INFORMATIEBEVEILIGING
MAGAZINE

- Hoe Meta met één advertentie gedreven bedrijfsmodel op twee manieren onrechtmatig handelde
- Interview met Winn Schwartau: The Metawar Thesis
- **Blog:** Hoe je zelf een podcast maakt over informatiebeveiliging

JAARGANG 23 - 2023 - EDITIE 6

ISOPlanner

Eenvoudig Compliance Management in **Microsoft 365**

Waarom Microsoft 365?

Simpel: benut de kracht van Microsoft.

- Iedereen heeft Outlook en Teams. Naleving van compliance wordt als onderdeel van het werk ervaren.
- Vertrouwelijke gegevens zoals beleidsdocumenten en bewijsmateriaal blijven in jouw omgeving.
- Je lift vanzelf mee met innovaties. Bijvoorbeeld detectie van kwetsbaarheden en het automatisch ophalen van bewijs.

ISOPlanner is de enige integrale compliance oplossing in Microsoft 365. ISOPlanner brengt ISO naar jouw medewerkers toe en zorgt voor betere acceptatie en borging van informatiebeveiliging in jouw organisatie. Uiteraard ook voor de overheid (BIO), zorg (NEN7510) en de NIS2.

Snelle implementatie van je ISMS door meegeleverde voorbeeldmaatregelen, templates en voorbeelddocumenten.

SPIE NL IT heeft de ISO 27001 certificering met een positief resultaat doorlopen. Wat mede heeft bijgedragen aan dit mooie resultaat was de inzet van ISOPlanner als ISMS.

Leon van der Valk
SPIE Nederland B.V.

Kijk op **www.isoplanner.app** voor meer informatie en jouw gratis proefperiode.

ISO 27001 2023 COMPLIANT

GDPR 2023 COMPLIANT

PENTEST 2023 SECURE

De wereld staat niet stil

Chris de Vries

Elke dag ervaren wij allen, gebeurtenissen die schokkend kunnen zijn, plezierig, verrassend of bedreigend. Europa heeft dan ook met de NIS2-richtlijn een antwoord willen geven op bedreigingen welke de Europese lidstaten digitaal of economisch kunnen raken. Het gaat dus om weerbaarheid. In Nederland moeten wij dit gaan opnemen in onze wetgeving. En zo verandert onze werkelijkheid.

À propos, werkelijkheid …, weten wij eigenlijk wat dat is? Zie de Big Tech en hun streven naar gedragsmanipulatie van de mens, naar het onmerkbaar in bezit nemen van ons bewustzijn en de werkelijkheid en zo dat te veranderen in het door hen gewenste verdienmodel. Zie het interview van 12 oktober jl. met Winn Schwartau, de spreker op onze bijeenkomst in Utrecht van 9 mei 2023.

En ja, als wij het hebben over die werkelijkheid, hoe past daarbinnen onze zicht op privacy en dat wij vrije wil hebben en dat ons niets ergs zal overkomen, want wij doen toch niets fouts? Verdiep je dan even in de reacties van onze redacteuren, die het thema Client-Side Scanning (CSS) hebben opgepakt. Eén verkeerd geïnterpreteerde fotootje van de eigen kinderen kan tot registratie leiden, een onderzoek van de politie en de opname van de foto (en wat nog meer) in de databestanden van Interpol, Europa en waar en voor hoelang nog elders?

Privacy is ook het thema van ICT en Recht. De 'Meta' casus wordt besproken waarbij dit Big Tech bedrijf voor de rechter bakzeil moest halen. Dit vanwege haar niet transparante, algemene voorwaarden waarmee zij van cliëntdata een verdienmodel maakten, welke de toets der kritiek niet doorstond. Het is wellicht wat slikken voor niet-juristen, maar het artikel zegt heel veel waarover wij bij de AVG en met het oog op transparantie moeten letten.

Er is eigenlijk heel veel te zeggen over alle artikelen van deze omvangrijke uitgave van ons magazine. Ik wil zeker nog even aandacht vragen voor Robert Metsemakers blog over 'Podcasts' en André Beertens artikel over 'MMA: het register'. Ook attendeer ik op de LinkedIn pagina van onze vereniging alwaar het 'Achter Het Nieuws' CSS-artikel al op voorhand was geplaatst en de vragen welke uit het Meta-artikel daar gesteld zijn. Wij blijven de interactie met jullie zoeken en daar horen dit soort experimenten bij!

Laat van jullie horen. Wij wensen jullie inspannend en toch goed leesplezier.

Chris

IN DIT NUMMER

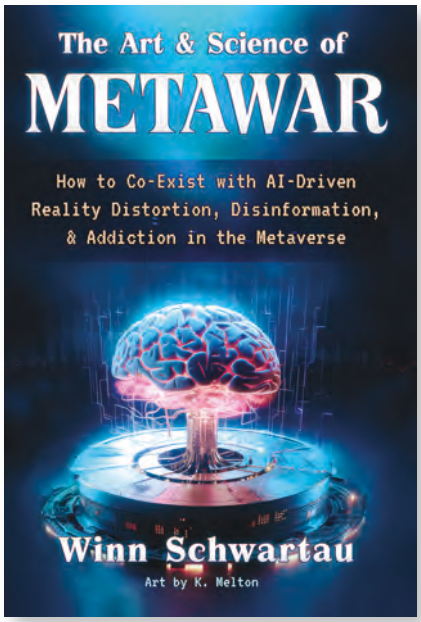
Authors: Stephan Guldenaar is a (retired) principal consultant and may be reached at sefguldenaar@planet.nl. Chris de Vries is chief editor of IB-Magazine and acts as independent consultant in his firm De Vries Impuls Management and may be reached at impuls@euronet.nl

INTERVIEW

How to Co-Exist With AI-Driven Reality Distortion, Disinformation, & Addiction in the Metaverse

The Metawar Thesis

On May 9th of this year, Winn Schwartau gave a seminar called `Metawar: The Battle for Reality in the Metaverse' at a meeting of the Platform for Information Security in Utrecht. He told us then, that he would travel through Europe inviting critical questions on this subject matter. Questions and conversations with folks from many different disciplines that would sharpen his mind on the content matter of his new book that will appear on December 4th, 2023. Winn kindly agreed that before such release he would welcome an interview to be published in our IB-Magazine. So we interviewed him! Before diving into the subject matter one may ask who is this guy Schwartau?



Who is Winn...? Winn Schwartau has lived Cyber Security since 1983, and now says: "I think, maybe, I'm just starting to understand it". His predictions about the Internet and security have been scarily spot on. He coined the term 'Electronic Pearl Harbor' while testifying before Congress in 1991 and showed the world how and why massive identify theft, cyber-espionage, nation state hacking, and cyber terrorism would be an integral part of our society. Winn was named the 'Civilian Architect of Information Warfare' by Admiral Tyrrell of the British Ministry of Defence.

He wrote about 15 books and participated in more than 1.000 TV-shows. His interests: loss of privacy, the psychological aspects of Cyber..., the Metaverse (being like the internet, but worse because immersive), the mathematics and sensory manipulations behind it and becoming aware that technology is only one of the steps of innovation, more important how-to live-in coexistence with it!

His visit May 2023 to The Netherlands and the United Kingdom "Changed my life, my views on the matter". He fears that too many people are blinded, have biased views or are exposed to external manipulation of their unconscious minds. So to test his hypotheses, he asks the audience "to call out my bullshit and let's discuss it". And he considers Europe the place to do that, because in the European Union the policies and compliances are more people centric instead money centric.

So as a courtesy to his positive view on us, Europeans, we should at least pay attention to his thoughts and visions. And it starts with Metaverse and the claim of Facebook that they are Meta! It's not theirs to claim the name, there is too much to be said about their privacy statements; so, let them come and bring it on. Let's consider the facts instead of words. Let's consider the presumptions, the arrogance of the Big Tech companies.

The Metaverse

According to Winn the Metaverse is a human condition strongly related to storytelling, and storytelling is a powerful way of human communication. Exemplary: the 'Nachtwacht (Night Watch by Rembrandt) in het Rijksmuseum' is a story. Metaverse convinces people that it is worth to listen to stories and by doing so change things leading to a distortion of reality. The reader should realise that everything in that process involves (and leads to) information!

Take your big TV-screen at home. Most people are not aware that she/he is being made part of the story shown, like a book that binds you, however with use of many more senses than the story in a book. In fact, the TV-story is attempting to absorb your mind. You see the 'bad guy', yourself being the 'good guy' and through this manipulation it is stimulating you to crave for the reward i.e., a plethora of 'feel-good chemicals' (made by one's own body). Such rewards will lead to addiction and compliance to act as you are guided, based on how you are influenced to think.

Consider the six domains of planetary conflict according to Winn Schwartau:

1. war on soil (army);
2. war on sea (navy);
3. war in the air (air force);
4. space war (satellites);
5. cyberwar (digital) and
6. Metawar (mind control).

To contain Metawar it is necessary that people care more about themselves, necessitating governments to regain their care roll in order to assure that Big Tech are giving up their power positions and their wish to progress their commercial

(also power) empires for the happy oligarchs. So like Bernie Sanders told on the TV-show of Arjen Lubach: "have a dislike for unregulated capitalism"; added by Winn with "content alone should shake people".
Winn elaborates: "... from immersive stories & music to real-time immersive reality made by Artificial Intelligence (AI) good intensions are paving the road to... addiction". It leads to a new way about how our minds work. He refers to the work of the Dutch professor Sander L. van der Linden.

Editors: Van der Linden is a social psychologist at the University of Cambridge, he is well-known for his studies regarding social influence, risk, human judgement and decision-making; all dealing with fake news and misinformation. Van der Linden developed: the inoculation – and conspiracy theory and the gateway belief model. He looks to generate psychological resistance, teaching people to recognise manipulation techniques, helping people to understand (mis)perception of scientific consensus (through a two-step process of attitude change) and to grasp the idea of strong identification regarding to conspiracy theories (1).

'From fun to threat?'

As discussed earlier, Big Tech is enticing people for the sake of profit making. Big Tech may therefore serve as an enabler when developing technology further. As such immersive reality may lead to people wanting more and more (as in an addiction) this may end up in reality distortion on purpose. The purpose being behavioural control of the person, groups of people or possibly a complete society/nation. How can this happen?

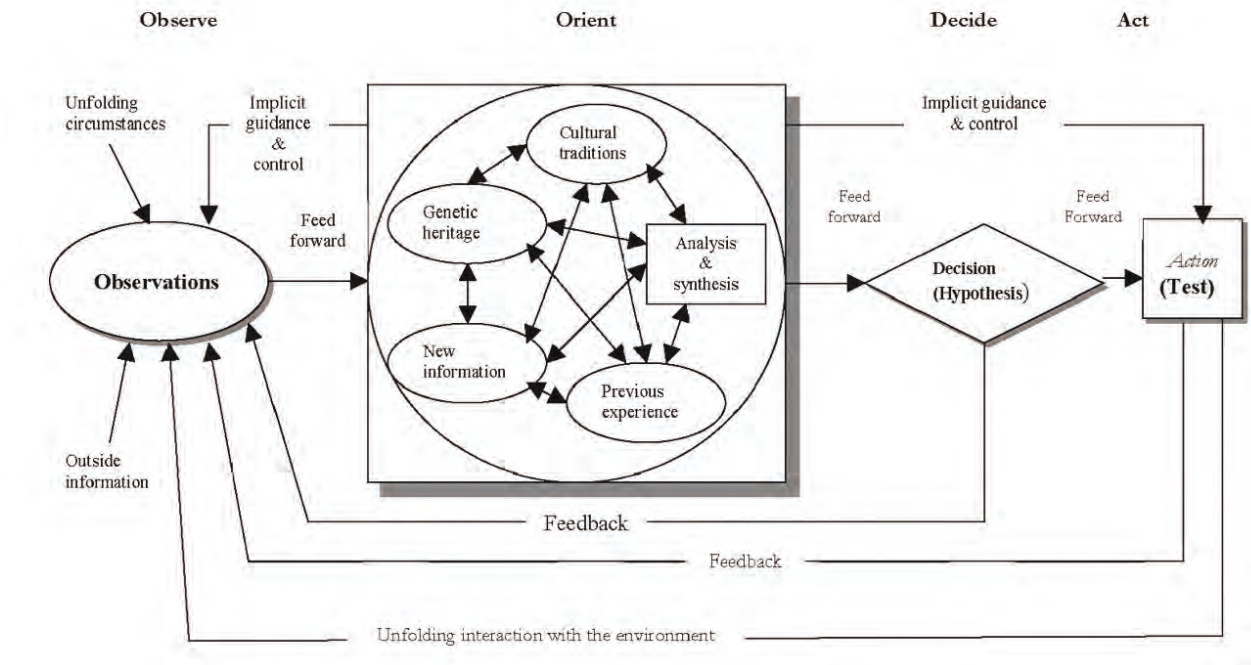
Winn explains that behind the immersive addiction lies neuroscience: starting with a reward mechanism (instant gratification, feel good `Likes', rewarding neurotransmitters in the brain pleasure centres), conscious versus subconscious processing in the brain, based upon: "our fast system 1 (unconscious) versus our slow system 2 (conscious) brain-structure" (D. Kahnemann (2)); and the focus question there: "Is it REAL?"
Winn states that our subconscious brain is targeted using (mainly) visual (about 80% sensory attack surface: 10 MB/s) and sound stimuli (about 10% sensory attack surface: 100 kb/s). The unconscious neural processing goes at a velocity of about 400 billion kb/s (European value: `miljard') versus the conscious neural processing of only 2 kb/s. Being aware of the Meta-warrior who uses social constructs to tell you to feel good about something and Big Techs, as the enablers, leads to the big question: "can people, as organic entities, combat the silicon/chips-based addiction machine(s); once such machine is seeking (Editor: having, think about the smart phone?) control over human behaviour?"

So, Big Tech is not concerned with people and people's privacy. They use more versed network (2.0/3.0) technologies creating surveillance capitalism. Will Government guard its citizens? Look - editors: as a not welcomed policy - what China is doing!? Winn adds to it: China is modifying its people's behaviour through Big Tech orchestration and that could signify disinformation and Metawar. Thus, do people really care enough about themselves and do they care about self-protection against the addiction?

Threat measures

Which mechanisms are there to counter the eminent threat of the Metaverse? In Sweden tomorrow is knocking at the door. There, the Psychological Defence Agency has been instituted. "Safeguarding their open and democratic society, the free formation of opinion through identifying, analysing and countering foreign malign information influence, disinformation and other misleading information directed at Sweden or at Swedish interests" (3).

Winn himself repeats there are three main strategies: Big Tech reforming, government safeguarding (caring!) its people and people making aware of the responsibility owned to themselves: "Caring for yourself". He thinks that the European



Union is doing better than the USA.

When you put forward to your audience statements like: "Mozart outsells the Beatles!"/"Meat from Belgium is infected!" or "Alien baby in Texas!" and follow up with the question: "Is this true or false?", every time a gut reaction can be expected. Such statements will spread 100 times faster than other news thanks to our gut. The reaction of a wise woman or man should be: "Is it real?" and Winn's suggestion: "Do verify and look it up!"
In general: humanity as a biological based being has no defence system against (dis)information, when encountering it, the reaction will be primal: freeze, flight, fight, – Winn adding: "the need for sustenance (feed) and the drive to mate". The foregoing being an adaptationist perspective on the acute stress response spectrum (4).

So, the main question would be: "Do I automatically accept it or not, do I believe it without verification?". The answer would be: critical thinking is necessary. Everybody has to co-exist with technology, so we have to press the PAUSE-button regarding our primal reaction. We have to take time to reflect; 'hold your breath', 'count to 10'; thus, asking ourselves - upon receiving the input received by our sensory system - "Is it real!" Within that context 'resistance is not futile'. Winn explained by a real-life example: "The Netherlands is a country with cobbled streets, that troubled my vestibular sense (movement, gravity and/or balance sense allowing us to move smoothly). I had to take into account to step higher when walking in order to prevent me from falling. So, I had to push my PAUSE-button.

Another aspect is that we all have different clocks in our minds. One specialised in conscious awareness of elapsed time and the other one remembering past experiences (5).

‘That also requests – from time to time – pushing the PAUSE-button in order to verify reality. But to discuss this in detail requires more than one book from me’

That also requests – from time to time – pushing the PAUSE-button in order to verify reality. But to discuss this in detail requires more than one book from me.”

Stephan reflected on his question in May: “If resistance might be futile”, now concluding as result of this interview that “resistance might not be futile”. Winn however, now added to it: “giving-up is a choice to allow yourself to fail”. Humans are not perfect, time to push the PAUSE-button might be missing. It also put forward questions like: “Do we have free will?” and “What do magicians do?” To answer the last question first: “They distort reality of their audience!” Regarding the free will, Winn refers to Benjamin Libet and his experiment regarding the brain initiating voluntary movements before we are aware of having decided to move; calling into question the efficacy of our wills (6). The results of Libet's experiments are important.
So “How to realise yourself that Metaverse is distorting reality?”. Winn retorted “that is a very beautiful question”. It deals with motivation: good or bad? He sees the distortion as a fast OODA-loop (Observe, Orient, Decide, Act) (7), which we - as human beings - can’t compete with. So, harness your human mind, take a deep breath and don’t overreact. Push the PAUSE-button.

New book release

Winn has written a new book in his already impressive series of books, titled: ‘The art & science of Metawar’. He gave us on atomic level an overview of the lay-out:

- act 1: foundation for the book, the brain as a time-system;
- act 2: strategic brain – as well as reality distortion;
- act 3: defensive metawar.

He is not disclosing all information on the book, but said that the 3 acts are to be recognized as him storytelling, relating also to the theme of Neuroscience, which has a young history of 20 years. And be aware that act 2 describes the unconscious distortion, changing reality. For us a non-brainer to read.

With thanks to Winn for his time, humor and intensive conversation.

A book review is on the action list for 2024. Interested readers can pre-order it for December 4th, 2023 at the Amazon site for the paperback and as Kindle book.

References

(1) https://en.m.wikipedia.org/wiki/Sander_van_der_Linden
(2) D. (Daniel) Kahneman, ‘Thinking, fast and slow’, 2011; ISBN 978-0374275631
(3) https://www.mpf.se/en/
(4) Cambridge Core, 07.11.2014
(5) https://www.scientificamerican.com/article/your-brain-has-two-clocks/
(6) https://en.m.wikipedia.org/wiki/Benjamin_Libet
(7) See our article: OODA-looping your security incident response, IB-Magazine IB1-2021 pages 22 up to 24.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Het gaat niet zo goed met de FG

Nog wat nieuws naspeurend herlas ik een bericht van de NOS uit 2018. Velen lieten zich jubelend omscholen tot Functionaris Gegevensbescherming, mooi nieuw werk gloorde aan de horizon met de komst van de AVG. De functie, die praktisch gezien allang bestond, maar door weinig organisaties ingevuld werd voor 2018, kreeg een hoog aanzien mee. Interne toezichthouder – hoeder van de privacy. Maar wat beklijft er nu eigenlijk nog van dat beeld nu we meer dan vijf jaar verder zijn?

Zelf was ik het ooit, kortstondig. In een organisatie die eigenlijk slechts een vinkje wilde zetten en de functie geen zware handen en voeten gaf. En eerlijk is eerlijk, ik vond het zelf ook niet zo geweldig – ik bouw veel liever samen met een team, ben een doener en los graag problemen op. De FG moet juist functionele afstand houden en een wakend oog vormen, issues signaleren en anderen aansturen die op te lossen. Streng, maar rechtvaardig. De rug recht tegen onrecht, een solistisch en onafhankelijk strijder. Maar die FG moet die ruimte wel krijgen. En daar gaat het in de praktijk vaak mis.

In talloze organisaties doet de FG 'het erbij', waarbij die vaak ook nog eens een adviserende functie heeft op het gebied van privacy en actief is in de operatie door bijvoorbeeld beleid te schrijven of te adviseren in dagelijkse casuïstiek. Dit verdraagt zich niet met de toezichthoudende functie – het zou immers de slager zijn die het eigen vlees keurt. De onafhankelijkheid is daarmee ver te zoeken. Autoriteit Persoonsgegevens is de afgelopen tijd ook veel actiever geworden in haar handhaving hierop. Verschillende organisaties hebben al een forse vermaning gekregen van de toezichthouder. En terecht ook. Je moet het verwateren en vermengen van de taken in de governance rondom privacy ook echt niet willen. Diegenen wiens gegevens worden verwerkt zijn er namelijk het slachtoffer van.

Die FG is vaak ook een dappere strijder. Want zelfs als die helemaal 'vrijgemaakt' wordt voor de specifieke taken die bij de functie horen, dan nog is het vaak sappelen. Zeker in grote organisaties. Niet zelden doen ze het alleen. En dat kan gewoon niet. Een FG heeft ondersteuning nodig, middelen en mensen en moet vrij hoog in de organisatie geplaatst worden om zo dicht mogelijk bij het vuur te zitten en diens invloed te kunnen uitoefenen. Gelukkig is er inmiddels wel veel aandacht voor deze benarde situatie en dankzij het ingrijpen van de AP lijkt er wat meer urgentie te komen om de FG steviger in de organisatie te verankeren. Menig mij bekend FG heeft het zwaar, soms met gezondheidsklachten tot gevolg. En dat kan toch echt niet de bedoeling zijn.

Dus, doe mij een lol en breek eens een lans voor de FG in jouw organisatie. Die verdient vaak beter dan die nu krijgt. En we worden er allemaal beter van, want wie wil er nu geen goed toegeruste waakhond op de privacy?

Rachel

Auteur: Fook Hwa Tan is redactielid van IB-Magazine en chief quality officer bij de Northwave Group. Hij is bereikbaar via fookhwatan@northwave-security.com.

VERSLAG

Verbondenheid en kennisdeling op het NCSC One Conference 2023

Het is opwindend om deel uit te maken van de digitale revolutie die onze wereld verandert en vormgeeft. In het begin van oktober 2023 kreeg ik de kans om mijn passie voor cybersecurity en digitale connectiviteit te voeden tijdens het NCSC One Conference in Den Haag. Als een enthousiaste deelnemer aan dit evenement, kan ik met zekerheid zeggen dat deze conferentie niet alleen mijn kennis heeft vergroot, maar ook mijn netwerk, allemaal onder het inspirerende thema 'We are all connected'.

Het tweedaagse evenement op 3 en 4 oktober jl., bracht professionals nationaal en internationaal samen om te discussiëren over de huidige staat van cybersecurity en de uitdagingen en kansen die de steeds groeiende digitale verbondenheid met zich meebrengt. Het was een opwindende gelegenheid om te leren van en te netwerken met enkele van de meest vooraanstaande experts en denkers in de branche.
De conferentie werd geopend door de burgemeester van Den Haag, Jan van Zanen, en organisator Hans de Vries om in verbinding de maatschappij samen een stukje veiliger te maken.

Inspirerende Sprekers

Een van de hoogtepunten van het NCSC One Conference waren de inspirerende sprekers, die hun inzichten deelden over het thema 'We are all connected'. De keynote-sprekers (een volledig vrouwelijk ensemble gekozen vanuit hun expertise en kennis in het vak) brachten een schat aan ervaring en kennis met zich mee, waaronder vooraanstaande cybersecurity-experts, vertegenwoordigers van overheidsinstanties en leiders uit de private sector. De volgende sprekers Lorena Boix-Alonso, Jaya Baloo, Esther Schagen-van Luit, Felicity Oswald, Katelyn Bailey en Bettina Haas wisten het publiek te boeien met hun expertise. Ze deelden hun visies op de uitdagingen en kansen van onze onderling verbonden wereld.

Informatieve sessies en workshops

Naast de boeiende lezingen waren er talloze informatieve sessies en workshops die deelnemers de kans gaven om dieper in te gaan op specifieke onderwerpen binnen de wereld van cybersecurity en digitale connectiviteit. Van technische diepgaande discussies tot beleidsgerichte panels, er was voor elk wat wils.

Zelf heb ik op de eerste dag meer geleerd over de kansen en dreigingen van de metaverse, security by behavioural design, Attacker Strategy Discovery from Intrusion Alerts, Cybersecurity behaviour decomposed, hoe een sleutel makkelijk gekopieerd kan worden vanuit een foto en de resultaten van samenwerking tussen de Verenigde Staten en Nederland. Op de tweede dag heb ik mogen vernemen hoe het Qakbot netwerk is ontmanteld, Paperbug en de valse veiligheid die Zero Trust kan creëren. Voor degene die dit lezen en er vreemde woorden zien staan, zou ik willen aanmoedigen indien de NCSC de opnames vrijgeeft deze terug te kijken.

Netwerkmogelijkheden

Een van de meest waardevolle aspecten van het NCSC One Conference was de kans om te netwerken met gelijkgestemde professionals. Tijdens koffiepauzes, lunches en sociale evenementen ontmoette ik experts uit verschillende sectoren en landen. Deze interacties openden deuren voor toekomstige samenwerkingen en het uitwisselen van best practices. Het voelde als een jaarlijkse reünie met dank aan de NCSC om dit te faciliteren.

Innovatieve technologieën en oplossingen

De expozaal op het evenement bood een overvloed aan innovatieve technologieën en oplossingen van bedrijven en organisaties, die de frontlinie van cybersecurity bezetten. Het was indrukwekkend om te zien hoe nieuwe technologieën worden ingezet om de uitdagingen van een steeds verbonden wereld aan te gaan. Hierbij waren ook veel partijen, die ook buiten de technologie kunnen helpen.

Conclusie

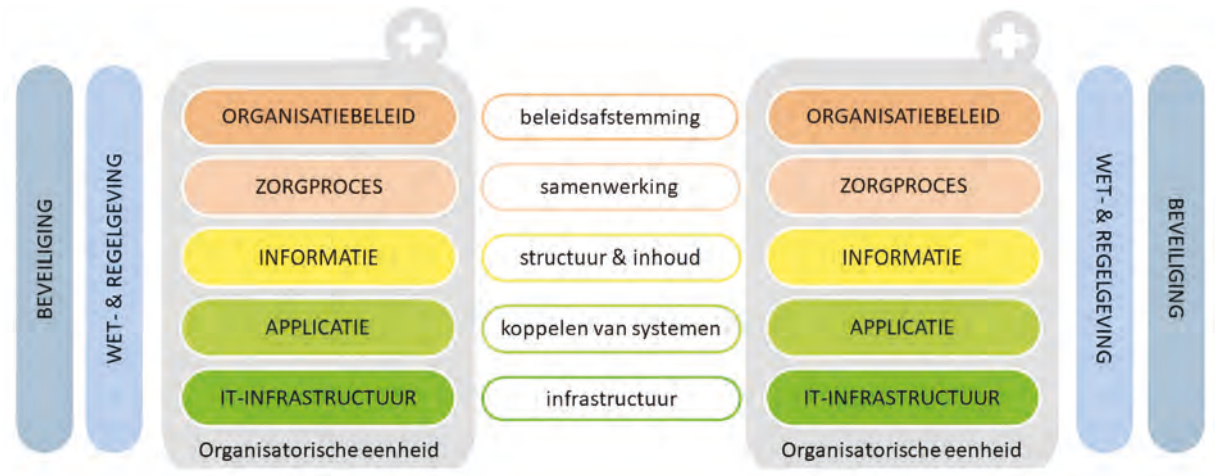
Het NCSC One Conference 2023 was een onvergetelijke ervaring voor mij als enthousiaste deelnemer. Het bood niet alleen diepgaande kennis en inzichten over de huidige stand van zaken in cybersecurity en digitale connectiviteit, maar het gaf me ook de kans om mijn netwerk uit te breiden en waardevolle contacten opnieuw te spreken. Het benadrukte het belang van samenwerking en kennisdeling in een wereld waarin we allemaal met elkaar verbonden zijn. Ik kijk ernaar uit om de opgedane kennis en contacten in mijn professionele carrière te benutten en te blijven werken aan een veiligere en meer verbonden digitale toekomst. Het NCSC One Conference heeft mijn enthousiasme voor dit vakgebied alleen maar versterkt, en ik kan niet wachten om te zien wat de toekomst zal brengen in onze voortdurend evoluerende digitale wereld. Verder ook benieuwd wat het volgende NCSC One Conference gaat brengen!

Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. Hij is te bereiken via: andre@octopus-ib.nl of via https://www.linkedin.com/in/andre-beerten/.

Gedachten over een 'Register'

OF HOE WE ZONDER INFORMATIE NIET KUNNEN BEVEILIGEN

Een plek waar voor alle betrokkenen bij informatiebeveiliging (en privacy, laten we die vooral niet vergeten) passende informatie vindbaar is noem ik het 'Register'. De informatie over informatie en beveiliging die onmisbaar is voor IB-inspanningen. En volgens mij ook voor een betrouwbaar beeld van de gevraagde 'passende beveiliging': daar hoort ook alle informatie over opzet-bestaan-werking van beveiliging in thuis, ongeacht de methode en middelen die je hanteert voor beveiliging. Waarom? Omdat de 'business', oftewel de vragers van beveiliging moeten weten hoe de beveiligers (de control-eigenaren) presteren. De risicoverantwoordelijkheid ligt immers in de business en niet bij de ondersteunende afdelingen (of zie jij dat anders?). En natuurlijk is zo'n register handig als de auditor wil weten hoe je de boel beveiligt.



Figuur 1: Datamodel van het Register.

Het beheersen van risico's is het hoofddoel van informatiebeveiliging. Beheersen begint met kennis van de scope, het bereik van je domein. De ISO27001 begint daar in hoofdstuk 4 niet voor niets ook mee, waar de grenzen, context en belanghebbenden bij het domein moeten worden verkend.

Strategisch

De kennis van je domein moet je onder meer een beeld geven van je 'risico-omgeving': wat is de betekenis van informatie in je branche, welke informatie verwerkt je organisatie, hoe groot is je afhankelijkheid, wat zijn bekende bedreigingen van beschikbaarheid, integriteit en vertrouwelijkheid ervan. Het geeft het belang aan van informatie en informatiebeveiliging voor je economische activiteit, waardoor de leiding een generieke beveiligingsambitie en een 'risk-appetite' kan formuleren waar je organisatie mee aan de slag kan. Het is 'chef-sache'.

Tactisch

Op tactisch niveau zet je deze ambitie en appetite om in beleidsregels en een concrete aanpak, waar betrokkenen mee aan de slag kunnen. Die vertaalslag kan alleen succesvol zijn als een betrouwbaar beeld bestaat van het informatielandschap ín de organisatie, gekoppeld aan verantwoordelijkheden ten aanzien van specifieke risico's per bedrijfsproces oftewel informatieverwerking en de daarvoor gebruikte middelen/diensten. Op basis van dit specifieke beeld kan beveiliging aangepakt worden. ISO, NEN & BIO vragen in control 8.1.1 om dat beeld 'Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris te worden opgesteld en onderhouden' (1). De opdracht gaat duidelijk niet (alleen) over de uitgereikte laptops, telefoons, usb-sticks, DVD's, etc.

Operationeel

De beveiligers, zij die de controls uit de norm moeten vertalen naar passende maatregelen, kunnen dat alleen doen als de informatie uit de strategische en tactische analyses hen bereikt. En niet alleen moet die informatie 'vindbaar' zijn, maar ook gestructureerd worden aangeboden, geordend naar risico, verwerking en control.
Dus een correlatie van risico's, verwerkingen, systemen/diensten en controls moet gelegd kunnen worden, anders vinden de beveiligingsinspanningen 'blind' plaats.

Wat ik waarneem

Ik heb in de tientallen organisaties waar ik heb gewerkt of opdrachten heb vervuld nog geen voorbeeld gezien van een Register zoals ik dat hierboven beschrijf.
Er zijn wel deelregistraties, zoals van IT-spullen en van het 'register van verwerkingen' van de PO/FG, maar die zijn vaak niet actueel en worden ook niet gedeeld in de organisatie en zijn niet of moeilijk te correleren.

‘Cruciale randvoorwaarde voor succes is ‘Eigenaarschap van risico’s, verwerkingen en controls’

Dat betekent dat betrokkenen voortdurend in het duister tasten over de stand van de beveiliging, over hoeveel systemen er zijn, wie die beheert, waar ze staan, welke cloud services we gebruiken en waarvoor, hoe de beveiliging per verwerking/systeem/dienst moet worden aangepakt en dan hebben we daarbij nog de onderwerpen eigendom, classificatie, toegang, koppelen etc... die ook allemaal aan beveiliging raken. CISO’s, PO’s, FG’s én control-eigenaren tasten vaak in het duister.

Voorbeeld van een Register-concept

Ik heb onlangs zijdelings kennis gemaakt met een model dat een beeld geeft van de mogelijke opbouw van zo’n Register en van de gebruiksdoelen: het NICTIZ 5-laags infra-model. In dat model staat het delen van informatie door partijen centraal, geordend naar functionele lagen. Deze structuur lijkt mij zeer handig voor het – conceptuele – datamodel van het Register.

Elk van de informatielagen kan (een groep van) eigenaren hebben die zorgen voor de actualiteit en betrouwbaarheid (en compleetheid) van de informatie. Gebruikers, zoals control-eigenaren, weten waar de informatie waar ze zich op baseren vandaan komt en hoeven niet meer op zoek.
Het Register (2) moet zélf natuurlijk ook een eigenaar hebben. Die zoek ik in de kolom informatiemanagement (in het 9-vlaks-model van Maes), tussen business en IT, waar overzicht de eerste opdracht is.

Voorbeeld van Register-beleid

Ik deel hier met jullie mijn voorstel voor een beleid dat dit Register instelt. Zoals het mij betaamt is dit artikel geen stuk met vrome wensen, maar geef ik (hoop ik) helder instructies aan benoemde rollen, waarop gehandhaafd kan worden. Cruciale randvoorwaarde voor succes is `Eigenaarschap van risico’s, verwerkingen en controls’, zoals ik dit al eens omstandig heb betoogd in een eerder artikel in dit blad.

Tactisch beleid Register

Elke organisatie heeft voor haar beheersing van de informatievoorziening behoefte aan een helder, actueel en compleet overzicht van haar informatiesystemen & -diensten eindverantwoordelijken voor beheer en beveiliging. Vooral bij incidenten is een dergelijk actueel en compleet overzicht van groot belang om snel te kunnen handelen. Dit beleidsdocument biedt kaders voor realisatie van een dergelijk overzicht.

Doel

Eén informatiepunt over de informatieverwerkingen in het domein: gestructureerde vastlegging en beschikbaarstelling van tactische en operationele (stuur-)informatie over projecten en middelen van de organisatie.
Specifieke doelen zijn:

- Ondersteunen van interne processen (ontwikkeling, beheer, veiligheid) voor gemak, snelheid en actualiteit;
- Procesverbetering, lagere (zoek-)kosten voor medewerkers, minder fouten, snellere analyse en response op incidenten;
- Makkelijker toezicht op de realisatie van kwaliteitseisen van opdrachtgevers en toezichthouders, zoals privacy en informatiebeveiliging.

Persoonsgegevens

Informatie over de verwerking van persoonsgegevens (welke gegevens waar, hoeveel, gebruiksbeperking, verwerker) moet tactisch en operationeel beschikbaar zijn. Ook voor informatiebeveiliging is er behoefte aan een intern `register’ waarin duidelijk wordt hoe elke verwerking compliant is en waar bewijzen gevonden kunnen worden van implementatie van risk-controls ten behoeve van privacy.

Bereik van het Register

De Registereigenaar (informatiemanagement dus) zorgt ervoor dat het Register de volgende informatie bevat:

- In de breedte: alle projecten, producten, informatieverwerkingen en middelen (waaronder interne applicaties, databases en hulpmiddelen voor beheer & onderzoeken);
- In de lengte: gedurende de hele levenscyclus, van idee tot en met afdanken;
- In de diepte: alle informatie rond opdrachtgever, risico's/gevraagde beveiliging (uit de BIA en DPIA), verantwoordelijkheden & (beheer-)afspraken, toegangsverlening (matrix & autorisaties), audits, koppelingen en documentatie over opzet, bestaan en werking van informatiebeveiligings- en privacy maatregelen.

Kwaliteit

Het Register moet een juiste, complete en actuele informatiebron zijn voor alle informatie-gerelateerde vragen (informatie over informatieverwerking). Om dat te bereiken zorgt de Register-eigenaar voor regelmatige toetsing van de kwaliteit van de informatie van het Register en onderneemt herstelacties door de bronnen aan te spreken. De eigenaar rapporteert hierover aan het IBMF/ de stuurgroep informatiebeveiliging.

Eigendom

Het Register of masterlist kent twee samenwerkende (groepen) eigenaren:

- Van functionaliteit en beschikbaarheid van de voorziening. Deze bepaalt ook in afstemming met de CISO inhoudelijke ambitie: welke informatie komt er wel/niet in het Register);
- Van de juistheid, toepasselijkheid, tijdigheid en compleetheid van de informatie in de masterlist: dit ligt bij eigenaren van verwerkingen en controls zoals verder uiteengezet in het 'Beleidsbijlage eigenaarschap van informatieverwerkingen' en de 'Beleidsbijlage eigenaarschap van controls'.

De tabel in het kader geeft een begin van een overzicht van de relatie informatie <> verantwoordelijke. De Register-eigenaar zorgt voor communicatie en overleg met alle betrokkenen.

(Een begin van) een inhoudsopgave van het Register

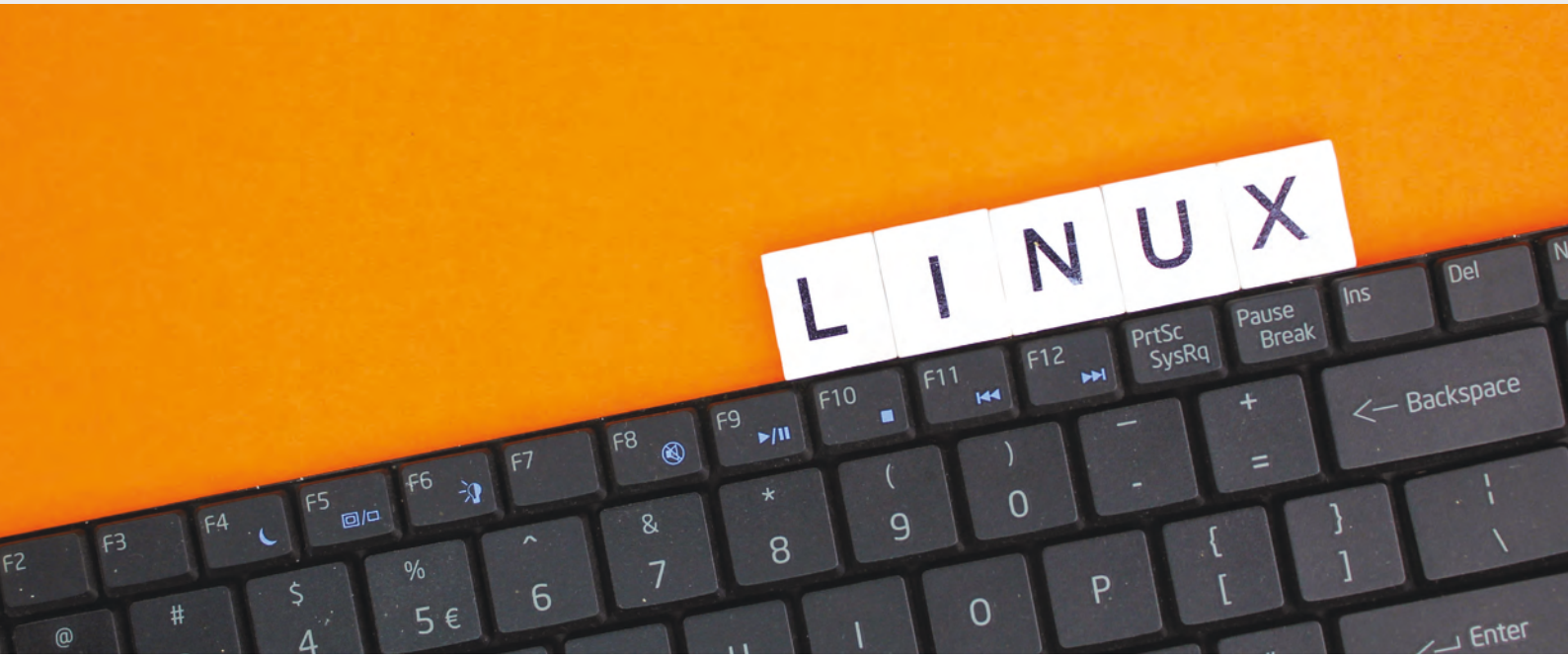
- Het verwerkingenregister van Privacy, aangevuld met alle overige 'verwerkingen'
    - o aangevuld met (of samenvallend met) bedrijfsprocessen
    - o aangevuld met de verwerkte informatie en classificatie
    - o informatie uit BIA & DPIA en andere risicobronnen:
        - alle risico-informatie, classificatie etc.
        - alle afspraken/voornemens (Maatwerk-Maatregelen) rondom beveiliging en toezicht, met agenda-/actiekoppelingen ('geactiveerd' dus die leiden tot signalen die tot actie aanzetten) voor actief toezicht op de beheerder/leverancier;
- Gerelateerde hardware en software, maar ook diensten (alle 'Cloud' etc.). Daar horen dan ook nog de diensten van 'vaste' en mobiele telefonie, Internet-lijnen, housing, hosting en beheer voor x systemen)) onder;
    - o koppelingen en (kritieke) afhankelijkheden;
    - o zicht op de gehele leverketen:
      applicatie < hoster < houser < implementatiepartner < servicepartner < leverancier HW & SW
      (misschien mis ik nog wat..);
    - o rollen rondom beheer (FB, AB, TB), gebruik, toezicht etc;
    - o niet alleen interne rollen, maar ook externe rollen (de BIA/DPIA heeft dat hopelijk in beeld gebracht). Daarbij hoort contactinformatie en operationele info zoals vastgelegd in een DAP, maar ook service-windows, responsetijden, hersteltijden, escalatie informatie;
- Alle contractuele informatie etc. etc..

Referenties

(1) In de ISO27001-2022-versie geldt een vergelijkbare opdracht: 'Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden'.

(2) Hét Register, ik schrijf het doelbewust met een hoofdletter.

Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.



Ook Linux-systemen niet immuun voor bedreigingen

HULPGIDS BEVEILIGING VOOR HET KLEINBEDRIJF (DEEL 5)

Linux, een krachtige en veelzijdige besturingssysteemfamilie, staat bekend om zijn robuuste beveiligingskenmerken en wordt daarom vaak gebruikt voor serveromgevingen. Echter, ongeacht hoe veilig een systeem is, is het nooit immuun voor alle mogelijke bedreigingen. Beheerders en gebruikers moeten een proactieve rol spelen om hun systemen te beveiligen en te onderhouden, en dat begint met een grondig begrip van het beveiligingslandschap en de beschikbare tools en configuraties.

In dit artikel duiken we in de wereld van Linux-beveiliging, waarbij we diverse aspecten verkennen zoals initiële installatie en configuratie, de configuratie van firewalls en secure shell (SSH), systeemmonitoring, en regelmatige beveiligingsaudits. Dit artikel biedt inzichtelijke informatie en praktische stappen om de beveiliging van Linux-systemen te versterken en optimaliseren.

Net zoals bij de vorige Windows en Mac artikelen zullen we de volgende onderwerpen behandelen.

1. Hygiëne;
2. Veilige configuratie;
3. Systeemkennis.

Hygiëne

Het actueel houden van systeembestanden is een essentieel onderdeel voor het onderhouden van Linux-systemen. Het regelmatig bijwerken van het systeem en de geïnstalleerde softwarepakketten zorgen ervoor dat beveiligingslekken worden verholpen, en dat het systeem is beschermd tegen bekende bedreigingen. Gebruik voor updates (command-line) pakketbeheerders zoals: de Advanced Package Tool (APT) voor Debian-gebaseerde systemen en yum voor Red Hat-gebaseerde systemen. Standaard voert Ubuntu namelijk (Debian-gebaseerde Linux-systeem) geen automatische updates uit. Hiervoor moet je de 'unattended-upgrades' package installeren en configureren.

Het is belangrijk om alleen de noodzakelijke diensten en toepassingen op het systeem te laten draaien. Onnodige diensten kunnen potentiële ingangspunten voor aanvallers zijn en het deactiveren of verwijderen ervan vermindert het aanvalsoppervlakrisico van het systeem. Gebruik daarom de APT of yum commando's om packages te beheren en te installeren waar nodig.

Gebruik je het Linux-systeem ook voor het dagelijks gebruik, zoals browsen, dan is het ook daar goed om je browser goed in te stellen. Browserhygiëne is ook belangrijk, vooral omdat de meeste gebruikers veel tijd online doorbrengen. Regelmatig wissen van browsercache, cookies en geschiedenis kan helpen om persoonlijke informatie te beschermen en blootstelling aan online bedreigingen te verminderen. Het installeren en gebruiken van browserextensies voor beveiliging, zoals uBlock Origin en HTTPS Everywhere, helpen ook bij het verhogen van de onlinebeveiliging.

Veilige configuratie

Het adequaat configureren van firewalls is van essentieel belang om systemen te beschermen tegen ongewenste toegang en aanvallen van buitenaf. Dit vormt de eerste verdedigingslinie tegen kwaadwillende activiteiten. Met behulp van Uncomplicated FireWall (UFW) kunnen gebruikers firewall-regels beheren, waardoor specifieke poorten en diensten toegankelijk worden, terwijl andere worden geblokkeerd. Deze tools zijn cruciaal voor het reguleren van inkomend en uitgaand verkeer op een Linux-systeem. Zeker omdat een Linux-systeem niet standaard met een firewall komt. Daarbovenop is het echt een vereiste om Fail2Ban installeren. Fail2Ban zorgt ervoor dat IP adressen die kwaadwillig aankloppen geblokkeerd worden als ze dat te vaak proberen: oftewel brute force bescherming.

Zeker bij servers wordt er vaak gebruik gemaakt van Secure Shell (SSH). Dat is sleutelgebaseerde authenticatie: een veiliger alternatief voor wachtwoordauthenticatie. Het gebruik van SSH-sleutels minimaliseert het risico op ongeautoriseerde toegang door brute force-aanvallen en andere soorten inbreuken alsook helpt het om de standaard SSH-poort te veranderen naar een ander port-nummer om de meeste geautomatiseerde aanval tools te slim af te zijn. Het uitschakelen van het root-account op Linux kan de beveiliging verhogen, omdat het aanvallers een potentieel doelwit ontneemt.

Hier volgen de stappen om het root-account uit te schakelen en over te stappen naar een gebruikersgebaseerdsysteem:

1. Maak een Sudo-Gebruiker:
Voordat u het root-account uitschakelt, moet u een nieuwe gebruiker aanmaken en deze sudo-rechten geven, zodat u beheerderstaken kunt uitvoeren.

```
sudo adduser <gebruikersnaam>
sudo usermod -aG sudo <gebruikersnaam>
```

Vervang <gebruikersnaam> met de gewenste gebruikersnaam.

2. Login onder de nieuwe gebruikersnaam:
Log uit als root en log vervolgens in met de nieuwe gebruikersaccount.

3. Pas SSH Configuratie aan:
Bewerk de SSH-configuratie om root-login via SSH te verbieden.

```
shell
sudo nano /etc/ssh/sshd_config
```

Zoek naar de regel die PermitRootLogin bevat en wijzig deze naar:

```
shell
PermitRootLogin no
```

Sla de wijzigingen op en herstart de SSH-service:

```
shell
sudo systemctl restart sshd
```

4. Schakel Root-Account Uit:
Nadat u hebt bevestigd dat u kunt inloggen en sudo kunt gebruiken als nieuwe gebruiker, kunt u het root-account uitschakelen door het wachtwoord te

verwijderen:

shell

sudo passwd -l root

Dit commando vergrendelt het root-account door het wachtwoord te verwijderen, zodat niemand ermee kan inloggen.

5. Beheer het Systeem met Sudo:
Nu, in plaats van in te loggen als root, logt u in als normale gebruiker (uw eigen gebruikersaccount) en gebruikt u sudo om commando's uit te voeren die verhoogde rechten vereisen.

Systeemkennis

Om jouw Linux-systeem veilig te houden, is het handig het systeem te bestuderen. Onderzoek hierbij het navolgende:
1. Folder en gebruikersrechten;
2. Netwerkinstellingen, zoals de firewall en
3. Inspectie van de logs.

Folder en gebruikersrechten

Het grondig begrijpen en correct implementeren van folder- en gebruikersrechten is cruciaal voor de beveiliging van Linux-systemen. In Linux worden permissies toegewezen aan bestanden en directories. Deze permissies bepalen wie deze kan lezen, schrijven of uitvoeren en zijn gecategoriseerd voor de eigenaar, de groep waartoe de eigenaar behoort, en alle andere gebruikers. Het is noodzakelijk om begrip te hebben van Read (lezen), Write (schrijven), en Execute (uitvoeren) permissies voor het instellen van adequate toegangscontroles. Commando's zoals chmod worden gebruikt om permissies te wijzigen en chown en chgrp om de eigenaar en de groep te veranderen. Ook de umask waarde is van belang; deze bepaalt de standaardpermissies voor nieuw aangemaakte bestanden en directories.
Bij het beheren van gebruikers en groepen heeft elke gebruiker op een Linux-systeem een unieke gebruikers-ID en is lid van ten minste één groep. Het is belangrijk om gebruikers toe te voegen aan de juiste groepen om correcte toegangsrechten te verzekeren. Gebruikers- en groepenbeheer omvat het gebruik van commando's als useradd, usermod, userdel, groupadd, groupmod, en groupdel. Het toekennen van minimale rechten aan gebruikers, volgens het principe van de minste privileges, helpt het risico op ongeautoriseerde toegang te verminderen. De configuratie van sudo is eveneens essentieel. Met sudo kunnen normale gebruikers tijdelijk privileges van de superuser verkrijgen om specifieke commando's uit te voeren. Een veilige sudo configuratie vereist begrip van welke gebruikers, of groepen van gebruikers, welke commando's mogen uitvoeren. Het is ook belangrijk om regelmatig de sudo configuratie en logs te reviseren om te verzekeren dat alleen geautoriseerde gebruikers geprivilegieerde acties kunnen uitvoeren.

Netwerkinstellingen, zoals de firewall

Een fundamenteel aspect hierbij is de configuratie van de firewall, die fungeert als een barrière tussen uw beveiligde interne netwerk en ongeautoriseerde externe netwerken. Een goed geconfigureerde firewall kan de toegang tot het systeem beperken en beschermen tegen ongewenste indringers en netwerkaanvallen. Binnen de Linux-omgeving zijn iptables en ufw (Uncomplicated Firewall) algemeen gebruikte tools voor het beheren van firewall-regels. Iptables maakt deel uit van de oudere generatie firewall-oplossingen, terwijl ufw is ontworpen om de configuratie van firewall-instellingen te vereenvoudigen. Door de beheerder in staat te stellen om toegangsregels effectief te definiëren en te beheren, helpen deze tools bij het vormgeven van het veiligheidslandschap van het systeem. Het is ook belangrijk om bewust te zijn van en begrip te hebben van netwerkprotocollen en poorten, aangezien deze kennis essentieel is bij het configureren van firewall-regels. Het beperken van de toegang tot alleen noodzakelijke poorten en het blokkeren van alle overbodige poorten kan helpen het aanvalsoppervlak van het systeem te minimaliseren en zo de blootstelling aan potentiële dreigingen te verminderen.

Inspectie van de logs

Het inspecteren van logs is een belangrijke vaardigheid om de integriteit van een Linux-systeem te behouden. Logs bieden gedetailleerde informatie over de activiteiten en processen die plaatsvinden op een systeem en kunnen waardevolle inzichten geven in de status van het systeem zowel bij eventuele problemen of beveiligingsincidenten die zich voordoen.
De tail-opdracht is een nuttig hulpmiddel voor het bekijken van logs. Met tail kunnen gebruikers de laatste regels van een bestand bekijken, wat handig is om de meest recente activiteiten of fouten in logbestanden te volgen. Bijvoorbeeld, tail/var/log/syslog zal de laatste tien regels van het syslog-bestand tonen, waarmee recente systeemactiviteiten bekeken kunnen worden. Het cat-commando is ook het bestuderen waard. Het wordt gebruikt om de inhoud van bestanden weer te geven en het is bijzonder handig om snel de gehele inhoud van een logbestand te overzien. Een voorbeeldgebruik zou cat/var/log/auth.log zijn, om authenticatie gerelateerde logs te lezen en te reviewen op tekenen van ongeautoriseerde

toegangspogingen. Voor diepgaande analyse en om specifieke informatie te extraheren, is het grep-commando van onschatbare waarde. Grep kan worden gebruikt om te zoeken naar bepaalde patronen, woorden of zinnen in bestanden, wat praktisch is bij het onderzoeken van specifieke incidenten of activiteiten. Bijvoorbeeld, grep `Failed password' /var/log/auth.log kan worden gebruikt om te zoeken naar mislukte inlogpogingen in het authenticatielog.
Naast het inspecteren van logs, is het ook belangrijk om regelmatig logs te monitoren om ongebruikelijke activiteiten of afwijkingen snel te detecteren. Het instellen van geautomatiseerde logmonitoring en alerting kan ook helpen om snel op de hoogte te zijn van potentiële beveiligingsincidenten.
Op mijn Linux-systemen heb ik altijd een alert die afgaat zodra een gebruiker inlogt via een IP-adres dat niet bekend is; of als admin rechten worden gebruik via het sudo commando.

Herkennen van backdoors

In cybersecurity zijn backdoors toegangspunten in een systeem die door aanvallers worden gebruikt om ongeautoriseerde toegang tot een systeem of netwerk te verkrijgen. Voor Linux-systemen kan het monitoren van de netwerkpoorten die in gebruik zijn, nuttig zijn om potentiële backdoors te identificeren. Zo kun je de commando lsof -i gebruiken om alle applicaties te zien die luisteren naar een poort. Zie je hier in de lijst een poort of applicatie staan die je niet herkent dan zou dat wel eens een backdoor kunnen zijn.
Toch maken veel hackers gewoon gebruik van SSH. Zo zul je soms geen vreemde applicaties zien die luisteren naar poorten waar ze niet naar hoeven te luisteren. cat /var/log/auth.log | grep Accepted | grep -v {IP-adressen die je verwacht}. Op mijn servers heb ik een klein script aanstaan dat me meteen een e-mail stuurt zodra iemand inlogt vanaf een onverwacht IP-adres.
Het beoordelen van systeemprocessen is een essentiële techniek in het identificeren van potentiële backdoors en andere kwaadaardige activiteiten op een Linux-systeem. Dit omvat het analyseren van lopende processen, services en daemons om eventuele ongeautoriseerde of verdachte activiteiten te identificeren. Hier volgt een tweetal commando's van hoe je dit effectief kunt doen:

- ps aux: Dit commando toont een gedetailleerde lijst van de lopende processen. Het kan helpen bij het identificeren van ongebruikelijke of niet-herkenbare processen.
- top/htop: Deze commando's bieden een real-time overzicht van systeemprocessen en hun verbruik van systeembronnen, waardoor snel processen die buitensporige bronnen verbruiken, kunnen worden geïdentificeerd.

Bekijk de commando's en besteed aandacht aan de gebruiker die het proces uitvoert, de CPU en het geheugen dat het verbruikt alsook de commando's die worden uitgevoerd. Verdachte processen kunnen een abnormaal hoog niveau aan systeembronnen verbruiken of onder een onbekende gebruiker draaien. Sommige malware kan processen verbergen. Tools zoals chkrootkit of rkhunter kunnen helpen bij het identificeren van verborgen processen en andere rootkit-functionaliteiten.

Instellen van alerts

Het instellen en de monitoring van je Linux-systeem zorgt ervoor dat je grip houdt op wat er gebeurt. Met de `crontab -e' commando kun je automatisch scripts instellen die ervoor zorgen dat je altijd op de hoogte wordt gehouden als er wat belangrijks gebeurt in jouw Linux-systeem. Heb je meer dan één server staan? Dan kan het goed zijn om te monitoren op backdoors door middel van een centraal logging systeem. Een open source applicatie zoals GrayLog is dan een goede oplossing. Daarnaast kan het gebruik van aanvullende monitoringtools, zoals Nagios of Zabbix, die realtime bijhouden van systeemprestaties en resourcegebruik mogelijk maken, bijdragen aan een meer uitgebreide monitoringstrategie. Deze tools kunnen worden geïntegreerd om je te helpen grip te houden op wat er gebeurt binnen jouw Linux-systeem.

Conclusie

In dit artikel hebben we een grondige duik genomen in de wereld van Linux-beveiliging, waarbij cruciale aspecten zoals systeemhygiëne, veilige configuratie en systeemkennis uitgebreid zijn behandeld. Van het up-to-date houden van systemen tot het nauwgezet beheren van firewall-configuraties en het inspecteren van logs, de versterking van de beveiliging van de Linux-infrastructuur. De besproken tips en tools, indien effectief toegepast, kunnen bijdragen aan het versterken van het robuust maken van een Linux-systeem.

Met dit vijfde artikel sluiten we deze serie af. Wij hebben getracht op heldere wijze de beveiliging voor meerdere operationele systemen te bespreken, zodat de niet specialistische MKB-ondernemer ermee aan de slag kan. Via het PvIB-LinkedInaccount en de e-mailadressen van de auteurs kan u ook toekomstig vragen blijven stellen en problemen voorleggen.

Even voorstellen: Lilian Knippenberg

Tijdens de ALV van 9 november ben ik benoemd tot bestuurslid met aandachtsgebied Redactie. De Redactie is de leukste commissie die er is, daarom een ode aan de Redactie en tegelijk een ode aan het product dat we maken: IB-Magazine. Vier tot zes keer per jaar vullen we een blad met interessante en goede artikelen, columns en blogs. Jij, onze gewaardeerde lezer, hebt naast digitaal een voorliefde voor het gedrukte tijdschrift (zo toont de enquête aan). Eerlijk gezegd begrijp ik dat heel goed.

- Terwijl je rustig thuis bent, wandelt er buiten iemand in een opvallend oranje uniform naar jouw voordeur. Je hoort het geklepper van de brievenbus. Papier is tastbaar, het ligt daadwerkelijk op jouw deurmat. Je kunt het oppakken, vasthouden en ruiken. Ook dat laatste is belangrijk, zo ondervonden we toen wij klachten hadden dat het blad stonk (1) in plaats van die heerlijke papier- en inktlucht.
- Je neemt je vertrouwde, naar inkt geurende blad erbij, nestelt je lekker op de bank of in jouw favoriete stoel en scheurt het plastic van de nieuwste IB-Magazine. Je begint met lezen. Merk je dat? Geen afleiding. Je magazine maakt geen geluid, zoemt niet en geeft geen (on)gewenste pop-ups. Wat een oase van rust!
- En dan nog een element dat papier zo fijn maakt: je houdt je IB-Magazine gewoon op de afstand van je ogen die je zelf fijn vindt, zonder je zorgen te maken over de helderheid van je papier of last te krijgen van vierkante ogen (zoals mijn moeder vroeger altijd zei). Een welkome afwisseling na een dag vol digitale vergaderingen, mails, chats en wat nog meer.
- We doen ons best het blad vol te zetten met artikelen die je aanspreken. Als het fysieke blad weer binnen is, schrijf ik altijd op de voorkant welke artikelen ik in mijn werk zou kunnen gebruiken. Tijdens het lezen onderstreep ik zinnen en zet ik uitroeptekens in de kantlijn. Dat kan digitaal ook, maar dat voelt toch anders.

Kortom: ik houd ervan om bezig te zijn met de beleving die het blad jou als lezer brengt!

Na vijf jaar redactielid geweest te zijn maak ik dus nu de stap naar het PvIB bestuur. Ik kijk ernaar uit om het blad en verwante projecten verder te brengen samen met Chris de Vries (onze excellente hoofdredacteur van IB-Magazine) en de redactie. Zo zoeken we meer interactie (lastig met een fysiek 'eindproduct'), kijken we naar de mogelijkheden van een digitaal blad (alweer), zoeken we uit of we de vormgeving willen vernieuwen. Onze andere plannen houden we nog even geheim.

Punt van aandacht is overigens altijd de tijd. Zowel voor mezelf bij de begeleiding van een auteur en de intensieve piek rond de due date en drukproef, als bij het zoeken van nieuwe auteurs die een goed stuk kunnen schrijven voor het blad. Kortom: meld je aan! Onze doelstelling is om een voorraad te hebben van artikelen die we kunnen plaatsen. Wil je of kun je geen artikel schrijven, maar heb je wel goede/praktische/vernieuwende ideeën?

Meld je dan ook via ibmagazine@pvib.nl. We kunnen je interviewen of samen een artikel schrijven. Voor nu wens ik je veel leesplezier en hoop ik dat je weer geniet van deze laatste uitgave van 2023.

(1) Betrof de 'special' over architectuur uitgave IB5-2019, de stank werd veroorzaakt door een chemische reactie van de drukinkten.

Lilian Knippenberg

COLUMN LEX

Een andere blik

Als analyticus ben ik altijd op zoek naar het volgende model of de volgende standaard die mij helpt mijn werk beter te structureren. Het directe werk van een CISO is heel goed gekaderd, als het goed is: dat het draait om het ISMS en het managen van de beoordelingen en verbeteringen. En dat managen verbreedt je werkveld enorm. Het vergt dat je connecties hebt met en afspraken maakt met vrijwel alle andere afdelingen in het bedrijf en ook buiten het bedrijf.

Het standaard raamwerk dat je als CISO omarmt, helpt je hierbij. De ISO 27001/27002 en afgeleiden hiervan (BIO, NEN 7510) geven je een praktische kijk op best practice maatregelen, het NIST Cybersecurity Framework geeft je een blik vanuit de operationele functies, de CIS Controls vanuit technische thema's. AI die raamwerken hebben een andere zienswijze, en je moet dan nog steeds maatregelen op afdelingen afstemmen. Maatregelen kunnen in verschillende vormen en binnen meerdere afdelingen uitgevoerd worden. Hoe weet je dan wanneer je alles in beeld hebt?

Als consultant spreek ik regelmatig CISO's en andere professionals die mij ook laten zien hoe zij een overzicht houden over hun specifieke werkveld. In de afgelopen jaren ben ik al een paar keer gewezen op mindmap die flink de ronde doet, onder andere op LinkedIn. Het helpt hen maatregelen in te delen naar stakeholder(s), intern en extern.

Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van IB Magazine. Lex is bereikbaar via lex.borger@tesorion.nl

Wat is een mindmap?

Een mindmap is een notatietechniek geschikt voor het overzichtelijk noteren van gedachten of concepten. Hiermee faciliteer je:

- het brengen van een structuur in ongestructureerde informatie;
- creatief denken;
- het oplossen van problemen;
- het communiceren van verbanden.

In een mindmap staat één onderwerp centraal en via uitwaaierende takken wordt het onderwerp verbonden met deelonderwerpen, die op hun beurt weer verbonden worden met daaraan ondergeschikte onderwerpen. Er zijn tools om mindmaps digitaal te maken, zoals iThoughts, Xmind en Freeplane. Deze laatste is open source.

Er is een mindmap van security domeinen opgesteld door Henri Jiang, zelf een Amerikaanse CISO, die precies voldoet aan de structuurbehoefte van een CISO. Elke tak van de mindmap is een wezenlijk ander deel in de wereld van security, alle onderdelen in een domein vind je doorgaans in dezelfde afdeling of in verwante afdelingen. Dit hangt natuurlijk mede af van de aard en grootte van de organisatie. Hij heeft dit vrij snel ontwikkeld van versie 1 tot aan 3. De huidige versie 3.1 lijkt stabiel die is in twee jaar niet meer aangepast.

Domeinen waar een CISO direct mee te maken heeft staan erin:

- governance;
- Enterprise Risk Management (het ISMS en aanverwante zaken).

De typische domeinen die goed ingevuld moeten zijn, maar niet onder een tactische CISO vallen zijn:

- security operations;
- security engineering (hij noemt het security architecture);
- application security.

Andere domeinen zijn weer zaken die met een externe leverancier geregeld of op een andere manier in de organisatie belegd moeten worden. Nu de nieuwe ISO 27001 norm een stuk minder vrijblijvend is over de invulling van maatregelen, kan zo'n mindmap alleen maar helpen om als CISO niet te verdrinken in verplichtingen, maar je wel in de gelegenheid stelt een overzicht te houden. Ik heb het toegevoegd aan mijn standaard toolbox.

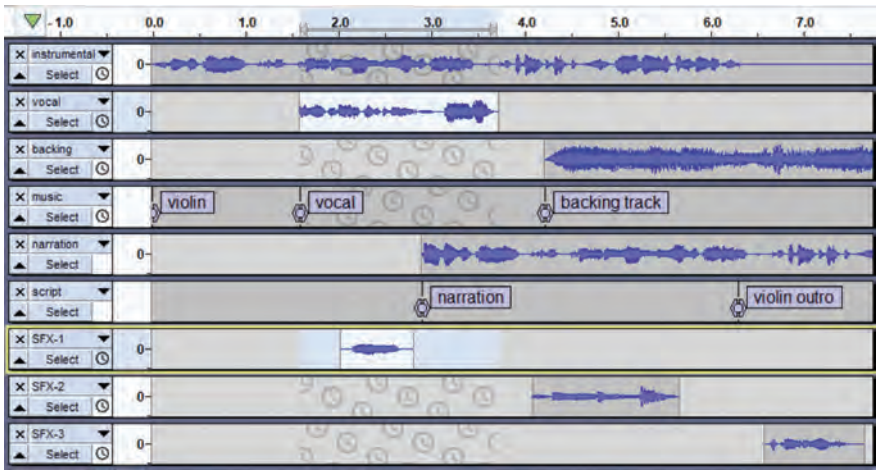
Auteur: Drs. Robert Metsemakers RA RE CISSP is als ervaren auditor en informatiebeveiligingsexpert beschikbaar voor securityadviesopdrachten en bereikbaar op robert.metsemakers@gmail.com.

BLOG

Hoe je zelf een podcast maakt over informatiebeveiliging

Deze keer een aantal tips voor wie een podcast over informatiebeveiliging wil maken. Bij een presentatie zijn drie dingen van belang: vertel het en ze weten het. Laat het zien en ze begrijpen het. Laat ze lachen en ze onthouden het. Met een podcast (een vooraf opgenomen radioprogramma) is dit allemaal mogelijk. Mits je duidelijk en niet te snel spreekt, een goede microfoon gebruikt en een mooie geluidsopname maakt. Die opname oppoetst met filters en geluidseffecten. Beeldende taal en voorbeelden gebruikt. En er wat humor instopt.

Bijna iedereen neemt zijn/haar podcasts op met een Digital Audio Workstation (DAW): een populaire is Audacity. Niet de meest uitgebreide, maar wel beschikbaar voor Windows, IOS en Linux, regelmatig ge-updatet, veel gebruikt (dus met uitlegfilmpjes op YouTube) en bovendien gratis. Het is een digitale meersporenrecorder. Je kunt dus je eigen spraak op een ander kanaal opnemen dan die van je gast. En je kunt dit op verschillende momenten doen! Of je gast maakt thuis een opname en stuurt die naar je toe. Jouw podcast maak je herkenbaar met een begintune (herkenningsmelodie) en een eindtune, die je beide op een ander kanaal opneemt met ieder een eigen volume en fade-out en fade-in, zodat de muziek mooi geleidelijk verdwijnt of opkomt onder de stemmen. Lijkt dat op het verzamelen van security-incidenten, patchlevel-metingen, threat intelligence, gevonden anomalieën uit diverse security-bronnen op één centrale digitale plaats? Ja, best wel.



Meerkanaals opname uit Audacity.

Ben jij weleens opgenomen?

Je kunt een goedkope microfoon kopen bij de Action of een speelgoedwinkel. Beter kun je de microfoon in je mobiele telefoon gebruiken. Die microfoons en digitale verbinding zijn zo goed, dat de stem van een inbellende luisteraar bij een radioprogramma speciaal bewerkt wordt met een geluidsfilter om hem slechter en zo als beller herkenbaar te laten klinken. Die opname op je mobiele telefoon kun je dan importeren in Audacity (1). Je kunt ook een goede externe microfoon van tussen de 30 en 100 euro kopen die aansluitbaar is via USB, dan kun je meteen je podcast inspreken. Of koop een heel goede microfoon (boven 300 euro), die speciaal voor mannen- of vrouwenstemmen is gemaakt. Maar bij zo'n specialistisch apparaat moet je ook een extra stevig statief gebruiken. En een plop/spuugscherm en een speciale ophangveer, omdat die microfoon zo ontzettend gevoelig is. En een voeding bij een condensator-microfoon (altijd) plus een voorversterker als die microfoon slechts weinig output levert. En gebrom van de koelkast of van TL-balken of het passerend verkeer hoor je met een zeer goede microfoon ineens wel in je opname! Het lijkt op de keuzes die je hebt bij antivirus-oplossingen:

1. Gekraakt antivirusprogramma. Gratis, maar wel riskant. Beter om dit niet te doen.
2. Beveiliging tegen malware die in Windows 'gratis' meegeleverd wordt.
3. Bekend antivirusprogramma. Als je security serieus neemt, moet je haast wel. De ingebouwde virusscanner van Windows moet je dan wel uitzetten, als je nog wat processor-capaciteit wilt overhouden.
4. Zelf een antivirusprogramma (laten) ontwikkelen. Als je bijzondere kroonjuwelen hebt of in een speciale militaire operatie zit, kan dit een goed idee zijn, maar het wordt duur door alle bijkomende noodzakelijkheden. Zoals betere monitoring en zelf virussen analyseren om virus-signaturen te bepalen.

Geluidsgrapjes

In PowerPointpresentaties kun je memes gebruiken. Dat zijn foto's en tekeningen, die een positieve associatie oproepen bij jouw publiek en die juist door hun veelvoudig gebruik populair zijn. Bij een podcast kun je een geluidskanaal besteden aan tussengeluidjes. Zoals de 'sad trombone' bij tegenvallend nieuws, de rinkelende kassa, het massale (overdreven) applaus, de drumroffel (voorafgaand aan een belangrijk nieuwtje). In tv-programma's over vakantiepark-eigenaar Peter Gillis of B&B-uitbaters die een levenspartner zoeken, gebruikt men ook een instrumentaal deel (vaak het intro) van een liedje met een toepasselijke titel. 'Sitting on the dock of the bay' (Otis Redding), of 'We are the Champions', 'Another One Bites the Dust' (beide Queen) of 'Money' (Pink Floyd). Zonder de tekstmatige verwijzing er al te dik op te leggen, betrek je zo het onbewuste van de luisteraar bij jouw podcast.

Vormgeving

Kanaalinhoud:

1. Begin- en eindtune (meestal instrumentaal);
2. Jingles ('u luistert naar', 'en dan nu', 'dit was het', 'de volgende podcast verschijnt…');
3. Spraak van de podcast-maker;
4. Spraak van gasten (ieder een eigen kanaal afgestemd op hun spreekvolume);
5. Inbellers (niet teveel studiogeluid terugsturen naar een inbeller, want dat gaat rondzingen, dit is waar de vakterm 'feedback' vandaan komt);
6. Grappige geluidjes, sfeergeluiden (voetstappen op grind, krakende deuren, inbelmodem, of de eerder genoemde geluiden) en
7. Muziek (als je per se veel gedoe met Buma/STEMRA en auteursrechtenvertegenwoordigers wilt).

Dicht met je mond bij de microfoon spreken geeft door het 'proximity' effect meer bas en 'warmte' en ook meer impact

Al het andere dan jouw stem heet 'vormgeving'. Jingles (korte tekst met muziek), bumpers (alleen spraak), tunes (langer met muziek), het bestaat allemaal in audioland en jij kunt het natuurlijk overdreven vinden. Echter, ook als je 'alleen maar' een podcast maakt voor intern gebruik binnen jouw eigen afdeling of organisatie, moet je als podcast-maker om aandacht concurreren met alle overige (eerdere, professionelere (2)) makers. Leuke aankleding helpt verkopen.

Proces versus inhoud

In podcasts over 'cold cases' (jarenlang niet opgeloste moordzaken waar een team rechercheurs toch maar weer eens naar zijn gaan kijken) hoor je vaak een meta-kanaal. De presentator geeft daar commentaar op het maakproces van de podcast: 'twee maanden later kregen we antwoord'. Of hij licht de beroerde kwaliteit toe van de geluidsopname van de hoofdverdachte: 'stiekem vanuit een boodschappentas gemaakt'. Die toelichtende stem klinkt dan altijd anders: via galm, een lichte echo, minder bas in de stem via een (EQ) filter. Of het is de stem van de buurvrouw op kantoor, de barrista (als je bij Starbucks je podcast opneemt) of een familielid (bij 'thuiswerken'). Die andere klank maakt de podcast gemakkelijker te begrijpen. Vergelijk het met een security rapportage waarin je vetgedrukte paragrafen en tussenkopjes gebruikt, in elke week dezelfde vaste volgorde. Lege paragrafen (kopjes zonder tekst eronder) zijn daarbij óók – geruststellende – informatie voor de lezer.

Mitigerende maatregelen

Neem stemmen zo droog mogelijk op. Voeg effecten of filtering pas later toe in postproductie. Zeg vaak: 'dat los ik wel op in post-productie' tegen je gasten, dat klinkt deskundig. Security incidenten laat je immers door de diverse experts van jouw security-afdeling ook zo sec en gedetailleerd mogelijk eerst in een database zetten. En daarna gaat een (andere) rapportage-expert ermee aan de slag om een mooi rapport te maken over die week. Je laat niet iedere securitymedewerker meteen in het format van de securityrapportage schrijven, toch? Kortom: eerst de feiten goed en zo droog/zakelijk mogelijk vastleggen, daarna presentatie en versieringen aanbrengen. Als de opnameruimte (op locatie) een hinderlijke galm heeft, is jouw stem minder goed te verstaan. Dan kun je tijdens het inspreken een handdoek of deken over je hoofd hangen. Dit geldt niet voor vloggers.

Als je veel beweegt achter de microfoon omdat je links en rechts documenten en spullen moet pakken of omdat je na elke pauze (of verspreking…) weer anders gaat zitten. Of omdat je de wekelijkse podcast in delen op drie verschillende dagen opneemt. Dan zou ik je het liefst vastpakken, door elkaar schudden en schreeuwen: 'stop it!' Maar omdat je dat allemaal waarschijnlijk toch blijft doen, kun je als alternatief een compressor-effect op elk spraakkanaal zetten. Een compressor haalt de dynamiek uit je stem, door alle harde stukken zachter en alle zachte stukken (bijvoorbeeld omdat die persoon verder van de microfoon weg zit) luider te maken. Iedere stem, microfoonafstand en spreektechniek heeft eigen compressor-instellingen nodig. In welke mate en hoe sloom of snel de compressor de volumes corrigeert, zijn instellingen (attack, release) waarmee je moet spelen.

'Hoe krijg ik een filmtrailer stem?'

Dicht met je mond bij de microfoon spreken geeft door het 'proximity' effect meer bas en 'warmte' en ook meer impact. Maar, vergelijk dit met de manager van de security-afdeling die zich plots inhoudelijk diepgaand met één bepaald incident gaat bemoeien. Dat incident krijgt dan ook veel aandacht, maar het wordt al snel vermoeiend voor de rest van de organisatie. Een redelijke afstand tot microfoon (zoals een 'handbreedte') is beter. Geen melk drinken, dat werkt negatief op je slijm. Beperkt koffie, wel water. Thee met honing helpt een beetje bij een vermoeide keel. Gebruik gewoon je eigen stem, dat komt 'echt' en 'integer' over bij de luisteraar.

Erin en eruit monteren

Stopwoordjes en tussenwerpsels (‘euh’) kun je wegknippen. Al het ademhalen óók, maar kijk uit dat het niet onnatuurlijk gaat klinken. Vooral als je de voor te lezen tekst door ChatGPT laat schrijven. Ook achtergrondgeluid kun je deels verwijderen. Neem daarvoor een kort stukje achtergrondgeluid op, voordat je begint met spreken. Dat stukje is als ‘noise profile’ te gebruiken voor de ‘noise reduction’ (in Audacity). Na een tijdje monteren van podcasts ontdek je dat je woorden als ‘niet, geen, never’ heel gemakkelijk kunt verwijderen of verplaatsen in de spraakopnames. In het algemeen vindt men dit onethisch: bijvoorbeeld als jouw gast ineens beweert dat hij ergens wél een actieve herinnering aan heeft. Door ‘wel’ iets luider te maken, lijkt de klèmtoon daar te liggen.

Meersporenbeleid

Bij ‘meersporenbeleid’ gaat het niet alleen over treinen. Door te werken met meerdere sporen kun je diverse opnamen op verschillende momenten maken. Je kunt ook kanalen hergebruiken voor de volgende postcast: bijvoorbeeld die met begin- en eindtune en tussendoor-jingles. Tussengeluiden kun je in de nieuwe podcast dan naar voor (eerder) of achter (later) verschuiven om ze op het juiste tijdstip te zetten. Zoals je dat ook doet met een securityrapportage-template met tussenkopjes zoals ‘datalekken/USB’, ‘DOS-aanvallen’, ‘ransomware’, ‘phishingmails’, ‘gestolen versleutelde laptops’. De paragraaflengte varieert natuurlijk. Selectie en volgorde van grappige tussengeluidjes in jouw podcast zou ik regelmatig aanpassen om het afwisselend te houden.

Beste versie van jezelf

Bij een verspreking, kun je beter opnieuw beginnen met inspreken vanaf het begin van de alinea of de zin waarin het fout ging. Meestal haal je namelijk even adem tussen twee alinea’s of (lange) zinnen. Dat is een mooi punt om een montage of ‘las’ te maken. Onder 150 Hz zit weinig menselijke stem, maar wel allerlei stoor- en stootgeluiden. Wegfilteren dus met een highpass-filter (dat geluid boven een door jou in te stellen frequentie doorlaat). Mensen zingen graag in badkamers omdat door de weerkaatsing tegen tegels hun stem voller klinkt. Dit is na te bootsen met een nagalm (reverb) effect op je stem. Neem wel een korte, die als ‘preset’ vaak gewoon ‘bathroom’ heet.

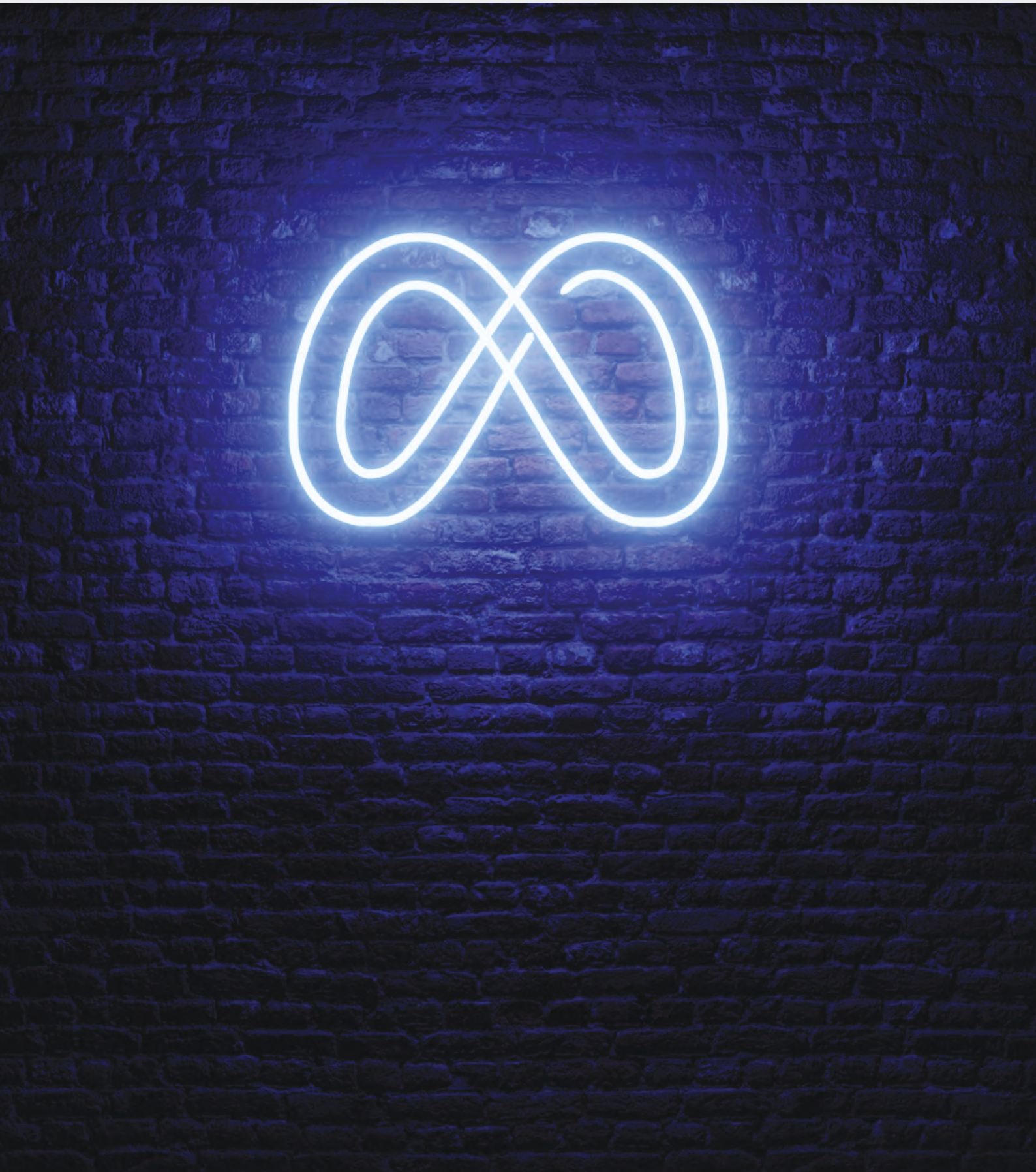
Toi toi toi. Ik hoor graag van je.

Referenties

(1) Zie bijvoorbeeld: https://www.lifewire.com/how-to-use-audacity-for-podcasts-4802258

(2) Bron van het plaatje: https://manual.audacityteam.org/man/sync_locked_track_groups.html

Auteur: mw. mr. Caroline van Ekeren is werkzaam bij ICTRecht, kantoor Amsterdam in de functie van Legal Consultant IT & Privacy. Zij is bereikbaar via: c.vanekeren@ictrecht.nl



Hoe Meta met één advertentie gedreven bedrijfsmodel op twee manieren onrechtmatig handelde

Twee vliegen in één klap

Op 15 maart 2023 publiceerde de rechtbank Amsterdam een uitspraak tussen de Data Privacy Stichting (de Stichting) en Facebook. Deze uitspraak ging over het onrechtmatig gebruik van persoonsgegevens en de oneerlijke handelspraktijk die Facebook, nu verdergaand onder de naam Meta, verrichtte tussen 2010 en 2020. Meta doet het goed fout volgens de rechter. Het feit dat Meta zo onrechtmatig handelt zal voor veel mensen niet nieuw zijn, maar de overwegingen daartoe zijn wel interessant.

In dit artikel leg ik je uit wat er gebeurde in deze zaak en waarom. Allereerst zet ik de feiten en de vorderingen van de zaak uiteen. Daarna ga ik in op waarom Meta onrechtmatig persoonsgegevens gebruikte volgens de regels van de Algemene verordening gegevensbescherming (AVG, en haar wettelijke voorganger), en behandel ik de vordering van de Stichting waarin ze stelt dat Meta een oneerlijke handelspraktijk verricht met de manier waarop zij de Facebookdienst in de markt zette. Dit alles met het doel om hier weer lessen uit te trekken. Waar moeten we voor uitkijken? Hoe interpreteert de rechter de AVG en het Burgerlijk Wetboek (BW) – dat 'boek' dat al eeuwenlang (1838) bestaat en nu toegepast moet worden op de digitale wereld?

1. De zaak

De Stichting die Meta voor de rechter sleepte is een collectieve belangenorganisatie die als doel heeft privacyrechten effectief te beschermen. Facebook is een online platform van Meta Ierland dat gebruikt wordt door consumenten voor onder meer contact met vrienden, familie en anderen. In dit artikel duiden we Meta Ierland (eerder bekend als Facebook Ierland) aan met 'Meta', en het platform zelf met 'Facebook' of 'de Facebookdienst'.

Eind 2014 stelde de Nederlands privacytoezichthouder, de Autoriteit Persoonsgegevens (AP) een onderzoek in naar het verwerken van persoonsgegevens (informatie over personen) door Meta in Nederland. In het rapport uit 2017 zegt de AP dat Meta de Wet bescherming persoonsgegevens (Wbp) schendt, de voorganger van de huidige privacywet. De AP ondernam geen actie meer tegen Meta naar aanleiding van de bevindingen, maar de Stichting ziet het rapport als onderbouwing van haar stellingen.

1.1 Wat vordert de Stichting?

De Stichting vordert in deze zaak dat de rechtbank oordeelt dat Meta toerekenbaar onrechtmatig handelde ten opzichte van haar gebruikers door:

- artikelen 12, 13 en 14 AVG te schenden, doordat
  (1) externe ontwikkelaars toegang hadden tot persoonsgegevens van de gebruikers en die gebruikten zonder dat de consumenten dat wisten,
  (2) Meta telefoonnummers (afgegeven voor tweefactor authenticatie (2FA)) van gebruikers ook gebruikte voor gerichte advertenties;
- artikelen 5 en 6 AVG te schenden door (bijzondere) persoonsgegevens te verwerken van gebruikers zonder grondslag;
- de cookieregels uit artikel 11.7a Telecommunicatiewet (verplicht toestemming vragen en krijgen in lijn met artikel 7 AVG) te schenden;
- oneerlijke handelspraktijken te verrichten (artikel 6:193b-d BW) door
  - consumenten (gebruikers) niet op tijd te vertellen over het gebruiken en delen met andere organisaties van persoonsgegevens over hen om daarmee winst te maken;
  - onduidelijk te zijn over hoe groot het gebruik van die persoonsgegevens over de consumenten was; en
  - de consumenten te vertellen dat het gebruik van Facebook volledig gratis was, terwijl in feite werd betaald door de consumenten met (vertrouwelijke) persoonsgegevens over zichzelf.

Dat 'toerekenbaar onrechtmatig' is relevant als consumenten na deze procedure, als is gebleken dat het handelen van Meta onrechtmatig was, schadevergoeding willen gaan eisen. Het komt erop neer dat, als een handeling of situatie toerekenbaar onrechtmatig was, er een juridische reden bestaat om Meta aan te schrijven en een schadevergoeding te eisen. Ik loop hierna door de vorderingen van de Stichting en het oordeel van de rechter heen, maar eerst nog wat achtergrondinformatie.

2. Wat deed Meta met persoonsgegevens?

Iedereen die lid werd van de Facebookdienst maakte een account aan en vulde daarvoor allerlei persoonsgegevens in. Die informatie had Facebook over de gebruikers, maar aanvullend worden door de activiteiten die een gebruiker uitvoert op Facebook ook nog veel persoonsgegevens verzameld. Welke informatiepagina's ze leuk vinden ('tuinieren voor ouderen'), met wie ze vrienden of familie zijn ('kusjes van oma'), of ze een relatie hebben en in welk gender ze qua liefdesrelatie geïnteresseerd zijn ('vrijgezel', 'panseksueel'), of ze kinderen hebben en ga zo maar door. Al deze informatie vormt een gedetailleerd plaatje van een persoon. Hieronder zet ik uiteen waarom en hoe bepaalde persoonsgegevens gebruikt werden door Facebook.

Delen met externe ontwikkelaars: Vanaf 2010 gebruikte Facebook een API waarmee externe ontwikkelaars (bouwers van applicaties of websitebeheerders) hun applicatie konden aansluiten op de Facebookdienst. API staat voor Application Programming Interface, dat is kort gezegd een technologie gebruikt om gegevens uit te wisselen tussen apps. Deze API sloot games of quizzen aan op de Facebookdienst. Diezelfde technologie maakte het mogelijk dat mensen via Facebook konden inloggen bij andere diensten van derde partijen (zoals AirBnB, Spotify en Netflix). Na toestemming kreeg de externe ontwikkelaar toegang tot persoonsgegevens over de gebruiker en zijn Facebookvrienden, en kon zelfs ook zelf (persoons)gegevens verzamelen.

Gebruik voor advertentiedoeleinden: Facebook gebruikte de door de gebruikers ingediende persoonsgegevens en de tijdens gebruik verzamelde persoonsgegevens (dus het: wie zijn je vrienden, familie, wat vind je leuk etc.) ook voor gepersonaliseerde advertenties. Meta exploiteert een 'advertentie gedreven bedrijfsmodel'. Daarbij kan je als adverteerder vragen aan Meta om jouw advertentie te laten zien aan een (zeer) specifieke doelgroep. De adverteerder betaalt Facebook vervolgens per aankoop die via hen doorkomt, en de adverteerder laat het aan Facebook weten als een Facebookgebruiker op haar website komt (zie 'Cookies'). Om dat allemaal te bewerkstelligen, deelt Meta persoonsgegevens over gebruikers met de adverterende derde partijen. Meta gebruikte hiervoor ook het telefoonnummer dat Facebookgebruikers indienden om 2FA in te stellen.

Cookies: Meta verzamelde gegevens door informatie te delen met derde partijen die Facebook informeerden als een gebruiker bij hen op de website langs is geweest. Als ik een Facebookaccount had, gaf Meta mij een bepaald uniek tracking nummer dat vervolgens herkend wordt als ik zit te zoeken naar een treinreis naar Triberg im Schwarzwald, bijvoorbeeld. Zo krijg je een nóg gedetailleerder plaatje van de bezoeker, want Caroline uit regio Amsterdam die jurist is (informatie van Facebookpagina) wil ook graag met de trein reizen naar Duitsland (informatie van derde partijen). Die gegevens zijn waardevol om mij weer de juiste advertenties te laten zien, die zorgen dat ik producten en diensten koop, zoals een kekke to-go mok.

3. Hoe ging 'privacy' mis bij Facebook?

3.1 Niet goed geïnformeerd

Meta was niet duidelijk genoeg over de reden dat de persoonsgegevens met derde partijen werden gedeeld. Dat is wel verplicht volgens artikel 13 en 14 AVG. Meta moest die noodzakelijke informatie (de doeleinden) in een pop-up venster tonen vóór het delen van de persoonsgegevens. Niet in een gegevensbeleid waarin je zelf moet zoeken, zoals Meta dat deed. Een verwijzing naar het gegevensbeleid in het pop-up venster had ook voldoende kunnen zijn, maar die was er niet. De algemene verwijzing naar het gegevensbeleid is onvoldoende. Dat Metagebruikers aanraadde het beleid te lezen (waar die informatie in zou staan), verandert niet de verplichting die Meta zelf had om de gebruikers, op een juiste manier, actief te informeren.

Bovendien was Meta niet duidelijk over het doorspelen van persoonsgegevens over de gebruikers en hun Facebookvrienden naar de externe ontwikkelaars. Het stond op een gegeven moment wel ergens in hun openbare beleidstukken, maar heel erg onduidelijk en verhuld tussen 30 pagina's aan wollige tekst.

In de procedure wordt ook niet duidelijk waaróm die externe ontwikkelaars eigenlijk toegang kregen tot al die (persoons)gegevens. Voor de functionaliteit om via Facebook in te loggen op een externe app, is het delen van al die persoonsgegevens zeker niet noodzakelijk.

3.2 Onrechtmatig gebruik voor advertentiedoeleinden

Om rechtmatig persoonsgegevens te gebruiken is een grondslag uit artikel 6 AVG nodig. Meta heeft geen grondslag om de persoonsgegevens van gebruikers en hun Facebookvrienden te verwerken voor advertentiedoeleinden. Meta beriep zich op meerdere grondslagen, die de rechter allemaal afwees. Op 4 juli 2023 is dit oordeel van onze Nederlandse rechter kracht bijgezet door de hoogste Europese rechter. Het Hof van Justitie van de Europese Unie oordeelde dat de grondslagen contractuele noodzakelijkheid en het gerechtvaardigd belang (komt hieronder aan bod) zelfs niet passen bij het gebruik van gepersonaliseerde advertenties. Alleen toestemming is mogelijk, maar het lukte Meta (in deze en de Europese zaak) niet om die op de juiste manier te verkrijgen.

Optie 1: artikel 6 lid 1 onder b AVG, contractuele noodzakelijkheid

Meta stelde dat het gebruik voor advertentiedoeleinden noodzakelijk is voor het contract met de gebruiker om hun Facebookdienst te leveren. De Facebookdienst is een gepersonaliseerde dienst, met gepersonaliseerde inhoud, inclusief advertenties. Gepersonaliseerde advertenties vallen zo onder de kern van Meta's dienstverlening en zijn noodzakelijk voor het naleven van het contract, aldus Meta.

De rechter oordeelt dat deze grondslag niet van toepassing kan zijn. Het gebruiken van de persoonsgegevens voor advertentiedoeleinden is niet (strikt) noodzakelijk voor de uitvoering van de overeenkomst tussen de gebruiker en Meta. Die overeenkomst ziet op het aanbieden van een profiel op een sociaal medianetwerk. Dat de verwerking van bepaalde gegevens valt onder een bepaalde overeenkomst, betekent niet dat het ook noodzakelijk is voor de uitvoering van die overeenkomst. Volgens de rechtbank is deze grondslag "geen geschikte rechtsgrond voor het opstellen van een profiel over de smaak en levensstijl van de gebruiker op basis van zijn klikgegevens op een website en de aangeschafte goederen." De voor de verwerking verantwoordelijke is namelijk niet aangesteld om een profiel op te stellen, maar om bijvoorbeeld bepaalde goederen en diensten te leveren.

Optie 2: artikel 6 lid 1 onder a AVG, toestemming
Meta zegt dat de gebruikers toestemming gaven doordat zij bij het aanmaken van een account bevestigden dat zij het gegevensbeleid van Facebook hadden gelezen, door op de knop 'registreren' te klikken. Meta zegt dat er duidelijk stond dat zij de verzamelde persoonsgegevens gebruikte om advertenties te personaliseren.

Anders dan Meta vindt, kan de 'leesbevestiging' het gegevensbeleid van Facebook niet gezien worden als het verkrijgen van rechtsgeldige toestemming van een gebruiker, ook niet onder de Wbp. De rechter verduidelijkt dat zulke stilzwijgende of impliciete toestemming onvoldoende is om geldige toestemming te verkrijgen. Het registratieproces was niet zo ingericht dat het duidelijk was dat Facebook toestemming vroeg voor het gebruik van de persoonsgegevens voor advertentiedoeleinden.

Optie 3: artikel 6 lid 1 onder f AVG, gerechtvaardigd belang
Onder dit artikel kan je persoonsgegevens verwerken als het noodzakelijk is voor het behartigen van een gerechtvaardigd belang. Voor een geslaagd beroep op deze grondslag, moet het belang (1) gerechtvaardigd zijn, (2) zwaarder wegen dan de rechten en vrijheden van betrokkenen die in het gedrang zijn, en (3) aan de noodzakelijkheidstoets voldoen. Dat laatste betekent dat het middel (de verwerking) in verhouding moet staan tot het doel (proportionaliteit), en dat het belang niet op een minder vergaande wijze te behartigen is (subsidiariteit). Zo hoef je geen cameratoezicht in te zetten omdat een kind van 4 een snoepje stal. De intensiteit van die privacy-inbreuk staat niet in verhouding tot het doel en je kan ook gewoon kinderen wat beter in de gaten houden in de Kruidvat.

Meta gebruikt een advertentie gedreven bedrijfsmodel, waarbij ze de dienst alleen gratis kan aanbieden als ze gepersonaliseerde advertentieruimte verkoopt. Daarom heeft zij een gerechtvaardigd belang de persoonsgegevens te gebruiken voor advertenties, aldus Meta. Haar belang zou zijn om 'een gepersonaliseerde ervaring' aan te bieden (verschillende termen worden voor dat belang gebruikt in deze uitspraak). Volgens Meta doet haar belang behartigen, geen afbreuk aan de fundamentele rechten en vrijheden van gebruikers. Als dat wel zo zou zijn, weegt haar belang alsnog zwaarder. Gebruikers

hadden immers moeten weten dat hun persoonsgegevens op deze manier werden gebruikt bij een gratis dienst. Hoe kunnen ze anders als bedrijf overleven?

De rechtbank is het niet eens met Meta.

De rechter zegt dat het gerechtvaardigd belang van Meta dat "mede" bestaat uit gepersonaliseerde ervaring bieden (waaruit dan nog meer..?) samenhangt met het advertentie gedreven bedrijfsmodel van Facebook. Zo "bestaat een legitiem economisch belang" (aldus de rechtbank). De rechter vindt dat een commercieel belang een gerechtvaardigd belang kan zijn (dit ligt voor bij de hoogste Europese rechter of dat echt zo is) en gaat er "veronderstellende wijs" vanuit dat Meta een gerechtvaardigd belang had.

Dat gerechtvaardigd belang dat 'mede' bestaat uit een gepersonaliseerde ervaring aanbieden, redt het niet door de rest van de toets. Het faalt op noodzakelijkheid. Meta is daar zelf in haar stukken niet op ingegaan en weerlegde de punten van de Stichting onvoldoende. Dat komt erop neer dat het volgens de rechter niet noodzakelijk is om de persoonsgegevens te gebruiken voor gepersonaliseerde advertenties, om de gepersonaliseerde ervaring (gerechtvaardigd belang) te realiseren - of misschien is dat niet de visie van de rechter, maar in ieder geval gaf Meta niet genoeg input aan de rechter om hun daarvan te overtuigen.

3.4 Onrechtmatig gebruik bijzondere persoonsgegevens

Uit profielvelden en iemands surfgedrag kan je bijzondere persoonsgegevens afleiden, zoals iemands seksuele geaardheid. Voor gebruik van bijzondere persoonsgegevens is aanvullend op artikel 6, ook een grondslag uit artikel 9 AVG nodig. Meta gebruikte bijzondere persoonsgegevens om de gepersonaliseerde advertenties te realiseren, zonder artikel 9 grondslag. Zij verwerkt dit dus (ook) onrechtmatig.

Een klein voorproefje van wat komen gaat, want vanaf 17 februari 2024 (voor de kleinere partijen, al sinds augustus 2023 voor de grootste partijen) mogen online platforms op basis van de Digital Services Act überhaupt geen bijzondere persoonsgegevens gebruiken voor het tonen van reclames op basis van profilering.

3.5 Onrechtmatig gebruik van volgtechnieken

Meta gebruikte cookies en andere volgtechnieken om informatie over het surfgedrag en appgebruik van gebruikers buiten Facebook te verzamelen. Voor zulk gebruik moet je toestemming verkrijgen volgens de (strenge) eisen uit de AVG. Meta zegt dat die verplichting niet aan hen is, maar aan de partij van wie ze die informatie krijgen (websites/apps). Daar gaat de rechter niet in mee. Degene die verantwoordelijk is voor het plaatsen van de tracking-gegevens in apparaten zoals laptops en telefoons, en het verkrijgen van toegang tot die gegevens, moet aan de toestemmingsverplichtingen voldoen. Omdat de third party cookies op Meta's verzoek worden geplaatst, is zij verantwoordelijk voor het naleven van de cookieregels.

4. Hoe handelde Meta onrechtmatig?

4.1 Meta's oneerlijke handelspraktijk uitgelegd

Oneerlijke handelspraktijken zijn situaties waarbij een handelaar misleidend of oneerlijk is tegenover een consument en daardoor de consument aanzet tot handelen, welke zij anders niet zou doen. Oneerlijke handelspraktijken zijn verboden, volgt uit de Richtlijn Oneerlijke Handelspraktijken (OHP) verankerd in de Nederlandse Wet oneerlijke handelspraktijken. Als een organisatie een oneerlijke handelspraktijk verricht tegenover een consument, handelt de organisatie onrechtmatig. Zo'n onrechtmatige daad kan leiden tot allerlei nare consequenties voor de organisatie, de consument kan bijvoorbeeld schadevergoeding eisen.

De Stichting stelt dat Meta met de Facebookdienst een oneerlijke handelspraktijk verrichtte. Er zijn verschillende manieren waarop een organisatie een oneerlijke handelspraktijk kan verrichten. De Stichting stelde dat het op de volgende twee manieren mis ging.

1) De handelaar presenteert informatie over zijn dienst(en) aan de consument die feitelijk onjuist is (6:193c lid 1 BW).

Hoewel Meta zei dat de Facebookdienst gratis was, betaalden consumenten met hun persoonsgegevens. De Facebookdienst is daarom níet gratis volgens de Stichting. Persoonsgegevens kunnen namelijk gezien worden als 'een prijs' in de zin van de

Richtlijn OHP. Daarin is overigens geen gekaderde definitie te vinden van 'een prijs'.

Deze gratis verklaring "kan (..) worden opgevat als de mededeling dat voor het gebruik maken van de dienst geen geldelijke tegenprestatie hoeft te worden verricht. Aangezien vaststaat dat er geen geld hoeft te worden betaald voor de Facebookdienst, is de gratis verklaring in de relevante periode op zichzelf beschouwd in zoverre dus niet misleidend." (§17.16), aldus de rechter. Dat de persoonsgegevens gezien kunnen worden als een geldelijke prijs, vindt de rechtbank niet overtuigend genoeg.

2) De handelaar presenteert misleidende informatie over de dienst aan de consument. Door die misleidende informatie nam de consument een besluit dat hij anders niet had genomen, en ging een overeenkomst aan die hij anders niet was aangegaan (artikel 6:193d lid 2 en 3 BW).

In dit geval deed Meta dat volgens de Stichting doordat zij over verschillende essentiële onderwerpen onduidelijk was.

De rechter is het met de Stichting eens. Meta was te onduidelijk over hoe zij de informatie die gebruikers invulden gebruikte, en over het advertentie gedreven bedrijfsmodel. Meta verdiende geld door persoonsgegevens van Facebookgebruikers en hun vrienden te gebruiken voor gepersonaliseerde advertentieruimte en deelde die persoonsgegevens ook met derde partijen voor dat doel, terwijl dat niet per se nodig was. Daar had Meta duidelijker over moeten informeren zodat de consument een weloverwogen keuze kon maken om lid te worden.

Dat Meta ook nog riep dat de Facebookdienst helemaal gratis was, maakt het allemaal nog onduidelijker voor de gebruikers, vindt de rechter. Dat dat gebruik van persoonsgegevens wel érgens in Facebook 's privacybeleid stond, verandert dat niet. De rechter vindt het privacybeleid van de Facebookdienst niet duidelijk genoeg. Meta gebruikte 'verhuld taalgebruik' en verstopte relevante punten over het gebruik van persoonsgegevens in een 'onderliggende informatielaag'.

Dat Meta niet vertelde dat ze de persoonsgegevens gebruikte voor gepersonaliseerde advertenties, ziet de rechter als een 'misleidende omissie'. Dit was essentiële informatie om de gemiddelde consument een weloverwogen besluit te laten nemen volgens de rechtbank. Zeker door de schaalgrootte van het gebruik van (bijzondere) persoonsgegevens voor advertentiedoeleinden en het delen van die informatie met derden. Dergelijke essentiële informatie weglaten is misleidend. Meta pleegt zo een oneerlijke handelspraktijk.

4.2 Meta's ongerechtvaardigde verrijking?

De Stichting vindt dat Meta zich ongerechtvaardigd verrijkte (artikel 6:212 lid 1 BW). Een ongerechtvaardigde verrijking is een situatie waarbij de een is verrijkt (rijker geworden) ten koste van een ander, die 'verarmt'. Ook dat is in het civiel recht onrechtmatig. De vereisten voor een succesvol beroep op ongerechtvaardigde verrijking zijn de volgende:

1. Verarming (schade);
2. Verrijking (vermogensvermeerdering);
3. Een verband tussen de verrijking en de verarming;
4. De verrijking moet ongerechtvaardigd zijn in de zin dat er geen redelijke oorzaak of rechtvaardigingsgrond voor bestaat.

De Stichting stelde dat de persoonsgegevens die Meta gebruikte een economische waarde vertegenwoordigen (zonder economische waarde is er geen verrijken of verarmen). Dat kan je zien doordat Meta's winst en vermogen met (het gebruik van) die persoonsgegevens toenam. Dat is ongerechtvaardigd volgens de Stichting omdat er geen grondslag was voor het gebruik van die persoonsgegevens (artikel 6 AVG).

De rechtbank legt uit dat deze persoonsgegevens overduidelijk waarde hebben voor Meta. Meta's gehele dienst is erop gebaseerd winst te genereren met het gebruik van persoonsgegevens en haar vermogen en winst zijn ook door dat gebruik vergroot. Dat komt omdat Meta de informatie zo gebruikt, dat het tot een personalisatie komt die goed te verkopen is aan derde partijen.

Voor de gebruiker is de waarde van de persoonsgegevens anders. De gebruiker wordt niet 'aangetast in haar vermogen' (wordt niet armer) volgens de rechtbank, als Meta zich verrijkt met de persoonsgegevens. Daarom is een ongerechtvaardigde verrijking niet mogelijk. De gebruiker 'verarmt' namelijk niet.. Hoewel Meta wel 'verrijkt'.

5. Samenvattend vooruitkijken: transparantie viert zege

Meta gebruikte persoonsgegevens onrechtmatig. Ze had geen

grondslag voor het gebruik van de betrokken persoonsgegevens voor advertentiedoeleinden, en informeerde gebrekkig en onduidelijk. Naast de inbreuken op de AVG, verrichte Meta – met hoe zij de Facebookdienst in de markt zette - een oneerlijke handelspraktijk. Meta was misleidend naar de Facebookgebruikers over hoe zij hun persoonsgegevens gebruikte om advertenties te verkopen en hoe groot die markt wel niet was. Zowel op basis van een oneerlijke handelspraktijk, als een inbreuk op de AVG, kan een consument schadevergoeding eisen.

Dit verhaal kan dus nog een staart krijgen, zeker als je kijkt naar de (enigszins nieuwe) Wet afwikkeling massaschade in collectieve actie (Wamca), waardoor een stichting namens meerdere consumenten schadevergoeding kan claimen. Verschillende stichtingen, digitale burgerrechtenorganisaties en de Consumentenbond zijn langzaamaan voorlopers aan het worden in het aankaarten van deze – (nog) naar het schijnt – shady praktijken: ze proberen aandacht te trekken voor de oneerlijke of onrechtmatige praktijken waar consumenten (onbewust?) slachtoffer van worden. Ze trekken alles uit de kast

Eerlijkheid duurt het langst, ook in het geval van privacy. You have nothing to fear if you have nothing to hide…

om de stoffige wetten op de digitale praktijk te plakken: privacywetten, grondrechten, creatieve en nieuwe interpretaties van het onrechtmatige daad verhaal in ons BW.

Maar alleen een inbreuk op je privacy levert nog geen vergoedbare schade op. Je moet wel aantonen dat er echt schade is, anders valt er niks te vergoeden. Desalniettemin is in Duitsland al meerdere malen schadevergoeding gehaald bij de rechter door het onrechtmatig gebruik van Google Analytics. Zo gemakkelijk gaat dat niet in Nederland, omdat (1) volgens civiel recht de immateriële schade aantoonbaar moet zijn (2) en een causaal verband bewezen. Beiden zijn een uitdaging als het gaat om een inbreuk op privacy door onrechtmatig gebruik van persoonsgegevens. Dat zal ook zo zijn bij een oneerlijke handelspraktijk, als persoonsgegevens voor de betrokkene geen economische waarde representeren.

Wat er gaat gebeuren met Meta daargelaten, zijn er belangrijke lessen te trekken uit deze uitspraak. Er is een overkoepelend onderwerp dat lijkt ten grondslag te liggen aan zowel de inbreuk op de AVG als op het BW: het gebrek aan transparantie.

Een van de kernpunten die belangrijk is als het gaat om het gebruik van persoonsgegevens, is transparantie: duidelijk vertellen wat je doet met persoonsgegevens. Met duidelijk bedoel ik echt duidelijk: liever een kern aan punten helder met een infographic, dan tientallen pagina's aan privacybeleid.

Veel organisaties zijn terughoudend in vertellen over het werken met partijen uit de Verenigde Staten of het gebruiken van persoonsgegevens voor andere doeleinden dan alleen de overeenkomst te sluiten. Dit hoewel transparantie toch aan te raden is. Niet alleen omdat de AVG dat voorschrijft, maar vooral omdat consumenten niet voor verrassingen willen komen te staan. Je ziet in de praktijk dat veel consumenten het bijvoorbeeld best fijn vinden als ze zo nu en dan acties of kortingen hun kant opgestuurd krijgen. Maar als dat gebeurt zonder dat ze wisten dat ze marketing e-mails zouden ontvangen, is de nasmaak van zo'n e-mailtje enigszins bitter: hoe kwamen zij aan mijn e-mailadres? Wanneer heb ik ooit wat van deze organisatie gekocht? En zo'n gevoel is het laatste dat je wil creëren bij je doelgroep.

Deze uitspraak over Meta's oneerlijke handelspraktijk benadrukt wederom de relevantie van transparantie als het gaat om het gebruik van informatie over consumenten. De uitspraak illustreert hoe transparantie de kern van bedrijfsvoering hoort te zijn als het gaat om werken met informatie over personen. Het is relevant vanuit een breder juridisch perspectief, en keert in specifieke regels terug in zowel de AVG als het BW. Eerlijkheid duurt het langst, ook in het geval van privacy. You have nothing to fear if you have nothing to hide…

Dimitri van Zantvliet is Directeur Cybersecurity bij de Nederlandse Spoorwegen

COLUMN DIMITRI

Van Socrates tot siliconen...

In een tijdperk waarin de onvoorspelbaarheid, de veelzijdigheid en de continue metamorfose onze realiteit kenmerken, vinden filosofie, leiderschap en cybersecurity elkaar op intrigerende wijze. Ik schreef er op LinkedIn reeds een stukje over. Zoek me daar vooral even op voor de uitgebreidere versie (en link ook gelijk even).

Het stoïcisme, de antieke filosofie die een voorliefde toont voor rationaliteit en introspectie, verschaft ons een kompas door het tumultueuze terrein van cybersecurity en het existentiële bestaan. Daarnaast propageert de Oneindige Speltheorie een paradigma van aanhoudende adaptatie en veerkracht in het cyberlandschap, transcenderend boven de beperkte blik op finiete triomfen. De doctrines VUCA (Volatility, Uncertainty, Complexity, Ambiguity) en BANI (Brittle, Anxious, Non-linear, Incomprehensible) verhelderen de gelaagde aard van chaotische globale infrastructuren en stellen ons in staat tot strategisch manoeuvreren.

Het stoïcisme, een eerbiedwaardige Griekse filosofie, heeft de mensheid tijdloze inzichten geschonken over co-existentie met het kosmische orkest. Het benadrukt het credo dat we ons dienen te richten op de facetten des levens die we kunnen sturen en de onvermijdelijkheden dienen te omhelzen. In de sfeer van cybersecurity impliceert dit een resolute, bezonnen respons op dreigingen, het inrichten van een onwrikbaar verdedigingsbastion. Het stoïcisme benadrukt, voorbij technologische ingrepen, de imperatief van een intrinsiek veiligheidsethos.

De Oneindige Speltheorie transcendeert afgebakende einddoelen en bepleit een eeuwige deelname, assimilatie en evolutie. Cyberbedreigingen zijn in een constante staat van mutatie, met opponenten die hun tactieken continue verfijnen. Deze theorie propageert een visie die het lange termijn panorama van de fluctuerende asymmetrische cyberrealiteit onderschrijft. Organisaties dienen adaptief en coöperatief te opereren, en moeten strategieën hanteren die deze cyberdynamiek kunnen anticiperen en beantwoorden.

In onze turbulent veranderende tijden, schenken de doctrines van VUCA en BANI ons de gereedschappen om de intrinsieke complexiteit van contemporaine vraagstukken te doorgronden. In het kader van cybersecurity accentueren deze paradigma's de noodzaak van wendbaarheid, luciditeit in strategische visie en onverzettelijkheid. Ze bevestigen dat we in een era vertoeven waarin transformatie de diapason slaat. Organisaties worden uitgedaagd tot een continuüm van educatie, collaboratie, ethische governance en avant-gardistische conceptie. In een tijdperk waarin verandering de enige constante lijkt en onvoorspelbaarheid eerder regel dan uitzondering is, komt de wijsheid uit het verleden. Om een uitgebreider perspectief te geven op deze gedachte: het is van essentieel belang dat we ons concentreren op de aspecten van het leven en werk die we daadwerkelijk in de hand hebben. Zet je energie in op wat je kunt beïnvloeden. Hyperfocus niet alleen op het bereiken van vooraf bepaalde doelen, maar investeer vooral in persoonlijke groei en onwrikbare discipline.

Het cultiveren van een leercultuur is meer dan alleen het opdoen van nieuwe kennis; het gaat om het aanmoedigen van een mindset waarbij continu leren en aanpassen de norm wordt. Dit stimuleert innovatie en creativiteit binnen individuen en teams. Door je teams te bekrachtigen en in hun kracht te zetten, geef je hen de ruimte om zelfstandig te denken, te handelen en verantwoordelijkheid te nemen.

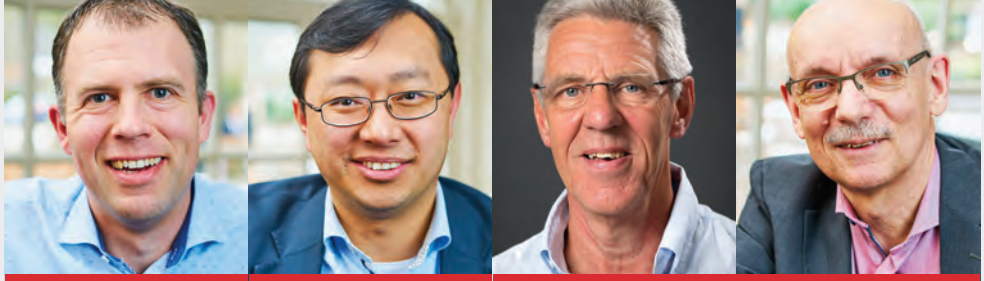
Leiderschap tot slot, is niet alleen het geven van richting, maar ook het tonen van voorbeeldgedrag. Door elke dag te streven naar een incrementele perfectie van slechts 1%, zet je een standaard van voortdurende verbetering. Dit concept kan op het eerste gezicht minimaal lijken, maar de cumulatieve effecten over tijd zijn enorm. Mijn bescheiden observaties wijzen althans in die richting.

Achter Het Nieuws

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.

Client Side Scanning: middel zoekt toepassing

Twee jaar geleden nam Apple het initiatief om de apparatuur van haar gebruikers actief te gaan controleren op (in eerste instantie) kinderporno. Experts (en heel veel medewerkers) waarschuwden massaal voor de risico's. Het resulteerde in een flinke deuk in het privacy-imago van het bedrijf, dat in 2021 de plannen snel op de lange baan schoof. Sinds het initiatief van Apple passeert Client Side Scanning regelmatig de revue en wordt er door voor- en tegenstanders druk gelobbyd. Hoe kijken de redactieleden naar CSS? Is dit de heilige graal om terrorisme, zware criminaliteit en plaatjes van kindermisbruik voor eens en voor altijd de nekslag toe te dienen? Of een privacy-nachtmerrie die ervoor zorgt dat niemand meer onbezorgd een babyfoto maakt met zijn telefoon?



Daar waar we de Facebooks van onze wereld inmiddels volop aan het verketteren zijn om hun verwerpelijke volgsystemen die gebruikt worden om geld te verdienen, viert het controleren van de samenleving voor opsporingsdoeleinden hoogtijdagen. Heel begrijpelijk. De halve wereld leeft inmiddels in zijn devices. En toegang tot dat gedrag biedt bijna ongelimiteerde mogelijkheden. De toegang tot die data is er momenteel wel. Maar vorderen of hacken is omslachtig, kostbaar en daardoor vooral nuttig om in te zetten bij personen die je al op de radar hebt. Daarmee mis je dus een enorme groep aan potentiële criminelen en terroristen die je via CSS eenvoudig inzichtelijk kunt maken. En laten we eerlijk zijn: wie wil kindermisbruik nu niet de wereld uit helpen? Tegen dat doel valt toch weinig in te brengen? Helaas grossieren we met elkaar ook in de voorbeelden waar een nobele toepassing die voor 'doel één' de wetgever passeert, in de loop der tijd wordt ingezet voor doeleinden waar initieel nooit draagvlak voor zou zijn geweest. Onze redactieleden reflecteren op het surveillancemechanisme dat al zoveel tongen heeft losgemaakt.

Maarten Hartsuijker

Als informatiebeveiliger wil je natuurlijk altijd tot in de puntjes weten hoe je gegevens worden verwerkt en wat je kunt doen om te borgen dat ze niet weglekken. Vanuit die verantwoordelijkheid is Client Side Scanning (CSS) een ongrijpbare zwarte doos. Eentje die wellicht begint als een heel klein doosje met een heel specifiek doel, maar die voor je het weet is uitgegroeid tot het 'manusje van alles' op de endpoints. Je hebt hierbij geen idee of dit 'manusje' besluit om jouw bedrijfsgeheimen door te sturen, of besluit ze ongemoeid te laten. En zowel dat besluit als de ontvanger van deze data kan daarbij ook nog eens afhankelijk zijn van het land waar een medewerker zich bevindt of geregistreerd heeft. Een bedreiging als deze verwacht je op sommige plekken op de wereld (en is vaak een reden om aan zakelijke devices reisvoorwaarden te koppelen), maar toch niet in Europa?

Zo nu en dan hoor ik in de discussie over client Side Scanning (CSS) iemand de opmerking maken dat de digitale wereld net als de fysieke samenleving niet wetteloos mag zijn. Ook weer niets tegenin te brengen. Maar deze valse tegenstelling suggereert ook dat CSS noodzakelijk is om een digitaal handhavingsgat op te vullen dat er in-real-life niet is. En dat is natuurlijk niet het geval, want in onze fysieke wereld kunnen we (gelukkig) op heel veel plekken onbespied onszelf zijn.

Laten we het eens omkeren en ervan uitgaan dat alle apparaten over een decennium onder 24x7 controle staan en dat kindermisbruik verhuisd is naar de achterkamertjes. Hoe zouden we het vinden als aannemers na oplevering van ons huis de sleutel zouden houden. Gewoon 'om af en toe even een handhaver binnen te laten om in de achterkamer te kijken of er niets geks gebeurt'? Of (veel efficiënter): dat aannemers je huis bij oplevering van camera's zouden voorzien met de opmerking: ze filmen alleen alles hoor. De beelden van wat je thuis doet gaan nergens heen. Tenzij je iets doet waarvan we denken dat het niet in de haak is natuurlijk, maar dat is bij jullie toch niet het geval!?

Ik zie aan deze maatregel dan ook vooral risico's kleven. Terwijl ik vermoed dat het digitale gedrag waar we terecht iets tegen willen doen heel eenvoudig een laagje dieper ondergronds kan en zal gaan.

Fook Hwa Tan - Het algemeen belang boven het individueel belang: de complexiteit van Client Side Scanning

In een tijd waarin technologie en privacy steeds meer met elkaar in conflict lijken te komen, is het cruciaal om een grondige afweging te maken tussen het algemeen belang en het individueel belang. Het recente debat rondom Client Side Scanning (CSS), zoals geïnitieerd door Apple, legt deze uitdaging bloot. Terwijl voorstanders beweren dat CSS een krachtig wapen kan zijn tegen terrorisme, zware criminaliteit en kindermisbruik, waarschuwen critici voor de potentieel verwoestende impact op onze privacy en de mogelijkheid tot misbruik door overheden en andere instanties.

Het is belangrijk om te erkennen dat de motivatie achter CSS nobel is. Het opsporen en bestrijden van kinderporno en ernstige criminele activiteiten is een doel dat niemand kan betwisten. Echter, het invoeren van dergelijke technologieën vereist een diepgaande overweging van de risico's en gevolgen voor onze samenleving.

Het belangrijkste argument voor CSS is de potentiële effectiviteit ervan bij het bestrijden van ernstige misdaden. Het systeem zou automatisch verdachte inhoud kunnen detecteren zonder dat deze informatie ooit de cloud of servers van een bedrijf verlaat. Dit zou een belangrijke stap kunnen zijn in de strijd tegen kindermisbruik en terrorisme. Het is echter van cruciaal belang om ervoor te zorgen dat deze technologie met de hoogste mate van nauwkeurigheid werkt en dat er strikte waarborgen zijn om valse positieven te voorkomen.

Aan de andere kant van het spectrum zijn de zorgen over privacy en mogelijke misbruiken van CSS. Het is begrijpelijk dat mensen bezorgd zijn over het feit dat hun gegevens en persoonlijke communicatie kan worden gescand, zelfs als het doel nobel lijkt te zijn. Het creëren van een technologische infrastructuur die potentieel kan worden misbruikt om privéberichten af te tappen of bedrijfsgeheimen te stelen, is een zorgwekkend vooruitzicht.

Daarom is het van essentieel belang dat er strikte en onafhankelijke controlemechanismen worden ingevoerd om misbruik van CSS te voorkomen. Deze controles moeten gebaseerd zijn op transparantie, verantwoording en naleving van strenge juridische normen. Bovendien moet de implementatie van CSS onderworpen zijn aan voortdurende beoordeling en evaluatie om ervoor te zorgen dat het systeem niet afdwaalt van het oorspronkelijke doel.

Het algemeen belang moet altijd worden afgewogen tegen het individueel belang, maar het mag niet ten koste gaan van onze fundamentele rechten en vrijheden. We moeten voorkomen dat we in een samenleving terechtkomen waarin privacy volledig ondergeschikt wordt aan veiligheid. Een balans moet worden gevonden, en deze balans vereist voortdurende discussie en reflectie, niet alleen door bedrijven als Apple, maar ook door overheden, experts en de samenleving als geheel.

Uiteindelijk moeten we ervoor zorgen dat CSS niet wordt gebruikt als een middel om onze privacy te ondermijnen of om inbreuk te maken op onze fundamentele rechten. De weg naar een veiligere samenleving mag niet leiden tot een surveillancestaat waarin niemand meer vertrouwelijk kan communiceren. We moeten zorgvuldig navigeren in dit complexe landschap en blijven streven naar een evenwicht tussen het algemeen belang en het individueel belang, terwijl we onze waarden en vrijheden hoog in het vaandel houden.

Leo van Koppen - CSS-wetgeving een opmaat naar Chinese surveillance?

Client Side Scanning lijkt een nobel initiatief van Apple. De mooie doelstelling ervan onderschrijven we allemaal. Het bestrijden van kindermisbruik verdient de hoogste prioriteit, maar met CSS geraken we toch wel in een heel lastig dilemma: kindermisbruik oftewel criminaliteit bestrijden ten koste van de privacy van de burger. Dat dilemma aanpakken vereist een grondige analyse en een beschouwing vanuit veel invalshoeken. In mijn reactie wil ik, in de wetenschap dat

Ik ben van mening dat CSS, zoals nu in Europees verband wordt voorgesteld een enorme inbreuk is op de privacy van de burger

ik niet volledig ben, op een aantal ervan reflecteren.
Op dit moment van schrijven ligt het voorstel in Brussel en op het moment van verschijnen van dit artikel zal duidelijk geworden zijn hoe de wetgeving eruit zal gaan zien. In het voorstel dat nu voorligt ter bestrijding van kinderporno wordt gesproken over drie vormen van scannen: 1. Scannen op bestaande afbeeldingen d.m.v. hashes, 2. Scannen van nieuwe afbeeldingen en 3. Scannen van grooming , beiden via AI. Deze technieken zijn overigens afwijkend van de technieken die Apple wil toepassen. Europa wil dus een eigen implementatie van CSS gaan doen.

Is de methodiek wel waterdicht? Is de gebruikte methode zodanig betrouwbaar dat er geen of tenminste een heel laag percentage false positives ontstaat? De gevolgen van false positives zouden kunnen leiden tot het aanklagen en wellicht ook (publiekelijk) veroordelen van onschuldige mensen. Dat kan een enorme impact hebben. In het verlengde van false positives moet je ook kijken naar de false negatives. Wat als de crimineel een werkwijze vindt om het systeem te ontduiken wat me overigens in het geheel niet ondenkbaar voorkomt.

Kan de stroom aan meldingen goed afgehandeld worden? Een dergelijk systeem genereert een enorme hoeveelheid meldingen, deze komen dan op een locatie (een speciale afdeling van Interpol) binnen. Is men a. in staat om deze stroom te verwerken, zijn er voldoende mensen beschikbaar die dit werk kunnen en willen uitvoeren, en b. is het bekijken van dit soort beelden werk dat een persoon kan volhouden? We kennen inmiddels de verhalen van de mensen die dit voor Facebook en het voormalig Twitter hebben verricht.
Wat kan een mogelijk gevolg zijn? Stel dat de CSS zal worden ingevoerd, hoe eenvoudig is het dan om het systeem te gebruiken voor een ander goed doel, bijvoorbeeld belastingfraude opsporen of Covid-ontkenners te volgen e.a. Het is een kleine moeite om naast de database met bekende kinderporno een tweede of derde toe te voegen voor het scannen en opsporen van andersoortige criminaliteit of ongewenst gedrag. De techniek maakt het mogelijk, dus waarom zouden we het (in tijd van nood) niet gebruiken?

Proportionaliteit? Staat een dergelijke maatregel, die zo'n inbreuk heeft op de privacy, wel in verhouding tot de opsporing van de criminelen en het uitbannen van kinderporno? De groep mensen die een privacy inbreuk ervaren is vele en vele malen groter dan de groep criminelen die er mee kan worden opgespoord.

Ik ben van mening dat CSS, zoals nu in Europees verband wordt voorgesteld een enorme inbreuk is op de privacy van de burger, dat het een opmaat kan zijn naar surveillance praktijken zoals we die van China kennen en dat het resultaat is dat we een ambtelijk monster gecreëerd hebben waarmee we meer leed bij burgers veroorzaken en heel weinig criminelen zullen vangen omdat zij andere wegen en middelen zullen vinden om deze maatregel te ontwijken.

Conclusie, NIET DOEN!

Chris de Vries - Neem de 'Big Tech' hun macht af!

Client Side Scanning roept bij onze redacteuren veel op, getuige de omvang van hun reacties dat het gebruikelijke woordenaantal overschrijdt. Daarbij gaan ze allen in op de onwenselijke neveneffecten, die het nastreven van de goede (nobele) doelen onoverkomelijk lijken te volgen. Tussen de regels door lees je: 'de weg naar hel is geplaveid met goede bedoelingen'. Godfried Bomans schreef eens dat veel futurologen of schrijvers van toekomstromans meestentijds pessimisten zijn. Dat, omdat zij de flexibiliteit en veerkracht van de mens onderschatten. Zijn onze redacteuren dan ook pessimisten? Neen! Het bespreekbaar maken van reële (be)dreigingen is de taak van elk kritisch levend mens, die werkelijk deel uitmaakt van de samenleving waarin hij leeft, woont en werkt. En het woord 'werken' hier bewust op de laatste plaats. Zij geven hierbij adem aan de gedachte dat een rationeel goed verdedigbaar besluit, terdege op sociale gronden zou moeten kunnen worden afgewezen.

'...He was walking down the white-tiled corridor, with the feeling of walking in sunlight, and an armed guard at his back. The long hoped-for bullet was entering his brain. … He had won the victory over himself. He loved Big Brother'

Benieuwd

De redactie van IB-Magazine is benieuwd naar jullie reacties en mening. Tag ook collega's en vakgenoten en nodig ook hen uit te reageren.

Dat daarbij de mening van de gewone mens zwaarder weegt dan die van politici, ambtenaren, die mogelijk (!?) dienstbaar zijn aan de (industriële/economische) oligarchen. Uit de Griekse taal: oligos (weinig of klein) en archein (heersen, regeren) en neen, oligarchen komen niet alleen in Rusland voor.

Ik verwijs graag naar dit nummer van IB-Magazine waarin het interview met Winn Schwartau, de spreker van de bijeenkomst van PvIB in mei van dit jaar. Winn is een specialist op het terrein van Cybersecurity & Cyberwar.

Eén van zijn belangrijkste waarschuwingen luidde dat het doel van Big Tech bedrijven is: winst behalen door vorming van een wereld (`terraforming') waar er geen oog is voor privacy en waarbij de menselijke conditie bepaald wordt door het vertellen van verhalen; die de werkelijkheid verdraaien (`reality distortion'), zaken veranderen en dat met het oog op gedragsmodificatie door inbezitname van de menselijke geest (`absorption of minds'). Zijn actie suggestie: **neem de 'Big Tech' hun macht af!**

Ik ben het dus met mijn collega's eens dat Client Side Scanning een groot gevaar vertegenwoordigt, maar dat niet alleen vanwege het misbruik van techniek, maar ook de inherente overgave van privacy (lees: de meest persoonlijke data) aan Big Tech bedrijven, die het voor de levensstandaard van hun eigenaren misbruiken om de mens ongemerkt te manipuleren op een nog nooit geziene schaal. Diezelfde mens ook nog eens in extase denkend: *'...He was walking down the white-tiled corridor, with the feeling of walking in sunlight, and an armed guard at his back. The long hoped-for bullet was entering his brain. … He had won the victory over himself. He loved Big Brother.'* George Orwell, 1984. Ik wens innig dat dit doembeeld niet de werkelijkheid zal zijn voor onze (achter)kleinkinderen!

NB.: Ik heb de gebruikelijke limiet ook overschreden.

Martijn Hoogesteger is Head of Cyber bij S-RM en is bereikbaar via m.hoogesteger@s-rminform.com.

COLUMN MARTIJN

Back to BEC

Cybercriminelen moeten harder op zoek naar nieuwe technieken. In een eerdere column schreef ik over de wapenwedloop tussen criminelen en organisaties. Cybercriminelen hebben een lange tijd ver voorgelegen maar moeten nu weer aanpoten. Een van de trends die we duidelijk zien is een vernieuwde aandacht voor het hacken van e-mailaccounts om vervolgens fraude te plegen, Business Email Compromise (BEC). De afgelopen drie weken heb ik drie BEC-zaken onderzocht waar iets geks mee aan de hand was.

De eerste BEC treft iemand uit het management van een advieskantoor. Zij hebben per ongeluk de MFA-instellingen niet helemaal correct staan, waardoor het account van deze persoon alleen met een wachtwoord beveiligd is. Dit wachtwoord wordt helaas buitgemaakt in een phishingaanval. Deze phisher gebruikt legitieme websites om bestanden uit te wisselen, waar het bestand weer een link bevat naar een neppe Microsoft-pagina. Op zich niets bijzonders. De crimineel logt in, kijkt heel kort rond, reset vervolgens het LinkedIn-account van deze manager en verwijdert alle e-mails gerelateerd aan deze reset. In het LinkedIn-account is verder niets bijzonders gebeurd, maar het resetten van accounts gerelateerd aan het e-mailadres om meer gegevens buit te maken is interessant. Gelukkig was deze klant er snel bij en is deze toegang tot LinkedIn niet misbruikt. Het zet de vraag: tot welke accounts kan ik nog meer toegang krijgen vanaf de mailaccounts? wat hoger op de risicolijst. Het is een techniek die ik 99% van de tijd kan misbruiken om toegang te krijgen tot accounts van voortvluchtigen in Hunted, dus ik moest wel even grinniken.

In de tweede BEC zaak gebeurt ook iets interessants. Deze aanval is opgevallen omdat er met een factuur gefraudeerd was. Op jacht naar de eerste login van de crimineel vinden we... niets! De e-mails zijn buitgemaakt door een applicatie te koppelen aan het account via de Graph API van Microsoft. Via deze API is de gehele mailbox meermaals gedownload, en zijn de factuurgegevens ontvreemd. De gebruiker heeft waarschijnlijk lang geleden deze applicatie toegang gegeven (naar aanleiding van een phishing aanval). Helaas was er geen expliciete goedkeuring voor dit soort applicaties nodig binnen de organisatie. Het is een techniek die niet onbekend is, maar we steeds vaker zien terugkomen.

In de derde BEC zaak zien we twee oude technieken samenkomen. De organisatie was nogal verrast dat ze waren getroffen, want ze gebruiken overal MFA. De phishingaanval bleek uitgevoerd met EvilProxy, die ook de MFA had onderschept om zo in te loggen. Na het inloggen is bijna direct een nieuwe phishingmail opgesteld en verstuurd naar alle contacten in dit account. Dit lijkt volledig geautomatiseerd te gebeuren, om zo een 'worm' te maken die zich snel verspreid naar andere doelwitten. Beide technieken zijn niet nieuw (EvilProxy is alweer bijna een jaar oud), maar de combinatie creëert wel weer flinke impact.

Nieuwe technieken voor Business Email Compromise zijn makkelijk uit te leggen en je kunt je er met een beetje configuratie en bewustwording goed tegen verdedigen. We zien ook steeds slimmere en nieuwe technieken die gebruikt worden in andere aanvallen, met name ransomware. Die vergen vaak een meer diepgaande en holistischere aanpak om effectief tegen te verdedigen. Stay safe!

PvIB Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Bianca Brooijmans
Alex Dingemanse
Maarten Hartsuijker
Fook Hwa Tan
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
Chris de Vries

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

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 2023 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

VERSTERK UW ISO/IEC 27001 MANAGEMENTSYSTEEM!

Wilt u zeker weten of uw organisatie klaar is voor certificering volgens ISO/IEC 27001? Doe de online DNV Self-Assessment en ontvang een rapportage in uw inbox. Of volg de Normkennis ISO/IEC 27001

Kent u de DNV Self-Assessment Suite al? Deze tool stelt u in staat te testen hoe goed u ISO/IEC 27001 kent en te beoordelen in hoeverre uw managementsysteem klaar is voor certificering. De evaluatie is op basis van puntenscores en laat zien waar er tekortkomingen bestaan en waar u verbeteringen kunt doorvoeren.

Stel een nulmeting op, stel kwantitatieve doelen vast voor een specifiek aandachtsgebied en meet regelmatig de geboekte vooruitgang. De Self-Assessment Suite biedt u in alle gevallen een gedetailleerd inzicht in uw kennis of prestaties en uw mate van beheersing.

Wilt u graag uw kennis vergroten over ISO/IEC ISO 27001? Volg dan de Normkennis ISO/IEC 27001 training! De trainer geeft u handige tips en voorbeelden uit de praktijk, zo leert u te kijken naar de norm, zoals een auditor dit doet.

Kijk voor meer informatie over de Self-Assessment Suite op dnv.nl/self-assessment of scan de QR-code als u wilt deelnemen aan de training.

DNV

TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2024

AIGP - Certified AI Governance Professional
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v12
OSCP - Offensive Security PEN-200
BIO - Certified Bio Professional
NIS2 - NIS2 Lead Implementer

GET SKILLED
WWW.TSTC.NL

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 - Privacy Management

www.tstc.nl

Onze trainingen zijn klassikaal of Live Online te volgen