleider bedoelt dan 'uitermate langzaam en omslachtig'. Veel mensen denken namelijk dat deze uitdrukking teruggaat op de trage manier waarop de Staten van Friesland overlegden. Deze Staten bestonden uit de afgevaardigden van 11 steden (van die schaatstocht) en 30 grietenijen (gemeten van het eind van de 16e eeuw tot 1851). Een grietenij is een voorloper van de Nederlandse gemeente, met name in Friesland. In de Groninger Ommelanden noemde men rechtsstoelen of plaatselijke rechtbanken ook zo. Het woord betekent 'bestuursgebied van een grietman'. 'Grietman' was een openbaar aanklager en verwijst naar het Oudfriese 'greta', dat aanklagen betekent. Greta Thunberg: what's in a name?
Leuk gevonden, maar onwaarschijnlijk. Volgens het Groot Uitdrukkingenwoordenboek van Van Dale (2006) had 'op zijn elfendertigst' oorspronkelijk juist een gunstige betekenis: 'keurig, netjes'. De elf-en-dertig was een weefkam voor het weven van zeer fijn textiel waar 41 (ja, ja) gangen doorheen gingen en 4.100 draden doorheen geschoven konden worden. Zo'n kam was een van de fijnsten die er bestonden en dit weverswerk vereiste precisie (1); vandaar de originele betekenis 'keurig'. Kies je metaforen goed. Want voor een intelligente, dus taalgevoelige, visueel denkende, zeer precies werkende security analist is het verwarrend als de 'baas' aan het begin van een project stelt dat het werk 'slordig, onnauwkeurig en met fouten' moet worden uitgevoerd.

(1) Werken met de elf-en-dertig was ook tijdrovend; daardoor ontstond de latere betekenis 'langzaam en omslachtig'.

Authors: Reinder Wolthuis, senior consultant/project manager cybersecurity at TNO. Can be reached at reinder.wolthuis@tno.nl.
Frank Fransen, senior scientist cybersecurity at TNO. Can be reached at frank.fransen@tno.nl.

SOCCRATES - Security automation in SOC & CSIRT environments

SOCCRATES (SOC & CSIRT Response to Attacks & Threats, based on attack defence graphs Evaluation Systems) is a European innovation project, co-funded by the Horizon2020 program and led by TNO. It brings together some of the best European expertise in the field to develop, implement and evaluate an automated security platform to support SOC analysts. This first article provides an introduction to SOCCRATES, in two follow-up articles we will highlight the underlying concepts.

Over the past years, the cyber threat landscape has greatly evolved. Advanced cyber-attacks are now conducted by professional threat actors that have substantial resources and (technical) capabilities. Such attacks are often targeted in nature and may involve a great degree of automation, persistence and (technical) sophistication. Meanwhile, the dependency on Information and Communication Technology (ICT) and thus the potential impact of any cyber-attack is ever increasing. Combined with the continuously evolving ICT infrastructures with diverse and emerging technologies (e.g. Internet of Things (IoT)), organisations are faced with a challenging task.

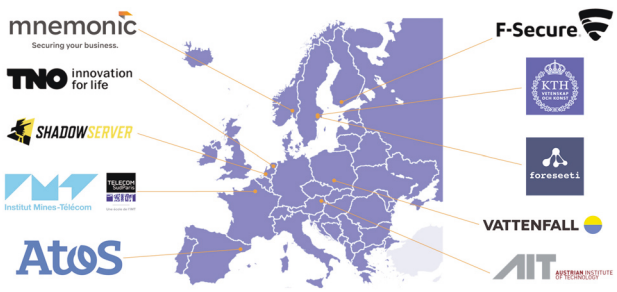


Figure 1 – The SOCCRATES partners.

To deal with these challenges, many organisations have increased their effort in security monitoring and incident response. Many organisations have setup internal Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) to perform these tasks, others outsourced these tasks to a Managed Security Service Provider (MSSP). In recent years, these security operation activities have been extended with collection and processing of Cyber Threat Intelligence (CTI), to anticipate upcoming threats and take appropriate precautions. Although security operations have gotten more attention over the years, these SOCs and CSIRTs (both internal and MSSP) are faced with complex challenges:

Improve and extend detection capability. Threat agents (attackers) continuously evolve and improve their Tactics, Techniques and Procedures (TTPs), including stealth techniques. The SOCs consequently need to improve the detection capability and coverage with more advanced techniques that assist the analyst in discovering indicators in a massive amount of data while reducing the number of false positives.
Automate the CTI process. As the amount of available CTI is increasing and the value of a large portion of that CTI is limited to a short time span, it is becoming more important to automatically assess and apply mitigation strategies to these threats.

Understand the ICT infrastructure. Simply put; you cannot defend what you don't know. As SOC analysts need to interpret and understand the detected security events, insight in the continuously evolving ICT networks and systems is essential. The SOC analyst also needs to understand the critical attack surfaces, attack vectors that may lead to a compromise of critical business assets as well as defence mechanisms deployed to counter attacks.
Assess business impact of an incident. In addition to understanding the ICT infrastructure, the SOC analyst needs to be able to assess the potential impact on the business of an ongoing attack or emerging threat. Business processes thus need to be mapped on the ICT infrastructure components, and insight in the consequences of a breach of confidentiality, integrity and/or availability of system resources or information assets needs to be (near real-time) available.

Recommend Course of Actions (CoAs). When faced with an attack or emerging threat, the SOC analyst needs to identify possible responses and determine which response is the best given the ICT infrastructure, available (on demand) reconfigurable security functions, and the effect on the business.

How SOCCRATES addresses these challenges

The Project

The SOCCRATES consortium is a collaboration of 10 partners across Europe (see figure 1), each with a different perspective (university, knowledge institute, end user, Managed Security Service Provider (MSSP), vendor) and providing unique contributions.

The main SOCCRATES objective is: 'Develop and implement a Security Decision Support framework that enhances the effectiveness of SOC and CSIRT operations.' The results specifically targeted at end user's inhouse SOC and Managed Security Service Providers (MSSP) that provide SOC services. The project has a total budget of 5.9 Million Euro for three years.

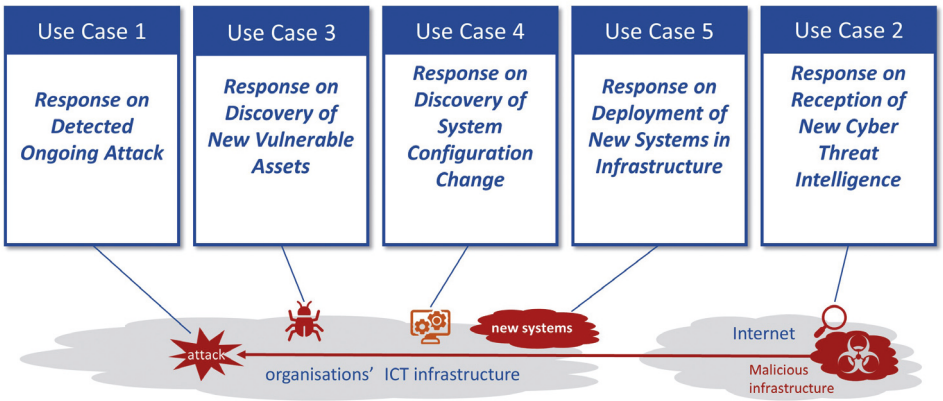


Figure 2 – The SOCCRATES use case.

The Use cases

The work in SOCCRATES is based on five different use cases, see figure 2:

- **Use Case 1: Response on Detected Ongoing Attack**
  Detect ongoing attacks and automatically analyse the attack, automatically determine the best response, and initiate deployment of the selected response.
- **Use Case 2: Response on Newly Received Cyber Threat Intelligence**
  Continuously collect new threat information, automatically analyse the potential business impact and determine best options for proactive mitigation.
- **Use Case 3: Response on Newly Discovered Vulnerable Assets**
  Automatically detect vulnerabilities on assets in the ICT infrastructure, assess if they enable new attack paths, determine and initiate mitigation actions.
- **Use Case 4: Response on Discovered System Configuration Change**
  Automatically detect configuration changes on assets in the ICT infrastructure, assess if they enable new attack paths and determine if action is needed.
- **Use Case 5: Response on Deployment of New Systems in Infrastructure**
  Automatically detect introduction of new systems to the ICT infrastructure. Automatically assess the new situation and determine if (additional) security measures are needed.

The use cases are used to derive requirements for the platform and to define KPI's for the evaluation of the platform.

The Platform

The integrated Security Decision Support framework will consist of a platform with a modular set of components with standardized interfaces and a central orchestration function, see figure 3:

The SOCCRATES platform will have the following capabilities:

1. **Automated discovery and modelling** of an organisation's technical assets to provide an accurate, machine-readable description of the ICT infrastructure;
2. **Detection of (sophisticated) cyber-attacks**, even in the case of encrypted network traffic, by applying advanced data analytics techniques (including AI and deep learning) on large amounts of network and log data;
3. **Attack simulation** by means of Attack Defence Graph (ADG) based analysis on a model of the ICT infrastructure (both before and during an attack), and determination of the best response to these threats and attacks;
4. **Quantification of the (potential) business impact of emerging threats and ongoing attacks** by means of business impact modelling and appraisal of business trade-offs in possible mitigations;
5. **Cyber Threat Intelligence (CTI) utilization** in incident detection, analysis and response, including Adversary Emulation Plans to enable threat actor specific attack simulation with Attack Defence Graphs;
6. **Identification, classification, and prediction of malicious activities and trends** through automated analysis on large amounts of malicious infrastructure and malware forensic data.
7. **Plan and enable automatic execution of Courses of Action (CoAs)**, while including humans in the loop for authorization or manual reconfiguration, by supporting open standards for security automation (i.e. OpenC2 (1) and CACAO (2)).

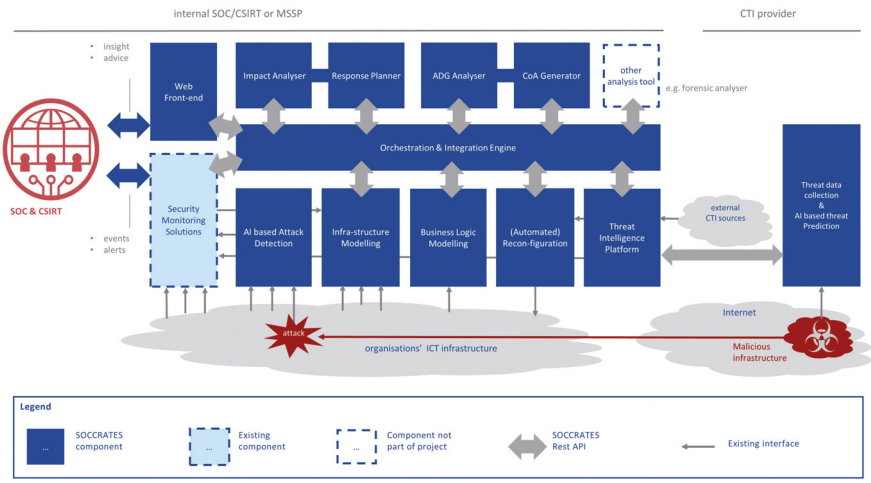


Figure 3 – The SOCCRATES platform.

The platform is a mix of technical innovations; both completely new innovations and innovations on already existing products. The platform is being built in three iterations between 2019 and 2022.

It has several components. The central component is the Orchestration and Integration Engine that facilitates communication and exchange of information between components and orchestrates the actions undertaken by the SOCCRATES platform when it is triggered.

Underneath the Orchestration and Integration Engine all components are presented that directly interact with the ICT infrastructure of an organisation or collect (threat) intelligence from external sources (e.g. the Infrastructure Modelling Component and Threat Intelligence Platform). Above the Orchestration and Integration Engine the analysis components are shown (i.e. Impact Analyser & Response Planner, ADG Analyser & CoA Generator, and other analysis components). The SOC and CSIRT teams that are envisaged as primary users of the platform are shown to the left of the Orchestration and Integration Engine, as are the organisation's existing Security Monitoring Solutions. Although these Security Monitoring Solutions are not part of the SOCCRATES platform, they are able to trigger and interact with it.

The Threat Data Collection & Threat Prediction component (see figure 2, shown on the right) resides at an organisation that specialises in analysing malicious infrastructures. This component is thus outside the scope of the SOCCRATES platform itself, which is typically operated by a corporate SOC or MSSP. It does, however, interact closely with the SOCCRATES platform via the Threat Intelligence Platform (TIP), one of the native SOCCRATES platform components.

The Evaluation

The SOCCRATES platform will be evaluated in three pilots. The SOCCRATES platform will be implemented at managed security service provider mnemonic and at the corporate ICT SOC of Vattenfall. In addition, Shadowserver (CTI collection, processing & analysis) will provide the pilots with CTI. We have defined specific KPI's that will be assessed during the pilots.

The first two pilots will be closed because they will handle confidential customer data. The third (demo) pilot specifically is targeted at demonstrating the usefulness of the SOCCRATES platform to a wider audience. The site for the demo pilot is yet to be determined, and the decision will be based on experiences from the previous pilots.

The Results

The main target groups for SOCCRATES results are:

- Managed Security Service Providers (MSSPs);
- Security Operations Centres (SOCs);
- Cyber Security Incident Response Teams (CSIRTs);
- National Certs;
- Security Product Vendors;
- Regulatory bodies;
- Policy makers;
- Standardisation bodies.

Considering the wide variety of the target group, we utilize different communication channels, such as webinars, conference presentations, workshops, demonstrations, the SOCCRATES website, social media, video. One of the goals here is to raise awareness among the target groups on how to improve SOC/CSIRT operations with SOCCRATES results and disseminate project results to relevant target groups and

potential users of the SOCCRATES Platform and components. Concrete examples are the SOCCRATES introduction video (3) and accepted presentations on the 2021 One conference and the prestigious FIRST (Forum of Incident Response and Security Teams) annual conference.

Another objective is to ensure active exploitation of SOCCRATES results. SOCCRATES is a so called 'Innovation action' and is expected to deliver results on Technology Readiness Level (TRL) up to 6 (System Adequacy Validated in Simulated Environment), but we anticipate that some results will even be on higher level. The integrated SOCCRATES platform will consist of a mix of commercially available components and Open Source components. We do not foresee actual commercial exploitation of the entire platform. Commercial exploitation will most probably only be done by individual partners on a module basis. The platform should be seen as an example for automation in security operations and inspire SOCs, CSIRTs and security product vendors. With the SOCCRATES innovation results, individual partners will be able to enhance their existing products and consequently improve commercial exploitation of those products.

SOCCRATES has adopted an active Open Source approach, in which we utilize the existing open source channels of all partners to publish the results that are available as Open Source. The Adversary Emulation Planner is already available (https://github.com/mnemonic-no/aep).
Finally, in the end phase of the project we will define more concrete exploitation activities for after SOCCRATES has ended which will include (besides the commercial exploitation and Open Source results) also activities such as education and further research. For the last item we will prepare a vision paper.

The Involvement

In order to have a project sounding board and interaction with the real experts in the field we have arranged two different bodies to support us in this:

- SOCCRATES Advisory board - The SOCCRATES Advisory Board (SOCAB) forms an independent review group of external (non-funded) experts within relevant areas. SOCAB members provide external reflection on the operational and strategic direction of the project and are invited to visit project events, will contribute to the requirements, and review project results. We have 4 experts in the field from different areas as member in the Advisory Board.
- Stakeholder group - The SOCCRATES Stakeholder Group is a group of people working at SOCs, CSIRTS, National CERTs, MSSPs, end-users and vendors that have indicated to be interested in the results of the project. They will be informed about progress, encouraged to provide input and be invited for SOCCRATES events. The Stakeholder Group also is important for the exploitation of project results, where we expect some of the members to become early users of SOCCRATES results. We currently have 26 members of 24 different organisations and are still expanding our group. If you want to become a member, it's free! Please contact us.

Current status

At this moment, we are already more than halfway of the project. The first half of the project mainly focussed on innovation, design and implementation. The second half of the project will be more focussed on evaluation and exploitation of results. We are well on track with delivering the results we promised in our original planning. The main evaluation pilot will start at the beginning of 2022.

Lookout to next articles

In the coming articles (next editions of the PvIB magazine) we will zoom in on some of the SOCCRATES platform underlying technology and innovations and the challenges we encountered.
More info at www.soccrates.eu

SOCCRATES has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No. 833481.

References

(1) https://openc2.org/ and https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2
(2) https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao
(3) https://vimeo.com/442734821

COLOFON

IB is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

PvIB
Platform voor InformatieBeveiliging

HOOFDREDACTEUR
Nicole van Deursen

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

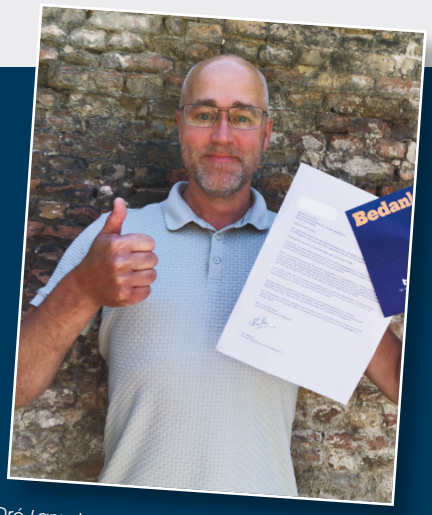
UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2021 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

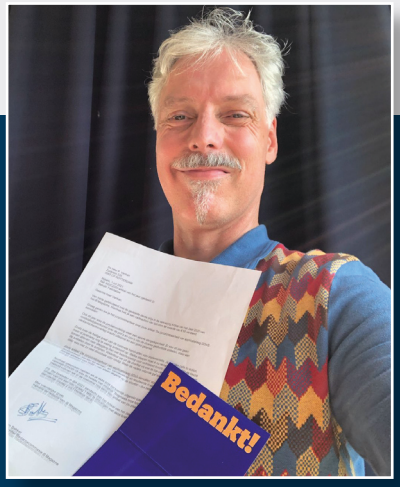
ABONNEMENTENADMINISTRATIE
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl

ISSN 1569-1063

Joost Geerts



Dré Lameir



Paul Vankan

Artikel van het jaar 2020

Ook dit jaar was de jurybeoordeling weer een aparte aangelegenheid. Geen rondetafelbijeenkomst over de pro's en con's van de diverse geshortliste artikelen, maar een vierkantschermoverleg bracht uitkomst en een goed gesprek. Zoals over de heilige graal van de concrete handvatten voor implementatie. Ja, we zien calls to action, maar al jarenlang nog te weinig antwoord op: welke stappen moet ik nu nemen?

Gelukkig lijkt de keuze tussen streven naar diepgang dan wel beschouwing en verfrissend inzicht, wel degelijk steeds beter in de artikelen door te schijnen. Waardoor we uit de shortlist vrij snel de top vier konden selecteren; daar was niet zo veel discussie voor nodig. Maar de nadere volgorde gaf wat debat.

Ex aequo - Paul Vankan en Dré Lameir

Dat resulteerde in een ex aequo derde plek voor FOMI (Fear of Missing Out) van Dré Lameir, en De (on)zichtbaarheid van applicatielaag DDoS-aanvallen van Paul Vankan. Beide scoren hoog op punten als: leesbaarheid, zet aan tot denken, en vernieuwend. Net als alle andere artikelen uit 2020 – niet alleen die op de shortlist – zijn dus beslist het nalezen waard! Echter, we zoeken altijd naar het stukje *je ne sais quoi* dat van een goed artikel een topper maakt, en dat troffen we bij de andere twee nog iets meer aan.

Runner-up - Robbin Begeer en Lex Borger

De jury oordeelde dat de runner-up dit jaar een behoorlijk vernieuwende aanpak presenteerde, die we graag veel meer zouden willen zien in ons vak. Cijfermatige analyses geven veel duidelijker inzicht dan kwalitatieve analyses alleen. Maar… zoals in Japan de beste scholieren het meeste commentaar krijgen omdat zij het waard zijn om verbetermogelijkheden aangereikt te krijgen, zo vond de jury na enig speurwerk toch nog een paar kleine dingetjes. Hetgeen onverlet laat, dat we het artikel inhoudelijk én naar onderzoeksopzet beslist aanraden om te bestuderen, om niet alleen iets met de conclusies te doen maar ook om het onderzoek uit te breiden naar andere relevante gebieden zodat ons vakgebied een betere, solider basis kan krijgen. Gewoon, omdat de vorige zin te lang was voor begrijpelijkheid. We hebben het immers over het artikel: Duidelijke en eenvoudige taal. Hoe beoordeel je die? door Robbin Begeer en Lex Borger.

Winnaar 2020 - Joost Geerts

Ook bij de uiteindelijke winnaar zochten we naar dat soort plusminnetjes terugtellend vanaf de perfecte 10. We vonden er nóg minder. Ook dit artikel opent de blik naar een groot, en nog veel te weinig bekend, onderzoeksterrein. Ja, OT is al eerder in beeld gekomen. Maar we denken nog veel te snel in termen van 'Oh ja, doe maar een framework-standaardje à la IEC 62443 dan zijn we er wel zo'n beetje'. Terwijl we nog te weinig diepgaand en nog veel te weinig in een praktische context hebben onderzocht wat er echt aan de hand is. Dit artikel doet dat wel, bottom-up. Dat klinkt soms wat eenvoudig als 'leuk voorbeeld, maar elders niet toepasbaar' — maar in het artikel wordt juist duidelijk dat de methoden van onderzoek en de vertaling van methoden en conclusies naar allerlei andere deelgebieden, juist heel goed kan. Én hard nodig is, omdat de IT-ontwikkelingen in (hier) de automotivewereld hard gaan, maar security er nog lang niet up to speed is. AI helemaal niet in brede zin. Daarmee is Hacker gehackt van Joost Geerts de winnaar van dit jaar.

Vakbreed interessant

In het artikel wordt uiteengezet hoe een technische security maatregel als een tachograaf op zichzelf ook weer hackgevoelig is en hoe vervolgens die hack dan weer aan te pakken is. Is dat dan zo breed inzetbaar? Jazeker wel. Omdat het toont dat iedere maatregel weer zwaktes kent en niet op zichzelf kan staan. En hoe ingewikkelder we het maken, hoe meer mogelijkheden we creëren voor uitschakeling, ondermijning en misbruik van juist de maatregelen die ons zouden moeten beschermen. In de complexiteit zien wij nog nauwelijks de bomen door het bos, terwijl we alle bomen en het bos in de gaten moeten houden. Dat vergt, zo zien we in het artikel, doorbijten in de materie om er wijzer van te worden. Zo'n onderzoek goed onder woorden brengen is een kunst – hier is het gelukt.

De jury feliciteert de winnaar van harte met dit mooie resultaat! Laat het een aanmoediging zijn voor meer afstudeerders om hun talenten in onderzoek en schrijverschap om te zetten in vakbreed interessante en leesbare briefings voor collega's.

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

AP: Google Workspace Education voldoet niet aan AVG-regels. Wat nu?

Begin juni 2021 kwam naar buiten dat de vastgestelde privacyrisico's van Google Workspace for Education zijn voorgelegd aan de Autoriteit Persoonsgegevens (AP) en dat zij deze risico's hoog opneemt. Google heeft in Nederland tot aan het begin van schooljaar 2021/2022 de tijd gekregen om maatregelen te treffen. Als dat niet lukt, zal het advies zijn om het gebruik van Google Workspace for Education te staken en kan de AP handhaven. Ondertussen moeten scholen zich beraden op een alternatief scenario – met nog een paar weken voor het einde van het schooljaar. Is er überhaupt een alternatief?

De AP heeft niet zelf onderzoek uitgevoerd en baseert in deze haar oordeel op de aangeleverde DPIA-resultaten en een schrijven vanuit het ministerie OCW. Uit de DPIA heeft de AP twee risico's uitgelicht waarvan zij aangeeft dat deze ertoe leiden dat de verwerking niet verenigbaar is met de AVG. Er kan niet eenduidig worden bepaald wie verwerkingsverantwoordelijke en wie verwerker is. Google geeft aan in gevallen verwerkingsverantwoordelijke te zijn, terwijl dat niet vaststaat. Daarnaast is Google niet transparant over welke persoonsgegevens ze verwerkt en ontbreekt het aan duidelijke grondslagen voor die verwerkingen. Gevolg hiervan is een advies aan onderwijsinstellingen om de dienst voorlopig niet te gebruiken. In juli 2019 verbood de Duitse deelstaat Hessen al eerder het gebruik van Microsoft Office 365 door scholen. De lokale toezichthouder HBDI meldde: '… dat wat voor Microsoft geldt, ook van toepassing is op de cloudoplossingen van Apple en Google. De cloudoplossingen van deze providers zijn tot nu toe niet transparant en inzichtelijk' (1). Bianca Brooijmans

Privacy is een grondrecht! – Fook Hwa Tan

Onlangs hebben we gehoord dat onze toezichthouder Google op de vingers heeft getikt vanwege privacy issues met betrekking tot hun Google Classroom product. Dit product is mede dankzij COVID-19 afgelopen jaar door vele onderwijsinstellingen ingezet. Naast gebruikersgemak speelt natuurlijk de prijs een grote rol. In het afgelopen jaar is privacy meerdere keren een uitdaging geweest, ook in de strijd tegen de pandemie. Hierbij kun je denken aan de coronamelder, maar ook aan het coronapaspoort. Hoe belangrijk is je privacy? Sommige mensen, slachtoffers van identiteitsfraude, kunnen je goed vertellen waarom privacy van belang is. We zien echter ook vele organisaties profileringen uitvoeren op verzamelde data van ons. Hiermee kun je vaak zelfs benadeeld worden zonder dat je weet waarom. Met nieuwe Europese wetgeving is een stap gezet om de privacy van burgers zo goed mogelijk te beschermen. We horen dat de autoriteit meer handhaaft en ook steeds meer middelen krijgt om te handhaven in Nederland. Dit zie je ook tot uiting komen in de verschillende boetes die zijn opgelegd de afgelopen tijd. Zo ook voor Google. Aan de andere kant kan ik me goed voorstellen dat functionaliteit, gebruikersgemak en natuurlijk ook de prijs die voor een product betaald moet worden voor sommige organisaties van groter belang is. Deze organisaties gaan er soms ook te vanzelfsprekend vanuit dat een leverancier van zo'n omvang zich houdt aan de lokale wetgeving. Ook omdat deze organisaties vaak zelf de kennis niet in huis hebben. Wat nu

Fook Hwa Tan | Lilian Knippenberg | Chris de Vries | Bianca Brooijmans

daarom van belang is om ons grondrecht te beschermen, is dat of grote leveranciers buiten Europa zich houden aan de AVG of dat er binnen Europa (mogelijk gesponsord) een Europees product wordt ontwikkeld met dezelfde of zelfs betere functionaliteit voor een lage prijs die wel voldoet aan privacywetgeving. Het is vaak uiteindelijk een keus van de gebruiker om onbewust privacy op te offeren!

Geschaad vertrouwen en samenwerking als oplossing – Lilian Knippenberg

Waar voorheen met name het standpunt leek te gelden dat de klant/opdrachtgever van de leverancier de eind-verantwoordelijke was voor 'alles', gaat met de AVG terecht meer aandacht uit naar de verantwoordelijkheid die de leverancier heeft. In dit geval blijkt ook weer: de samenwerking tussen leverancier en klant is gestoeld op vertrouwen dat de ander zijn rol pakt. Zeker met als basis de verantwoordelijkheden die verwerkers krijgen in de AVG, is het voor opdrachtgevers makkelijker geworden om ook naar deze verantwoordelijkheden te verwijzen in contracten. Daarbij blijft natuurlijk wel staan dat de opdrachtgever verantwoordelijk blijft voor het uitzoeken van haar leveranciers. Door een goed proces aan de voorkant, met een risicoanalyse en toets van de leverancier, kunnen opdrachtgevers aan die verantwoordelijkheid voldoen. En natuurlijk komt daar ook lef bij kijken: het lef van informatiebeveiligers en/of privacy officers om een negatief advies neer te leggen en het lef van de proceseigenaar om dan een andere leverancier te zoeken. Terug naar deze casus. Hierbij ontstaat direct een probleem als de grote giganten niet blijken te voldoen aan hun verplichtingen op privacygebied. Het vertrouwen blijkt onterecht. Ik ken deze markt van leveranciers niet, dus ik weet niet of er goede alternatieven beschikbaar zijn en de tijdsdruk voor het nieuwe schooljaar maakt dit vraagstuk nog lastiger. Wat ik hoop dat er gaat gebeuren is samenwerking, buiten de wellicht ijdele hoop dat deze specifieke leveranciers hun verantwoordelijkheid gaan nemen. We hebben te maken met een aantal internationale leveranciers (Google en Microsoft), dus de Europese toezichthouders zouden moeten samenwerken om iets gedaan te krijgen. Daarnaast is een dergelijk complex vraagstuk bij uitstek waar de brancheverenigingen hun krachten kunnen bundelen. Van de PO-raad (basisonderwijs) en de VO-raad (voortgezet onderwijs) tot aan de MBO-raad, vereniging Hogescholen en de Vereniging samenwerkende universiteiten (VSNU): alleen als zij de krachten bundelen en kennis delen, kunnen we een oplossing vinden die de privacy van onze kinderen en (jong-)volwassenen goed beschermd. Is er een alternatief? Natuurlijk! Desnoods terug naar pen en papier.

Een tweerichtingenstrijd – Chris de Vries

Op deze plaats heb ik al vaker de lans gebroken voor een versterking van het Europees, lees Rijnlands, denken! Dit denken baseert zich op een naoorlogse ontwikkeling binnen met name drie Europese landen, t.w.: Frankrijk, Duitsland en Nederland; die ervan uitgaat dat aan het Angelsaksisch denken weliswaar veel meetbare (kwantificeerbare) voordelen kleven, maar ook grote nadelen. Het Rijnlandse denken baseerde zich al op sociaal-maatschappelijke verantwoordelijkheid (SDG's), duurzaamheid, transparantie ('governance') en democratische participatie van de werknemers voordat deze termen modieus werden. Deze drie landen vormden een ideale Europese rollencombinatie:

- Frankrijk de ideeëngenerator, de innovator;
- Duitsland de efficiënte producent met logistieke – en normvaardigheden en
- Nederland de verkoper van die op DIN-norm gebaseerde producten.

Google (machtiger en rijker dan de Nederlandse staat!?) en de Autoriteit Persoonsgegevens (AP) strijden vanuit twee opponerende denkrichtingen. Een strijd tussen puur kapitalisme versus het Europees 'socialistisch'(!?) denken. Kapitalisme vanuit de overtuiging dat maximale winst nastreven bestaat naast het morele besef om te zorgen voor de burger zo niet de mensheid (de 'invisible hand', Keynes) versus socialisme (Amerikanen vertalen dat als communisme) dat zegt dat er een overheid moet zijn die juist de belangen van de burger beschermt tegenover het bedrijfsleven.

Conclusie: het advies van de AP richting de onderwijsinstellingen is te slap, een verbod hoorde op zijn plaats. Het alternatief ligt in Europa en wordt het programma Horizon Europe genoemd en de EIT strategie 2021-2027 (2) en daarbinnen specifiek het Higher Education Institute initiatief (3) en in meer algemene zin Work Package 5 'Integration of emerging new technologies into education and training' (4).

Referenties

(1) Hessische Beauftragte für Datenschutz und die Informationsfreiheit

(2) https://eit.europa.eu/who-we-are/eit-glance/eit-strategy-2021-2027

(3) http://eit-hei.eu/

(4) https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-5-culture-creativity-and-inclusive-society_horizon-2021-2022_en.pdf

YOUR CLOUDS. YOUR DATA. YOUR KEYS.

OUR DATA PRIVACY SOLUTION.

Maintain the privacy, security, and integrity of sensitive data, systems, and encryption keys across your cloud platforms with Enturst nShield as a Service. Whether you use Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), or Salesforce, you can rely on nShield as a Service to provide complete cryptographic capabilities from FIPS- and Common Criteria-certified hardware security modules, without the need for on-prem maintenance:

- Key generation and protection
- Compliance with industry and regulatory mandates
- Containerized application development

NEW INTEGRATION: Keep your most sensitive data private in Microsoft Azure Information Protection with Entrust Double Key Encryption.

LEARN MORE AT ENTRUST.COM/HSM

ENTRUST

SECURING A WORLD IN MOTION