ib

INFORMATIEBEVEILIGING MAGAZINE

15 PvIB reconnect in cyber security

- De kloof tussen awareness en gedrag
- Wat leert de AP-boete van Transavia ons?
- Column – Als je niet normaal bent

JAARGANG 22 - 2022 - EDITIE 1

GOEDE PRIVACY EN INFORMATIEBEVEILIGING

Beschermt u gevoelige informatie op een gestructureerde manier? ISO 27701 is het “ISO antwoord” op de AVG.

Wilt u uw kennis op het gebied van informatiebeveiliging of privacy vergroten? DNV biedt normkennis trainingen aan voor de ISO 27001 en ISO 27701 en een training Lead Auditor ISO 27001. Heeft u het ISO 27001 certificaat in bezit? Dan kunt u uw ISMS uitbreiden met de privacy specifieke eisen conform de ISO 27701.
U kunt uw managementsysteem in één keer tegen beide normen certificeren met één combinatie-audit. Met als resultaat: twee certificaten waarmee u laat zien dat uw privacy en informatiebeveiliging gewaarborgd is.

Kies DNV als uw partner in certificering en training. Bij DNV staat uw organisatie centraal. We kijken bij de certificering ook naar de aandachtspunten waar u zelf op beoordeeld wilt worden. Tijdens onze trainingen vormen uw ambities en doelstellingen het middelpunt. Onze trainingen gaan verder dan alleen kennisoverdracht: leren door zelf te doen en zelf te ervaren. Training met impact.

Vind meer informatie over ISO 27001 en ISO 27701 op www.dnv.nl/ISO27001.

DNV

Het is nog niet te laat!

Tom Bakker

Allereerst de beste wensen voor 2022! Dat het een mooi en veilig(er) jaar mag worden. Velen van ons hebben zich de laatste weken en feestdagen van 2021 beziggehouden met de log4j vulnerability. Ook een aantal redactieleden! Vandaar dat ondergetekende deze keer voor hoofdredacteur speelt. Meer over log4j in Achter het Nieuws.
Twee columnisten zijn in de loop van vorig jaar gestopt. Berry en Inge Wetzer. Inge blijft ons nog wel periodiek voorzien van artikelen over de psychologische kant van informatiebeveiliging.
Ook in dit nummer: deel 2 van het drieluik de human factor in informatiebeveiliging. Na 'kennis' nu 'gedrag'.
Inmiddels hebben we een oude bekende bereid gevonden om onze nieuwe columnist te worden: Lex Borger, onze vroegere hoofdredacteur. Hij geeft in zijn eerste column een terugblik op alle narigheden van 2021 en blikt vooruit naar 2022. Hij heeft meteen ook een boekreview ingeleverd.
Ook Paul Oor blikt in zijn artikel vooruit en geeft CISO's tips voor 2022 in de vorm wat hij de '10 commandments' noemt.
Het kan niet missen, het coalitieakkoord 2021 komt aan de orde. Wat staat erin over informatiebeveiliging en de algoritmetoezichthouder? Ard Ruiter bespreekt het.
Vorig jaar werden weer de Joop Bautz Awards (JBISA) uitgereikt. De 1e prijswinnaar van 2021, Dieuwke van der Ende, heeft een inleiding geschreven over haar winnende scriptie hoe de privacy van de input data voor beslisbomen gewaarborgd kan worden door de toepassing van homomorfische encryptie. Lees dan vooral ook de hele scriptie door die te downloaden.
De blog van Robert Metsemakers gaat over antivirussoftware dat niet zaligmakend is en maakt een vergelijking met het ontstaan van griep/corona virusvarianten en PCR testen. Heel actueel.
Toch ook weer een paar artikelen over privacy en met name over de AVG. Dat blijft toch een belangrijk onderwerp. De verrassende manier van toetsing van de AVG door de AP wordt besproken door Peter van Schelven en Bianca Brooijmans naar aanleiding van het boetebesluit voor Transavia.
Een kritische blik op de AVG door Jan Willem de Vries. Hoe is het gesteld met de privacy in Nederland? Volgens hem 'is het de afgelopen jaren slechter gesteld'. Maar het is nog niet te laat!

Veel leesplezier!

Tom

IN DIT NUMMER

Auteur: Paul W.M. Oor is freelance Security & Data Protection Manager/Consultant. Paul is te bereiken via paul@shared-experiences.nl. Dit artikel is eerder verschenen op de ISACA NL Chapter https://isaca.nl/nieuws/cisos-enabling-business/#_ftn1.

CISO's enabling business

The 10 commandments for CISO's in 2022

In June 2021 ISACA NL allowed me to publish my opinion on what business leaders should do to take ownership for security and enable their CISO's to be more effective: 'CEO's enabling CISO's; the 10 commandments for CEO's when positioning a CISO in their organization...' (1) In this sequel I'll explain my sense of urgency and how we need to change security governance, now presenting: 'The 10 commandments for CISO's in 2022' (2). Adapting our organizations to survive and prosper in an increasingly complex, chaotic world.

The mentioned article triggered discussions with business managers and my security peers. Managers challenged me on them taking full ownership of cybersecurity and data protection while my professional peers saw the chance of a seat in the boardroom vaporize. Both audiences urged me to explain why this change is required now? A hopeful sign! We need all the attention we can get to close the gap between organizational leaders and security professionals, managing expectations on both sides.

Piracy and an increasingly complex world

We live in a time where our activities in the past are re-evaluated and excuses offered. With the vision of hindsight, the activities of my (Dutch) ancestors were often debatable to say the least. A lot of our wealth and fortune originates from piracy (3) when measured by today's standards. In those days however, my ancestors were tolerated and respected in their society. Their activities were considered of vital importance for the nation's prosperity as they were developing global supply chains and colonies by semi-legit activities. Tolerated and supported by governments and large commercial organizations like the VOC (4). Today's developments and threats related to global cyber-supply chains and data colonies have a lot in common with this period of history. Hackers i.e., pirates, force us to collaborate, innovate and drive us to maturity. At the same time, we're in business with the nations and multinational companies who back and protect todays pirates while loot and ransom are still being used to become more powerful.

Taking back control

During several centuries pirate activities proved to an essential driver for the development of the colonies and trade-routes. In the end nations took back control by treaties and navies, protecting legitimate merchant fleets and fortified, controlled cities in the colonies. History seems to repeat itself in cyberspace. Some nations provide protection to today's pirates; hackers are respected, extremely rich and popular. Their comfortable position is now more and more challenged and tensions are rising due to the vital importance of global cyber supply chains and data-colonies. This complex landscape has thus become a topic to be effectively tracked by leadership in all organizations.

Laws and regulations vs. effective cybersecurity

History has shown that protecting interests and sovereignty with legitimacy i.e., laws and regulations has its limitations. Nevertheless China, the USA, Russia, the EU and others are developing stringent laws and regulations to protect their digital sovereignty and data. But on top of that everyone, even the EU (5), is stepping up their defensive and offensive cyber-capabilities. We've come to realize that laws and regulations alone are not effectively protecting our digital interests and sovereignty. Developments in this increasingly complex landscape; compliance combined with effective protection is a topic requiring direct involvement of leadership in any organization too, supported by security and data protection professionals.

Global politics, cyber and business

Organizational leaders must monitor the impact of this fast-moving, unpredictable, war-like landscape. Like the military do: OODA: Observe, Orient, Decide and Act (6). Cybersecurity has become a matter of national security in many countries and has a direct impact on any organizational strategy and operation. With whom can and may your organization conduct business today and in the future? Who's to be trusted, legally and effectively reliable in the long run? Where can and may we process our data, in which data-colony? Business leadership is accountable and responsible; as professionals we must support them. With the emphasis on support, there's no way cybersecurity and data-protection professionals can or will carry all of the burden, no matter how well we are paid. Leadership must integrate cyber in their governance. Business managers have to talk cybersecurity and data-protection if they want to trade supported by professionals like us, as described in the `10 commandments'!

Address complexity: tangible advise for a challenging job

Managers can't maintain their traditional attitude; 'I've hired expensive security professionals and services; let them take on their responsibility and deal with it'. Security must be integrated in the organizational governance and the DNA of the organization. Everyone was well aware of the threats and dealt with it. Commercial companies, state sponsors and everyone in the crew, from captain to deckhand, were always alert and responsive. Protecting their lives, trade and business profits.
Considering an unpredictable future and the evolving threat landscape means that our organizations and we, as professionals, must reach a similar level of vigilance. I hope you will find 'The 10 of commandments for CISO's in 2022' helpful to align with your leadership and support them to effectively integrate security in your organization.

The 10 commandments for CISO's in 2022

1. Take good care of yourself. Like any first responder or person working in high pressure environments; ensure good physical and mental health. Only when you are safe and in good shape, you can be of service and support others.
2. Don't ask for a security budget. Security is the responsibility of the entire organization, not of a single department. Adequate funding and related cybersecurity-KPI's (7) should be requested by and allocated to divisions and departments. I've never understood the bill of materials of security costs as referred to in surveys or demanded by financial controllers. The salary and expenses of the CISO and perhaps some very specific services exempted. The majority of security costs and investments are tactical and operational costs, to ensure business continuity of the whole organization. You don't specify costs for brakes, mirrors and seatbelts in a car as optional security cost, do you?
3. Forget about 100% security assurance. Some colleagues are struggling in their organization and even considering employment elsewhere as they consider the organization's efforts not in line with their professional standards. As a CISO you must accept to live with uncertainties and risk acceptance by management. Which is alright, as long as you provide tangible, pragmatic professional advice and risks are seriously evaluated and explicitly accepted, not ignored. Embrace risks, changes and innovation without becoming reckless.
4. Develop and maintain an excellent information position. Invest heavily in your professional network to maintain situational awareness and keep abreast of developments relevant for your organization. Not limited to technology! Global politics and compliance developments (8) included! Try to recognize and be aware of plans within plans, schemes within schemes in the landscape to identify relevant developments and support your organization to address potential risks.
5. Invest in continuous education. Our profession requires at least a basic level of knowledge in many areas and this knowledge must be maintained, despite rigorous changes. Security certification helps as it provides at least a Common Body of Knowledge (CBK) (9) and will get you recognized for your professional drive and – at least – basic knowledge and capabilities.
6. Track environmental and social developments. Security and data protection are increasingly important for organizations as they must live up to the changing expectations and standards in society. Not limited to formal compliance; be aware of what's socially, politically and ethically acceptable now. Tracking e.g., politics is essential in our job to advice e.g., in which data-colonies (clouds) your organization's data can be processed, today and in the long run!
7. Declassify data and information. Reconsider need-to-know to increase resilience and vigilance of your organization. Make information more widely available within your organization. Declassification information where possible; enabling Teams of Teams (10) in today's dynamic environment. Only a very small amount of data in the organization really needs strict protection; focusing on the protection of these Crown Jewels will reduce workload and costs.
8. Stop fighting for a CISO-seat in The Board. It's a distraction and waste of your precious time and energy. Focus on having one or more board members becoming aware and familiar with your security agenda. Support these sponsors in the board to get security implemented, financed and controlled in the whole organization. Get them as interested in security KPI's as they are in the financial performance of the organization.
9. Forget about compliance, rules and regulations. OK, that sounds a bit harsh but DO focus on effectiveness; no pirate-hacker will be scared away by laws or security certification. On the other hand, don't ignore developments on standards, laws and regulations. Get and stay familiar with these and treat potential non-compliance as a potential, serious threat to the organization.
10. Focus on organizational readiness. Avoid becoming too complacent and too dependent on structures and processes. Hackers and their sponsors are unpredictable; make sure your organization is prepared for the unexpected; simulate and exercise. Think evil and out-of-the-box. Always supplement PENetration tests with frequent Red/Blue Team exercises. Practice will make everyone in the organization better understand what's at risk. By doing so your organization will be in a strong position when an inevitable incident occurs. During an actual situation stress will be higher because it's real. But nothing will be totally new!

Can we still learn from the past?

The world has become more complicated, but the real challenge is its complexity. I've lost my 'been there, seen that, done that' attitude. Experience counts but even seasoned business managers and security professionals must admit that experience is not enough anymore. It has to be complemented with a new attitude, genuine interest in developments in many areas and the input of the new generation in our organization. Leading us to increased organizational vigilance and commitment of leadership on security to ensure organizational resilience.

There is some comfort in the parallels with Piracy in the old days. Dealing with continuous piracy by Japanese pirates raiding the coasts of China and Korea in medieval times rulers realized that piracy was something to be considered as something natural that could not be avoided but had to be reacted on. Deal with it, even make use of it. This resulted in a kind of equilibrium, a balance, formalized by a treaty (11). Compromising with, even pardoning and hiring pirates and at the same time disrupting their business cases. By challenging sovereignty and ceasing ground and other possessions of rulers in areas where pirates were sheltering and protected.

Today's piracy is complex but applying this approach today might be effective again. It's still all about wealth, power, controlling supply chains and sovereignty. I'm embracing tomorrow with optimism, confident that our security community, working with management can deal with today's threats and challenges. As long as we adapt our modus operandi to cope with a dynamic and complex world. Like in the days of global exploration by seafaring nations we're going through a fascinating period of change, only quite a bit faster than our ancestors… This makes security a great and challenging job never a dull day!

ISACA Netherlands Chapter

References

(1) https://isaca.nl/opinieartikel/ceos-enabling-cisos/

(2) I'll be using the term security instead of security and data protection to improve readability. However, I strongly believe in close collaboration and merging activities of CISO's and DPO's! Especially since too many DPO's focus on the legal aspects of data protection while effective protection of (personal) data has to be taken care of as well.

(3) https://en.wikipedia.org/wiki/Golden_Age_of_Piracy

(4) https://en.wikipedia.org/wiki/Dutch_East_India_Company

(5) https://www.consilium.europa.eu/en/policies/cybersecurity/#

(6) John Boyd, Military Strategist

(7) Key Performance Indicators

(8) Advancing IT, Audit, Governance, Risk, Privacy & Cybersecurity | ISACA

(9) (ISC)² CBK | Common Body of Knowledge (isc2.org)

(10)Team Of Teams: An Emerging Organizational Model (forbes.com)

(11) Wokou, Wikipedia

Auteur: Jan Willem de Vries is jarenlang actief geweest in de wereld van informatiebeveiliging en IT-architectuur bij o.a. Capgemini. Na zijn formele pensioen was hij nog enige tijd werkzaam bij de Kamer van Koophandel als architect security. Hij is nog steeds actief als docent/trainer op beide onderwerpen. Jan Willem is bereikbaar via: janwillem.de.vries@xs4all.nl

Privacy in het dagelijks leven

Er wordt veel aandacht aan privacy besteed in de vakbladen en daarbij wordt veelal en terecht gerefereerd aan de AVG. Dit was onder meer het geval in het iB-Magazine 5 2021, waarin onder andere werd ingegaan op AVG en op de WPG. De artikelen werden geschreven vanuit de wet- en regelgeving en hadden een positieve grondhouding over wat er met de wet bereikt kan worden.

De vraag is of deze positieve conclusie terecht is. Ik had graag in hetzelfde nummer een verhandeling gezien over de werkelijke situatie met betrekking tot privacy. Is privacy-bewustzijn toegenomen en is het niveau van privacy door AVG (en WPG e.d.) zelfs verbeterd? Ik heb er mijn twijfels bij.
In dit artikel wil ik, zonder dat ik hier een wetenschappelijke studie aan heb gewijd, betogen dat het de afgelopen paar jaar slechter is gesteld met privacy in Nederland en wil ik afsluiten met een aantal voorstellen voor veranderingen. Veranderingen overigens die alleen door politieke druk (en lobbywerk) kan worden bereikt.

Bedreigingen en oorzaken

Hoe komt het dat, ondanks een privacywetgeving en ondanks goede initiatieven vanuit met name het Europees Parlement, het privacy-niveau achteruitgaat? Ik zie dat vanuit verschillende richtingen onze privacy wordt bedreigd: de overheid, de banken, sociale media, fysieke winkels, surveillance industrie en websites; en ik zal nog wel niet compleet zijn. Ik zie hiervoor een paar grote oorzaken en ik weet dat ik daarmee ook politieke uitspraken doe.
Er zijn (grote) problemen in de maatschappij – drugs, geweld, witwassen, fraude, politiek extremisme aan linker- en rechterkant – waar de overheid terecht zicht op wil hebben of krijgen. De diensten die hierop gericht zijn, lopen in hun dagelijkse praktijk aan tegen beperkingen door wet- en regelgeving. In plaats van creatiever te zijn binnen de bestaande regelgeving gaan ze er juist buiten en krijgen daarbij impliciete en expliciete steun van de overheid. Daar komt bij dat het erg lijkt dat de overheid de burgers niet als hun opdrachtgevers beschouwt, maar, al dan niet bewust, als lastige onderdanen die ze niet vertrouwen – zie ook Toeslagenschandaal en het Fraudesysteem van de Belastingdienst, alsmede de werkwijzen van UWV en bijstandsdiensten van de gemeenten. De Tweede Kamer heeft daar zelf ook zeer aan meegewerkt na de Bulgarenaffaire.

De consequentie is dan dat dezelfde overheid die gedwongen door Europa de AVG als wet heeft aangenomen, nieuwe wetten voorstelt en laat aannemen die hier tegenin gaan (Wet gegevensverwerking door samenwerkingsverbanden (WGS), Wetsvoorstel wettelijke grondslag voor verwerking persoonsgegevens (NCTV), maar waartegen vanuit privacy-organisaties, waaronder de Autoriteit Persoonsgegevens, grote bezwaren zijn.Het is een voorbeeld van een werkwijze die de Nederlandse overheid voortdurend lijkt te volgen: (beperkende) wetgeving oprekken, wetgeving voorstellen die rechtszekerheid benadeelt, processen traineren (Groningen, Toeslagenaffaire, maar ook vele zaken waarbij burgers de overheid dwongen tot correcties). Het kapitalisme tot in het extreme. De recente bankenrichtlijn PSD2 is typisch een voorbeeld van de lobby van grote IT-bedrijven die de burger een behoefte aanpraten: als wij jouw bankgegevens mogen inzien of zelfs namens jou betalingen kunnen regelen, dan… en dan komt het grootse vergezicht aan mogelijkheden. Hier zie je dat het grote geld het gewonnen heeft van de privacy van de burgers. Je kan er als burger nee tegen zeggen – en dat heb ik gedaan –, maar velen zullen en kunnen de consequenties van deze zaken niet overzien. De burger op het internet niet als klant zien, maar als

product of grondstof. Veel surveillancetechnologie die aanwezig is, is het gevolg van het feit dat sociale media, met Facebook voorop, het internet hebben kapotgemaakt ter eigener voordeel. Door gegevens te verzamelen (welke websites bezoek je, op welke advertenties reageer je, op welk deel van de webpagina blijf je wat langer hangen) en deze gegevens te aggregeren en te verrijken met gegevens van andere organisaties, kunnen ze hele profielen verkopen. Om dat mogelijk te maken, zijn er allerlei technieken in het leven geroepen om burgers te kunnen volgen, ook als ze even niet op Facebook of Twitter zitten. De overheids-surveillanceorganisaties van diverse landen maken hier ook dankbaar gebruik van. Als de Facebooks e.d. echt gericht waren geweest op bescherming van hun grondstoffen (meer zijn we immers niet) waren de systemen op onze eindstations (browsers, tablets, smartphones) veel geslotener geweest en daarmee beter beveiligd.

Dictatoriale regimes (zoals China, Rusland) willen 100% grip op hun onderdanen houden. Technologiebedrijven en wetenschappers willen graag hun kennis verkopen en werken mee aan technologieën die dit mogelijk maken: trackingsystemen, gezichtsherkenning, spraakherkenning, etc. En deze landen bieden omgekeerd dit soort diensten aan aan andere overheden in bijvoorbeeld Afrika of Azië, maar ook in Europa. Hierdoor worden wij ook nog meer gevolgd.

Als gevolg van al dit soort ontwikkelingen zijn bedrijven dit ook in de fysieke wereld gaan toepassen: gebruik maken van Bluetoothtracking, camera's in winkels, aanbieden van hotspots in winkels; allemaal bedoeld om het koopgedrag en winkelgedrag van individuele klanten te kunnen volgen en dat bij voorkeur ook te kunnen koppelen aan specifieke klanten. De daarbij ontstane profielen zijn ook weer handelswaar geworden.

Tussentijdse conclusie

Ik kom daarmee tot de volgende tussentijdse conclusie: de AVG en overige regelgeving van de EU hebben ons een goed handvat gegeven om onze privacy te beschermen, maar tegelijkertijd zijn er door dezelfde EU, door overheden en bedrijven grote en geslaagde aanvallen op onze privacy uitgevoerd, waarbij bewust de privacy van burgers is en wordt aangetast. Naar mijn mening is op dit moment die aanval groter dan wat door de AVG kan worden beschermd.

Veranderingen

Hierboven heb ik een omgeving geschetst waarin in feite de privacy van ons als burgers, ondanks veel wet- en regelgeving in Nederland, de EU, maar zeker ook de VS, wordt verkwanseld. Ik denk dat dit anders moet. Wat er moet veranderen, weet ik zo goed nog niet. Ik heb wel wat denkrichtingen, maar die zijn vast veel te simpel.

Veel kan en moet door nieuwe wet- en regelgeving op nationaal en internationaal niveau worden geregeld. Maar deze komt niet tot stand zonder actieve ondersteuning door parlement, lobbywerk vanuit privacy-organisaties, zoals de Autoriteit Persoonsgegevens of Bits of Freedom, vakbonden en een goede en vrije pers. Bij die laatste denk ik niet alleen aan de gevestigde Nederlandse pers, zoals NRC, Trouw, Vrij Nederland, maar ook aan nieuwe persdiensten, zoals The Intercept, Now This, De Correspondent e.d.

Nieuwe wet- en regelgeving zal overigens langzaam ontstaan omdat (a) het parlement door meerderheidsakkoorden erg aan het kabinet is gebonden, (b) de benodigde en actuele kennis hiervoor vaak bij parlementsleden ontbreekt, (c) er vanuit de grote IT-bedrijven en sociale media veel tegengesteld lobbywerk plaatsvindt en last but not least (d) er altijd nog de (terechte!) angst bestaat tegen terrorisme en georganiseerde en grootschalige criminaliteit en dus vanuit de opsporingsdiensten om bijzondere rechten wordt gevraagd.

Ik schreef hierboven al dat ik niet goed weet hoe we de privacy kunnen verbeteren, anders dan door goede wet- en regelgeving. Maar waar ik aan denk – en dat zal zeker tot veel al dan niet terechte kritiek leiden – is het volgende: in de AVG is al expliciet opgenomen dat er sprake moet zijn van dataminimalisatie. De (Europese en Nederlandse) wetgeving op dit punt moet nadrukkelijker worden uitgewerkt om zeker te maken dat surveillance door bedrijven en overheden, anders dan als het vanuit wet- en regelgeving wordt geëist, niet meer toegestaan is. De volgende punten zijn daar een technische uitwerking van:

Privacy by design: websites mogen per definitie niet meer volgen, alleen bij opt-in en daar mag niet elke keer om gevraagd worden. Dit moet niet alleen betrekking hebben op cookies, maar op alle manieren waarop burgers kunnen worden gevolgd, zowel client side als server side. Natuurlijk moet een website volgen; voor goede performance of om de transacties goed te laten uitvoeren. Maar ze mogen alleen volgen wat je in de eigen omgeving doet. Niet wat je verder allemaal op je werkplek doet. Ook mag dat niet gebruikt worden voor diensten op andere websites. Voorbeeld: als ik via Google wat zoek, zie ik vervolgens op diverse websites reclames over waarnaar ik zocht. Waar

Onze vrijheid wordt bedreigd door aanvallen op onze privacy.

gaat die informatie nog meer naar toe?
De consequentie van deze beperking is dat er geen tracking reclames, pixelreclames, tracking cookies, algemene trackers (anders dan om performance van systemen te meten) meer toegestaan zijn.
PII en PHI data móet in Europa worden gehost. En dat is tegenwoordig niet zo'n rare eis meer, sinds Rusland, China, Turkije, India etc. dit ook vereisen. Ook privacygevoelige data die ontstaan door het toepassen van diensten (Zoom, Teams, Discord etc.) mogen alleen worden opgeslagen in landen waarvan de EU aangeeft dat deze betrouwbaar zijn (per definitie dus niet de VS). Wellicht kunnen dit soort eisen niet algemeen worden gesteld, maar wel aan cloudproviders en aan clouddienstverleners die zich expliciet op Europa richten: data opslaan in de regio waar deze ontstaan en deze ook niet voor analyse naar elders sturen, anders dan na afdoende anonimisering.

We moeten veel meer toe naar een situatie waarin we zelf als burgereigenaar zijn en blijven van onze eigen persoonlijke gegevens en gezondheidsgegevens. Door het gebruik van een beschermde omgeving waarin deze gegevens (versleuteld) zijn opgeslagen en middelen om gericht bepaalde gegevens vrij te geven aan specifieke gebruikers, verhogen we het niveau van onze privacy.
Wetgeving moet altijd door de Eerste Kamer getoetst worden op grondrechten, grondwet en internationale verdragen. Het wordt tijd dat de Eerste Kamer hier weer de tijd voor krijgt en neemt bij nieuwe wetgeving en daarbij ook kijkt naar werkbaarheid, proportionaliteit en risico van misbruik van maatregelen. Wetten waarover momenteel veel wordt gesproken (wetgeving voor inzage van banksaldi, wet gegevensverwerking door samenwerkingsverbanden (WGS), wetsvoorstel wettelijke grondslag voor verwerking persoonsgegevens (NCTV) zijn wellicht positief bij bestrijding van zware criminaliteit, maar zijn te zwaar om alle andere redenen en zijn dan m.i. strijdig met rechtszekerheid en zullen leiden tot zelfde soort situaties als we bij de Toeslagenaffaire al hebben gezien.
Systemen (browsers, mobiele systemen) dienen veel meer dan nu het geval is, er op gericht zijn om misbruik van gegevens te onderkennen en te waarschuwen als privacygevoelige gegevens lekken of er gevolgd wordt. Cloudproviders, clouddienstverleners en bedrijven met websites zullen periodiek via verklaringen (vgl. SOC II Type 2 verklaringen) moeten kunnen aantonen dat ze de privacy van de burgers handhaven en geen profielen e.d. doorverkopen
Dit is vooralsnog een eerste aanzet. Ik ben geen expert hierin, maar wil discussie loskrijgen. Iedereen die betere ideeën heeft, is natuurlijk welkom.

Conclusie

Onze vrijheid wordt bedreigd door aanvallen op onze privacy. Aanvallen die op dit moment vanuit de overheid weliswaar niet bewust gericht zijn op vernietiging van privacy, maar wel mogelijkheden bieden om volledige controle op mensen te hebben. Ik heb zelf nog het geloof dat onze huidige Nederlandse en Europese overheden op zich geen kwaad willen. Maar de huidige stand van technologie is zodanig dat met de hedendaagse middelen dit zondermeer wel mogelijk is, mede door druk vanuit IT, sociale media en opsporingsorganisaties.
Ik denk niet dat het te laat is; we kunnen vanuit Nederland en Europa nog maatregelen gaan treffen om de bedreigingen van onze risico's te stoppen; maar dan moeten we wel nú actie gaan ondernemen door nieuwe vertrouwenwekkende maatregelen.

Auteur: Peter van Schelven is jurist en arbiter bij BIJ PETER - Wet & Recht en bereikbaar via linkedin.com/in/petervanschelven. Bianca Brooijmans is FG bij Enovation Group en zelfstandige. Bianca is bereikbaar via linkedin.com/in/biancabrooijmans.

‘Mind your step’: wat leert de AP-boete van Transavia ons?

Afgelopen november publiceerde de Autoriteit Persoonsgegevens (AP) het besluit waarmee Transavia een bestuurlijke boete van 400.000 euro is opgelegd. De toezichthouder kwam tot die sanctie vanwege een ondermaatse beveiliging van persoonsgegevens. Het boetebesluit van de AP is de moeite van het lezen waard omdat het uitvoerig ingaat op het onderwerp van de toegang tot IT-systemen.

In de herfst van 2019 bleek dat een hacker zich onbevoegd toegang tot de IT-systemen van de luchtvaartmaatschappij te hebben verschaft, waardoor gegevens van zo’n 80.000 passagiers, 3.000 medewerkers en 200 leveranciers konden worden bemachtigd. Daar zaten onder andere BSN-nummers en gezondheidsgegevens van passagiers, bijvoorbeeld over rolstoelgebruik, tussen. Kortom, een fors datalek.

De melding van het datalek vormde de opstap voor onderzoek van de AP, die begrijpelijkerwijs concludeerde dat de Algemene Verordening Gegevensbescherming (AVG) was overtreden. Het onderzoek maakte duidelijk dat de hacker gebruik had gemaakt van een aanval door middel van ‘password spray’ en ‘credential stuffing’. Van ‘password spray’ is sprake als veelgebruikte wachtwoorden op een geautomatiseerde wijze worden ingezet om toegang tot IT-systemen te krijgen. Bij ‘credential stuffing’ gebruikt een hacker, uit andere datalekken, van derden afkomstige gebruikersgegevens. Eenmaal bij Transavia binnen deed de hacker in kwestie zich voor als vertrouwde gebruiker met de hoogste privileges in het systeem.

Nadere concretisering van securitynorm

Artikel 32 van de AVG, de algemeen geformuleerde bepaling over de verplichting tot beveiliging van persoonsgegevens, geeft niet concreet aan hoe en met welke middelen een organisatie de toegang tot haar IT-systemen moet inrichten. De AVG zegt wel dat je als organisatie ‘passende technische en organisatorische maatregelen’ moet nemen die een, op het risico afgestemd, beveiligingsniveau waarborgen. Al met al een tamelijk vage norm. Met name de openheid van deze wettelijke regel roept in de praktijk meer dan eens de vraag op of je als organisatie wel voldoende security in huis hebt om compliant te zijn met de AVG. Het boetebesluit inzake Transavia helpt ons wat die vraag betreft wel een klein stapje verder. De Autoriteit Persoonsgegevens zegt onder meer het volgende: ‘De maatregelen die Transavia had kunnen nemen ten tijde van de inbreuk, waren reeds een norm volgens Transavia zelf, volgens leveranciers en volgens internationale standaarden. Verder bleek dat er bepaalde maatregelen wel al deels waren geïmplementeerd door Transavia.’

Het opmerkelijke van dit citaat is dat de AP, bij de beantwoording

van de vraag welke securitymaatregelen zij onder de AVG geboden acht, niet alleen uitgaat van min of meer objectieve maatstaven, zoals de welbekende securitystandaarden, bijvoorbeeld ISO27001. Volgens die standaarden moeten, naar wij bekend veronderstellen, toegangsrechten worden beperkt en gecontroleerd. Maar de AP gaat in haar aanpak een behoorlijke stap verder. Zij doet namelijk voorkomen dat die aanpak past in de toepassing van artikel 32 AVG. Want wat doet de toezichthouder? In zekere zin subjectiveert zij de wettelijke securityverplichting door uitdrukkelijk aan te knopen bij dat wat in de ogen van Transavia zélf, zo blijkt uit haar eigen securitydocumenten, relevante maatregelen zijn. Anders gezegd: de regels van het IT-securityrecht komen niet alleen van buiten en zijn niet louter een extern gegeven, maar is ook iets wat je als organisatie zelf inhoud geeft. Een voor de hand liggende insteek nu de securityregels van de AVG meer vragen dan antwoorden opwerpen. De set van spelregels onder de AVG voor wat betreft informatiebeveiliging wordt door het eigen gedrag van de organisatie ingevuld. Securityrecht is geen 'law in the books', maar 'law in action'. Het boetebesluit lezende maakt het ons dan ook duidelijk dat de AP Transavia (mede) heeft afgerekend op de inhoud van haar eigen securitybeleidsdocumenten en de gebrekkige wijze waarop het luchtvaartbedrijf aan die documenten uitvoering heeft gegeven. Dat gaat dus aanzienlijk verder dan louter een toets aan de tekst van de AVG en de gangbare securitystandaarden.

Een voorbeeld: wachtwoordbeleid

Transavia beschikte over een uitvoerig uitgewerkt wachtwoordbeleid. Daarin was aangegeven welke eisen er golden per gebruiker en per mogelijk risiconiveau. Hoe hoger het risiconiveau, des te zwaarder de eisen voor een wachtwoord. Het bedrijf onderscheidde wachtwoorden met een standaard risiconiveau, wachtwoorden met additionele maatregelen voor gebruikers met meer bevoegdheden en tevens wachtwoorden voor 'hoog risico gebruikers'. In de beleidsdocumenten was ook het gebruikelijke onderscheid gemaakt tussen 'generieke accounts' en aan individuele gebruikers gekoppelde 'user accounts'. In haar onderzoek heeft de AP Transavia gevraagd waarom de generieke accounts die betrokken waren bij de hack niet voldeden aan het eigen wachtwoordenbeleid. De luchtvaartmaatschappij heeft daarop geantwoord dat haar focus vooral lag op user accounts, enerzijds omdat dat meer accounts betrof en anderzijds omdat zij meende dat bij die accounts de meeste risico's zouden liggen. Transavia stelde zich op het standpunt dat de kans op een succesvolle 'password spray'-aanval of 'credential stuffing attack'-groter was bij user accounts dan bij generieke accounts. De AP gaat daaraan volledig voorbij. Zij maakt met het antwoord korte metten: "De wachtwoorden van de gecompromitteerde accounts voldeden niet aan het eigen beleid en waren in die zin niet passend voor het beoogde niveau van beveiliging."

Zie hier de dus insteek van de AP:

- Het 'eigen beleid' van Transavia blijkt voor de AP een wezenlijk vertrekpunt te zijn bij het bepalen van de reikwijdte van de securityverplichting. Zo krijgt het eigen securitybeleid in zekere zin een juridische lading.
- Niet de vraag of, zoals de AVG verlangt, Transavia voorziet in 'passende' security-maatregelen staat voorop, maar wel of de getroffen securitymaatregelen passend zijn voor het door Transavia zélf 'beoogde' niveau van security. Het eigen beleid is dus 'leading' in de beoordeling van de vraag of de AVG geschonden is.

Slot

Het boetebesluit van de AP lijkt ons op zich niet onredelijk; de informatiebeveiliging van Transavia zoals aanwezig in najaar 2019 kon de toets der kritiek eenvoudigweg niet doorstaan. Maar meer specifiek leert het boetebesluit ons ook dat de AP bij een security-onderzoek naar aanleiding van een datalek een klassiek-juridische 'truc' toepast: confronteer de organisatie met haar eigen woorden. Dus: kijk naar dat wat de eigen beleidsdocumenten van de organisatie zeggen en geef die documenten vervolgens een prominente plek bij het bepalen van de vraag of een organisatie de securityverplichting van de AVG wel of niet naar behoren heeft nageleefd. Zoals gezegd: niet alleen de tekst van de AVG en de algemeen aanvaarde beveiligingsstandaarden (bijv. van ISO en NEN) geven inhoud aan het securityrecht, ook het eigen securitybeleid van de organisatie vormt een bron voor de beoordeling. De AP betrekt in de beoordeling of je je eigen woorden als organisatie serieus hebt genomen. Is dat niet het geval, dan maak je de AP het makkelijk om jouw organisatie daarop af te rekenen. Grof gezegd: opgeknoopt aan je eigen woorden…

Dit alles gezegd hebbende, is securitybeleid onmiskenbaar meer dan alleen 'een' securitybeleid. Je maakt er eigen normen mee waar de AP op kan terugvallen. Houd dat voor ogen wanneer je je als security- of privacy professional buigt over het maken of beoordelen van een securitybeleidsdocument. 'Mind your step...'

Referentie

(1) Besluit Autoriteit Persoonsgegevens 23 september 2021 t.a.v. Transavia Airlines C.V, gepubliceerd 12 november 2021.

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

De kloof tussen awareness en gedrag

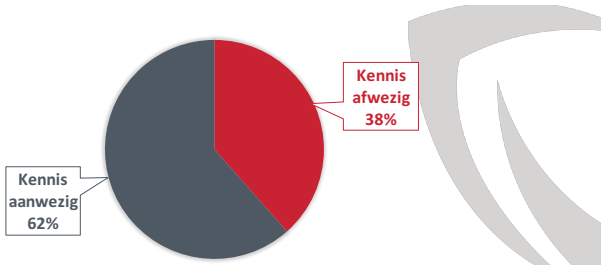
Deel 2 van drieluik: Onderzoek naar de human factor in informatiebeveiliging

Als we willen dat mensen zich cyberveilig gaan gedragen, moeten we verder kijken dan kennis en awareness. Kennis over cybersecurity leidt niet één op één tot het gewenste gedrag, wordt aangenomen, maar empirisch is dit nog maar weinig onderzocht. Hoe groot is die kloof tussen weten en doen in cybersecurity nou echt?

Dit artikel beschrijft onderzoek dat voor vijftien verschillende ISO-, NEN- en NIST-onderwerpen onderzocht hoeveel mensen nou wéten over cybersecurity en vervolgens in hoeverre zij het ook daadwerkelijk veilig handelen. Deze data maken de kloof tussen kennis en gedrag in cybersecurity inzichtelijk en geven daarmee beeld van wat er nodig is om mensen te bewegen naar het gewenste cyberveilige gedrag.

Even snel koffie halen zonder je computerscherm te vergrendelen. Je weet wel dat het eigenlijk geen goed idee is, maar de kans dat er iets misgaat is maar klein en het kost toch weer moeite om je wachtwoord opnieuw in te voeren. Een vertrouwelijk document even omgedraaid onder je toetsenbord leggen. Je weet dat je dat eigenlijk in je afgesloten kast moet opbergen, maar die heb je net dichtgedaan en de sleutel in het sleutelkastje gestopt en nu moet je rennen om je trein te halen… Traditionele awareness campagnes zijn gericht op het zenden van kennis. In de tijd dat cybersecurity nog een nieuw en onontgonnen terrein was, was dit uitermate belangrijk; om je veilig te kunnen gedragen, moet je wéten wat veilig gedrag is. De traditie van kennis zenden heeft zich voortgezet. De vraag of dit nog steeds de effectiefste manier is om gedrag te beïnvloeden, nu cybersecurity meer bekend is bij een breder publiek? Om die vraag te kunnen beantwoorden moet je weten hoe het staat met het huidige kennisniveau: hoeveel weten mensen eigenlijk over verschillende cybersecurity-onderwerpen? Deel 1 van dit drieluik beschreef de resultaten van een onderzoek naar het huidige kennisniveau, onder vijftien respondenten van twintig organisaties (Wetzer, 2021) (1).

De resultaten in figuur 1 laten zien dat wanneer we kijken naar het gemiddelde over de vijftien onderzochte onderwerpen, in 38% van de gevallen mensen niet het juiste antwoord gaven op de kennisvraag. In 62% van de gevallen wist men wel het juiste antwoord. Kennis ontbrak dus gemiddeld in iets meer dan een derde van de gevallen.



Figuur 1: Kennis gemiddeld over vijftien onderwerpen.

In termen van bewustwordingscampagnes zijn dit best mooie cijfers: in iets meer dan een derde van de gevallen ontbreekt het nog aan kennis. Voor de overige 62% hoef je niets meer te doen. Tenminste, als bewustwording je einddoel is. Bij doorvragen in organisaties blijkt echter bijna altijd dat men uiteindelijk toe wil naar veilig gedrag. Maar weten wat je moet doen is niet zomaar hetzelfde als ook daadwerkelijk veilig handelen. Dit besef wordt steeds breder gedeeld, alleen ontbraken tot nu toe de cijfers die dit konden onderbouwen en die inzicht gaven in hoe groot het verschil tussen weten en doen nou echt is in cybersecurity. Dit artikel beschrijft een onderzoek dat zich specifiek richt op het meten van de kloof tussen kennis en gedrag in cybersecurity.

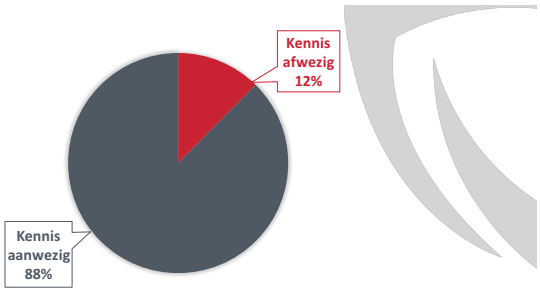
Onderzoeksmethode

Zoals in deel 1 werd beschreven, hebben we data van onze nulmeting van twintig organisaties in de zorgsector gecombineerd. Dit resulteerde in een dataset bestaande uit vijftien respondenten. De meting bestond uit een online vragenlijst met verschillende delen. Voor dit artikel richten wij ons op het kennisgedeelte en het gedragsgedeelte van de studie. Om een goed beeld te krijgen, zijn door cybersecurity-experts vijftien onderwerpen geselecteerd, gebaseerd op ISO-, NIST- en NEN-richtlijnen. Allereerst werd voor elk van deze onderwerpen een kennisvraag gesteld. Deze (meerkeuze-) kennisvraag is door experts vanuit verschillende vakgebieden (psychologen, cybersecurity-experts

en securityspecialisten uit de zorg) getoetst. Vervolgens werd voor ieder onderwerp een gedragsvraag gesteld. Hierin werd mensen gevraagd aan te geven op een schaal van 1 (nooit) tot 5 (altijd) of zij het gedrag ook daadwerkelijk vertonen.

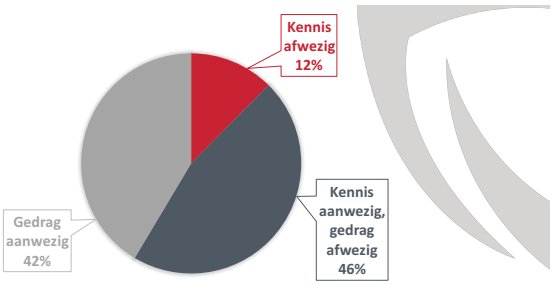
Cijfers

Om te beginnen een rechttoe rechtaan onderwerp: het vergrendelen van je computerscherm als je wegloopt bij je computer. De data uit de kennistest (figuur 2) laat zien dat 88% van de respondenten het juiste antwoord gaf op de vraag wanneer je je computerscherm dient te vergrendelen.



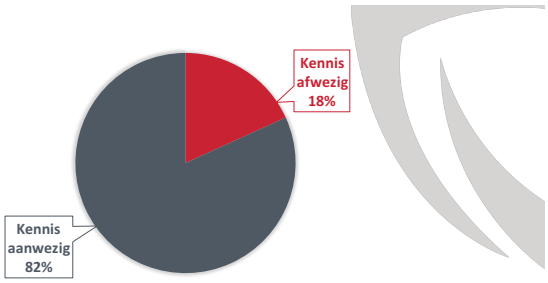
Figuur 2: Computerscherm vergrendelen: Kennis.

Op basis van deze cijfers zou je kunnen concluderen dat je bijna klaar bent. Slechts 12% weet het nog niet, geen slechte score als je ervan uitgaat dat weten betekent dat iemand het ook doet. Maar als we nu verder kijken en die groep die het weet vragen of ze het ook daadwerkelijk dóen, ontstaat er een heel ander beeld, zoals te zien is in figuur 3.



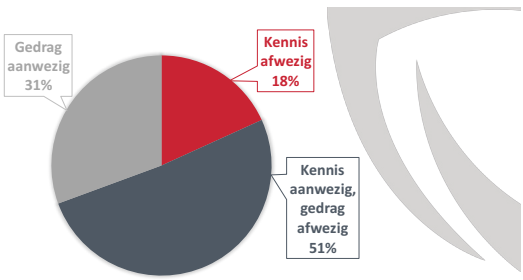
Figuur 3: Computerscherm vergrendelen: Kennis en gedrag.

Ondanks dat 88% van de respondenten in dit onderzoek dus wel degelijk wéét wanneer zij hun computerscherm horen te vergrendelen, geeft slechts 42% aan dat ook daadwerkelijk te dóen. Dat betekent dus dat meer dan de helft van diegenen die het weten, niet handelen naar deze kennis; 46% van de mensen in dit onderzoek heeft wél de kennis maar vertoont toch niet het juiste gedrag. Een kloof tussen kennis en gedrag voor dit onderwerp van 52% dus! Hoe zit dat voor andere onderwerpen? Eén van de andere onderzochte onderwerpen, is het kiezen van een sterk wachtwoord voor je werkaccount. Wanneer we mensen vroegen om uit verschillende wachtwoorden aan te geven welk wachtwoord het sterkst was, zagen we dat kennis over wachtwoordsterkte bij 82% van de respondenten aanwezig was (zie figuur 4). Hierbij is het van belang te weten dat er geen makkelijk te raden juist antwoord was, men moest echt op de hoogte zijn van wat een sterk wachtwoord definieert om het juiste antwoord te kunnen kiezen.



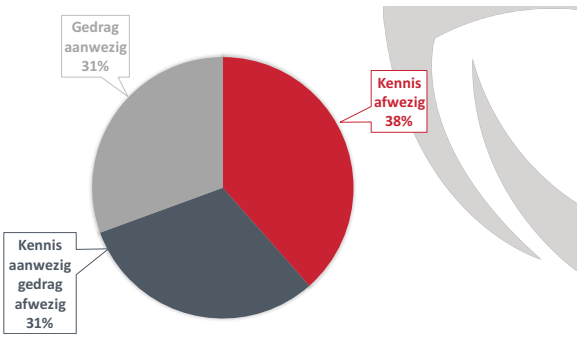
Figuur 4: Sterk wachtwoord: Kennis.

Vervolgens werd de respondenten gevraagd of zij zelf ook een sterk wachtwoord gebruiken voor hun werkaccount. De resultaten in figuur 5 laten zien dat weliswaar 82% van de respondenten wel weet wat een sterk wachtwoord is, maar dat slechts 31% van de respondenten ook daadwerkelijk een veilig wachtwoord gebruikt. Een kennis-gedragskloof van 62%.



Figuur 5: Sterk wachtwoord: Kennis en gedrag.

Bovenstaande data laat een grote kloof zien tussen kennis en gedrag in cybersecurity. Deze kloof was bij alle vijftien onderzochte onderwerpen aanwezig, maar er was wel een behoordelijke variatie in de grootte van deze kloof. Gemiddeld over vijftien onderwerpen werd het volgende beeld zichtbaar (figuur 6):



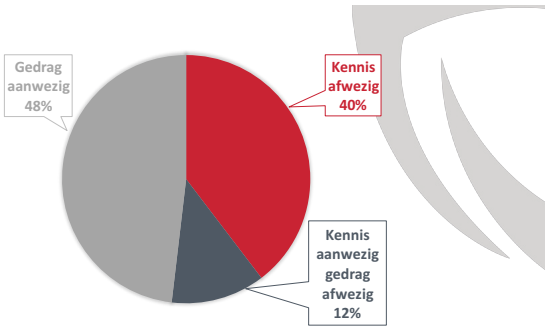
Figuur 6: Kennis en gedrag in cybersecurity gemiddeld over vijftien onderwerpen.

In 38% van de gevallen is kennis afwezig. In de overige 62% van de gevallen weet men wel het juiste antwoord op de kennisvraag (zie figuur 1). Wanneer we echter kijken naar gedrag, zien we dat van deze 62% mensen die het wéét, maar 31% aangeeft het ook daadwerkelijk te doen. Met andere woorden: over vijftien cybersecurity-onderwerpen gemiddeld, vertoont 31% van de mensen het gewenste gedrag. Als we kijken naar het percentage mensen dat wel over de noodzakelijke kennis beschikt (62%), zien we dus dat de helft (31%) van deze mensen daar ook naar handelt, en de andere helft (31%) niet. De kloof tussen kennis en gedrag in cybersecurity is dus 50%.

Veilig gedrag afdwingen

Zoals hierboven beschreven, is de kloof van 50% een gemiddelde over vijftien onderwerpen. Wanneer we meer inzoomen op specifieke onderwerpen, worden verschillende interessante patronen zichtbaar. Allereerst is er een sterk effect te zien van gedrag dat kan worden afgedwongen versus gedrag dat meer afhankelijk is van eigen keuzes. Hierboven werd de kloof tussen kennis en gedrag getoond: 52% voor het onderwerp 'computer vergrendelen' en 62% voor 'het kiezen van een sterk wachtwoord'. Beide onderwerpen betreffen gedrag waarbij de organisatie wel faciliterend kan zijn, maar veilig gedrag niet volledig kan afdwingen. Het is wel mogelijk om een computer na een korte tijd automatisch te laten vergrendelen, maar het is niet mogelijk om af te dwingen dat mensen zelf hun computer vergrendelen wanneer zij weglopen. Ook het gebruik van een sterk wachtwoord hangt nog af van de menselijke keuze. Technisch kan worden afgedwongen dat een wachtwoord een bepaald aantal karakters heeft en ook welke karakters er in ieder geval in moeten zitten, maar een wachtwoord als @msterdam01! voldoet al gauw aan deze eisen, zonder een sterk wachtwoord te zijn. Dus we kunnen mensen instrueren en feedback geven over wat een sterk wachtwoord is, maar of ze er uiteindelijk ook voor kiezen om daadwerkelijk een sterk wachtwoord te maken, is niet af te dwingen.

Er zijn ook gedragingen die wel (gedeeltelijk) af te dwingen zijn. Denk bijvoorbeeld aan het gebruik van tweefactorauthenticatie (2FA). Een organisatie kan ervoor zorgen dat mensen alleen maar in de beveiligde omgeving kunnen werken wanneer zij inloggen met een wachtwoord én een tweede factor, bijvoorbeeld een code die men ontvangt per SMS na het invoeren van het wachtwoord of een tag die gescand moet worden nadat het wachtwoord is ingevoerd. Voor de 60% van de respondenten die over de benodigde kennis beschikt voor wat betreft tweefactor-authenticatiebeleid binnen diens organisatie, bleek uit de analyse dat slechts 12% níet het bijbehorende gedrag daadwerkelijk vertoont. Dit komt neer op een kennis-gedragskloof voor 2FA van 20%. Dit is veel lager dan de gemiddelde kloof van 50%. Deze resultaten zijn in lijn met de hypothese dat de mogelijkheid om gedrag (technisch) af te dwingen een aanzienlijke invloed heeft op de kloof tussen kennis en gedrag.



Figuur 7: Tweefactorauthenticatie: Kennis en gedrag.

Wat kan ik met deze data?

De data in dit artikel geeft inzicht in de huidige status van kennis en gedrag in cybersecurity. Daarmee bieden ze handvatten voor stappen die genomen kunnen worden om cyberveiliger gedrag binnen organisaties verder te stimuleren en faciliteren. Wanneer we kijken naar het gemiddelde beeld, wordt namelijk duidelijk dat in 38% van de gevallen kennis de ontbrekende factor is. Welke onderwerpen dat voornamelijk betreft, werd in het vorige artikel van dit drieluik beschreven (Wetzer 2021) (1). Voor deze onderwerpen is de meeste winst te behalen door te beginnen met het verhogen van de kennis.

Dit artikel maakt duidelijk dat in 31% van de gevallen het juiste gedrag al wordt vertoond. Voor deze onderwerpen is dus geen verdere actie nodig. Wellicht is dit percentage in werkelijkheid nog wat lager omdat er sprake kan zijn van sociale wenselijkheid bij het invullen van het onderzoek. Wanneer mensen een rooskleuriger beeld schetsen dan de werkelijkheid, is de kennis-gedragskloof dus nog wat groter. Hoe dan ook blijft er zeker 31% van de gevallen over, waarbij de kennis wel aanwezig is, maar het gedrag niet. Voor deze gevallen heeft het uiteraard geen zin om verder in te zetten op kennis verhogende activiteiten, omdat hier sprake is van de kennis-gedragskloof. Sterker, ga je iemand die iets al weet maar het niet doet nog een keer uitleggen dat dit toch echt moet, dan schieten wij eigenwijze Nederlanders hoogstwaarschijnlijk in de weerstand. Om de kennis-gedragskloof te overbruggen, zal gekeken moeten worden naar de andere aspecten die gedrag beïnvloeden. Hier zal verder op worden ingegaan in het derde deel van dit drieluik.

Referentie

(1) Wetzer, I. M. (2021). Het begint met bewustwording. Hoe ver zijn we daar inmiddels mee? Informatie Beveiliging, 6, 26-29.

Auteur: mr. A.IJ. (Ard) Ruiter werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen- en Opsporingsdienst (ILT-IOD). Hij schreef dit artikel op persoonlijke titel en is bereikbaar via LinkedIn.

Vooruitzien met cyber- en datasecurity

Over informatiebeveiliging en de algoritmetoezichthouder in het coalitieakkoord 2021

Op de dag dat het kabinet-Rutte III al elf maanden demissionair was, presenteerden de partijleiders van VVD, D66, CDA en ChristenUnie het coalitieakkoord met de titel 'Omzien naar elkaar, vooruitkijken naar de toekomst' (1). Een wereld zonder ICT-voorzieningen en zonder de steeds voortschrijdende digitalisering, is inmiddels ondenkbaar. Op welke wijze geeft de nieuwe, oude coalitie invulling aan de eisen van informatiebeveiliging en cybersecurity?

Na de Tweede Kamerverkiezingen op 15, 16 en 17 maart 2021 startte de onderhandelingen voor een (nieuwe?) coalitie met de aanstelling van twee verkenners. Eén verkenner werd op 25 maart 2021 gefotografeerd met notities, waarop onder andere de inmiddels zeer bekende frase was aangetekend: 'Omtzigt, functie elders'. Dit had betrekking op het Kamerlid dat zich in de maanden daarvoor had vastgebeten in de zogenoemde Kinderopvangtoeslagaffaire, waarover het kabinet viel. Het veroorzaakte een kettingreactie waar we de gevolgen nog steeds van merken, ook uit het oogpunt van informatiebeveiliging. Dit voorval zette de formatie op zijn kop en werd uiteindelijk hét politieke moment van 2021. De interne informatie had vrij gemakkelijk beveiligd kunnen worden en had nooit op straat mogen komen te liggen.

Op 17 november 2021 schreef De Volkskrant over een soort 'proeve van een regeerakkoord' dat een 'betrokkene bij de formatie' in de trein had laten liggen. Met enige schaamte werd opgebiecht wie dat was. Daaraan kon je zien dat de awareness zeker wel aanwezig is, maar geen mens onfeilbaar is (2). Na de langste coalitieonderhandelingen uit de vaderlandse parlementaire geschiedenis is er dan voor de kerst nog overeenstemming. Met in de titel een tautologie: vooruitkijken is immers altijd gericht op de toekomst. Voordat we kijken wat er in dit document staat over informatiebeveiliging en cybersecurity, bezien we even wat op Duits federaal politiek niveau is gebeurd.

IT-beveiliging: cyber- en datasecurity

IT-beveiliging krijgt steeds meer aandacht. Informatiebeveiliging omvat zowel cyber- en datasecurity. Cyber- en datasecurity zijn van oorsprong twee verschillende disciplines. Ze liggen in elkaars verlengde en worden vaak met elkaar verward, maar kunnen elkaar zeker versterken. Cybersecurity omvat het bredere spectrum van beveiliging van data en IT-systemen tegen diefstal, verstoring of misbruik van hardware, software of data. Cybersecuritymaatregelen zijn ontworpen om dreigingen tegen netwerksystemen en applicaties te bestrijden, ongeacht of deze dreigingen van binnen of buiten een organisatie komen. Datasecurity gaat over de bescherming gedurende de gehele lifecycle van digitale informatie tegen bedoelde of onbedoelde aanpassing, verwijdering, diefstal of openbaarmaking van data door ongeautoriseerde personen.

Duits akkoord: 178 pagina's

In Duitsland verliepen die onderhandelingen in 2021 wat sneller. Ook in de Bondsrepubliek waren namelijk recent parlementsverkiezingen. Onze oosterburen schreven in ruim twee maanden een akkoord onder de titel: 'Durf meer vooruitgang te boeken: verbond voor vrijheid, gerechtigheid en duurzaamheid', dat uit maar liefst 178 (!) pagina's bestaat. Het Duitse akkoord vermeldt het woord 'informatiebeveiliging' ('IT-Sicherheit') elf keer, de Algemene Verordening Gegevensbescherming (AVG) ('Datenschutz-Grundverordnung' (DSGVO) vier keer en heeft een separate paragraaf over digitale burgerrechten en informatiebeveiliging. 'Het uitbuiten van zwakke punten in IT-systemen staat in een zeer problematische verhouding tot informatiebeveiliging en burgerrechten', aldus het Duitse coalitieakkoord. Zo wordt geschreven over het instellen van een recht op encryptie, een effectief beheer van kwetsbaarheden, met als doel om beveiligingslacunes te dichten, en de specificaties 'security-by-design/default' in te voeren. Tevens wordt gesproken over anonimiseringstechnieken, het creëren van rechtszekerheid via normen en het overschrijden daarvan moet gaan leiden tot strafrechtelijke aansprakelijkheid bij illegale deanonimisering. Ook wordt de ambitie uitgesproken om het MKB te ondersteunen in de ongecompliceerde promotie en ondersteuning voor informatiebeveiliging, AVG-conforme gegevensverwerking en het gebruik van digitale technologieën (3).

Nederlands akkoord: 55 pagina's

Na bijna negen maanden onderhandelen in Nederland in 2021 was er dan eindelijk de 55 pagina's tellende overeenstemming. Deze tekst kent de woorden 'informatiebeveiliging' en 'information security' niet één keer; 'cybersecurity' staat er twee keer in. 'Privacywetgeving' wordt niet genoemd in de paragraaf over digitalisering, maar in die over gezondheid. De digitale revolutie met nieuwe technologieën biedt kansen, maar zij brengt ook een breed scala aan nieuwe vraagstukken met zich mee: 'De huidige digitale revolutie biedt geweldige kansen voor onze samenleving en economie. Die kansen gaan we benutten met uitstekende digitale vaardigheden, een sterke Europese digitale markt, hoogstaande digitale infrastructuur en ambitieuze samenwerking in technologische innovatie. Tegelijkertijd zorgt digitalisering voor een digitale kloof en groeiende ongelijkheid in onze samenleving. Ook onze veiligheid, rechtsstaat, democratie, mensen- en grondrechten en concurrentievermogen staan onder druk. Dat vraagt om solide spelregels, toezicht en strategische autonomie.'

De citaten uit het coalitieakkoord die gerelateerd (kunnen) zijn aan informatiebeveiliging:

- Wetenschap, bedrijfsleven, 'startups', 'scale-ups', kenniscoalities en overheid slaan de handen ineen om de kansen die digitale technologie biedt te verzilveren. We stimuleren innovatie en investeren in chips- en sleuteltechnologieën zoals kunstmatige intelligentie en quantumcomputing.
- We pakken (in Europees verband) de marktmacht en datamacht van grote tech- en platformbedrijven aan om de concurrentiepositie van bedrijven en de privacy van burgers te verbeteren.
- Nederland wordt het digitale knooppunt van Europa en krijgt robuust, supersnel en veilig internet in alle delen van het land.
- We nemen het voortouw en zetten in Europees verband in op versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en 'open source'.
- Iedereen krijgt de kans om mee te komen door digitale kennis- en vaardigheden aan te bieden in het onderwijs en via om- en bijscholing. We pakken digibetisme gericht aan via een publiek-private strategie voor digitale geletterdheid en we verbeteren de toegankelijkheid van digitale overheidsdiensten, met behoud van alternatieven voor digitale overheidscommunicatie.
- We willen dat inlichtingendiensten beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om nieuwe en toenemende digitale dreigingen en aanvallen assertief op te sporen en te bestrijden, met waarborgen voor goed en effectief toezicht en digitale burgerrechten.
- We beschermen onze bedrijven, vitale infrastructuur en economisch kapitaal beter door centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en 'hacks'.
- Cybercriminaliteit zoals 'ransomware' is zeer ondermijnend. We investeren daarom in een brede meerjarige cybersecurity aanpak en in cyberexpertise bij de politie, rechtspraak, het Openbaar Ministerie (OM) en defensie.
- We erkennen fundamentele burgerrechten online. We versterken daarom veilige digitale communicatie en passen geen gezichtsherkenning toe zonder strenge wettelijke afbakening en controle. We investeren in een sterke positie van de Autoriteit Persoonsgegevens en versterken samenwerking en samenhang tussen de diverse digitale toezichthouders. We regelen wettelijk dat algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur. Een algoritmetoezichthouder bewaakt dit. De overheid geeft het goede voorbeeld door niet meer data te verzamelen en onderling te delen dan nodig en ontwikkelt regels voor data ethiek in de publieke sector.
- We geven mensen een eigen 'online' identiteit en regie over hun eigen data.
- We beschermen kinderen (...en...) geven ze het recht om niet gevolgd te worden en geen dataprofielen te krijgen.
- Iedereen blijft eigenaar van de eigen gezondheidsgegevens. Gegevens- en data uitwisseling tussen patiënt/cliënt en aanbieder en aanbieders onderling wordt, conform privacywetgeving, verbeterd waarbij uniformiteit noodzakelijk is.
- We zorgen dat toezichthouders als de Autoriteit Persoonsgegevens (...) extra middelen krijgen om hun taken goed te kunnen uitvoeren.
- We maken afspraken met het bedrijfsleven en overheden over het stimuleren van thuiswerken.
- Hyperscale datacentra leggen een onevenredig groot beslag op de beschikbare duurzame energie in verhouding tot de maatschappelijke en/of economische meerwaarde. Daarom scherpen we de landelijke regie en de toelatingscriteria bij de vergunningverlening hiervoor aan.
- We versterken de expertise van de aanpak van cybercriminaliteit in alle delen van de strafrechtketen.
- We zorgen ervoor dat de grondslagen voor die gegevensuitwisseling met de juiste waarborgen, zoals doelbinding en proportionaliteit, zijn verankerd in de wet en dat in adequaat toezicht is voorzien.
- We stimuleren de vrije en veilige uitwisseling van ideeën en borgen de academische vrijheid van wetenschappers. We stellen kaders vast voor de wetenschappelijke samenwerking met onvrije landen. 'Open science' en 'open education' worden de normen, mits de nationale veiligheid hierbij niet in het geding komt.
- We zetten in op open strategische autonomie van de EU en stimuleren innovatiekracht en slimme industriepolitiek. Zo worden we leidend in digitalisering en nieuwe technologieën.
- We versterken onze specialismen in 'cyber' en inlichtingen. Dit gebeurt in nauw overleg met onze belangrijkste partners (bij de Defensieparagraaf).
- We maken afspraken met het bedrijfsleven en overheden over het stimuleren van thuiswerken.

De AP is opgericht en aangewezen als toezichthouder op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.

Algoritmetoezichthouder

De coalitie gaat 'cyber' en inlichtingen bij Defensie versterken, en zet zich ervoor in dat inlichtingendiensten beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om nieuwe en toenemende digitale dreigingen en aanvallen assertief op te sporen en te bestrijden. Dat moet zijn omgeven met waarborgen voor goed en effectief toezicht en digitale burgerrechten. Er zal wettelijk worden vastgelegd dat algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur. Een algoritmetoezichthouder moet dit gaan bewaken.

De algoritmetoezichthouder – onthoud die naam, het kan nog van pas komen bij het scrabbelen – wordt inmiddels ook al 'algoritmewaakhond' (4) genoemd en moet 'fundamentele burgerrechten' online beschermen. De nieuwe toezichthouder wordt ondergebracht bij de Autoriteit Persoonsgegevens (AP) en moet volgens plannen van het kabinet de transparantie van algoritmes bewaken en zorgen dat ze niet discrimineren of willekeurig zijn. Het aanstaande kabinet wil daarnaast investeren in de AP en de 'samenwerking en samenhang tussen de diverse digitale toezichthouders' versterken. Welke organisatie de coalitie rekent tot de 'diverse digitale toezichthouders', wordt niet helder; daarover is echter wel een uitgebreide beschrijving (5).

De AP is opgericht en aangewezen als toezichthouder op de naleving van de wettelijke regels voor bescherming van persoonsgegevens, waaronder de AVG, de Uitvoeringswet AVG (UAVG), de Wet politiegegevens (Wpg), de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Wet basisregistratie personen (Wet BRP). De taken van de AP bestaan onder andere uit: toezicht, klachtafhandeling, advisering, voorlichting en internationale taken. De budgettaire bijlage bij het coalitieakkoord vermeldt dat de separate algoritmetoezichthouder een budget krijgt van 3,6 miljoen euro per jaar. De extra gelden voor de AP bedraagt in 2023 één miljoen euro, in 2024 twee miljoen euro, in 2025 drie miljoen euro en vanaf 2026 structureel 3,6 miljoen euro, bovenop de 25 miljoen euro die de AP al krijgt. Vanaf 2022 moet de AP volgens een KPMG 2020-prognose groeien van 184 naar 470 voltijdsbanen om alle taken 'goed uit te kunnen voeren' (6). In dat onderzoek werd ook gekeken naar de doelmatigheid en doeltreffendheid van de AP en naar mogelijkheden om efficiënter te werken. De minister voor Rechtsbescherming schreef in zijn Kamerbrief van 19 november 2020: 'Geconstateerd is dat de AP nog altijd een organisatie in opbouw is. Een aantal functies zijn nog niet ingevuld, de automatiseringsgraad is laag en haar bedrijfsvoering staat nog in het begin van ontwikkeling. Volgens accountants- en adviesorganisatie KPMG is het aannemelijk dat er op termijn door leereffecten, procesoptimalisatie, investeringen in automatisering (zoals de invoering van een zaakvolgsysteem) en investeringen in de bedrijfsvoering efficiënter gewerkt kan worden. Daarnaast kan meer datagedreven en risicogericht gewerkt gaan worden. Het oppakken van risicoanalyse en effectmeting moet leiden tot een efficiëntere en effectievere uitvoering. Hier valt in de toekomst veel winst te behalen (6)." Recent berichtte de Nationale ombudsman in zijn rapport 'Voor een dichte deur', dat de AP niet goed omgaat met privacyklachten van burgers en het lijkt zelfs dat de AP de klachten voornamelijk afhoudt (8).

De kritische lezer kan opmerken dat nog niet bekend is wanneer de algoritmetoezichthouder er daadwerkelijk moet zijn en welke wettelijke bevoegdheden deze toezichthouder precies krijgt, wat er onder algoritme moet worden verstaan en

wat de reikwijdte van deze autoriteit zal zijn. Houdt ze toezicht op enkel overheidsorganen of ook op publiek-private partnerships, op (wetenschappelijke) onderzoeksinstituten, particuliere ondernemingen of wellicht internationaal opererende private bedrijven? Komt er toezicht op de algoritmen of op datgene wat een algoritme verwerkt? Als een algoritme persoonsgegevens verwerkt, dan ligt het toezicht nu al bij de AP. Bij andere vormen van data-analyse en dataverwerking waarbij geen persoonsgegevens in het geding zijn, ligt het toezicht bij instanties als het Agentschap Telecom of bij de Autoriteit Financiële Markten zolang het financiële gegevens betreft. Waarschijnlijk zal de nieuwe autoriteit gaan opereren op het snijvlak van consumentenbescherming, data- en gegevensmanagement, behoudt van de 'online' identiteit, het zelfbeschikkingsrecht over privacy- en persoonsgegevens en wellicht nog andere domeinen die door het gebruik van algoritmes geraakt worden. Het Duitse coalitieakkoord vermeldt dat: 'Voor een betere handhaving ('Durchsetzung') en coherentie van gegevensbescherming willen we voor de toepassing van de privacybescherming bindende besluiten mogelijk maken.' Dus hier rijst ook de vraag welke tanden, standvastigheid en bijtkracht de Nederlandse waakhond krijgt. Algoritmes moeten natuurlijk vooraf, heel voorzichtig worden vormgegeven, op basis van de waarden en normen die wij in dit land belangrijk vinden.

In het nieuwe kabinet zal een bewindspersoon speciale aandacht hebben voor digitalisering; net zoals in het huidige kabinet is dat de staatssecretaris van Binnenlandse Zaken en Koninkrijkrelaties.

Bekijk het eindverslag van de informateurs en het coalitieakkoord op de site van het Bureau woordvoering kabinetsformatie 2021 op: https://www.kabinetsformatie2021.nl/actueel/nieuws/2021/12/15/aanbieding-en-toelichting-eindverslag-en-coalitieakkoord

Uitwerkingen

De uitgangspunten in het coalitieakkoord zullen nog moeten worden uitgewerkt. De verwachting is dat de nieuwe bewindslieden deze uitwerkingen samen met de Voorjaarsnota in de Tweede Kamer zullen behandelen. De volgende Tweede Kamerverkiezingen staan gepland voor 2025, tenzij die vervroegd worden. Kortom, het nieuwe kabinet heeft tweeëneenhalf jaar om die plannen in daden om te zetten. Binnen de samenleving en alle organisaties vinden ontwikkelingen plaats die te maken hebben met het toenemend gebruik van ICT, digitale informatie, data- en informatiesystemen. De transitie van het computertijdperk naar het datatijdperk is volop gaande waarbij aandacht komt voor de positie van de burgers, de veilige en betrouwbare informatie en een (duurzame) innovatie. Data wordt gezien als een belangrijke aanjager voor innovatie. Er zijn daarbij volop uitdagingen rondom privacy, (data- en cyber) security, ethiek en compliance. Ook burgers/ klanten kunnen vanwege de technologieën steeds meer zelf doen: geen werkprocessen in organisaties, maar video-on-demand, in het weekend zakendoen met de bank via internet en op dinsdagavond nog even een aanvraagformulier voor een overheidsdienst invullen. De behoefte aan gespecialiseerde vakmensen wordt steeds groter: van IT-monteurs tot data/cybersecurityspecialisten.
Er is dus werk genoeg; een mooi vooruitzicht, niet?

Referenties

(1) https://zoek.officielebekendmakingen.nl/blg-1009826; bijlage bij Kamerstukken II, 2020/21, 35788, nr. 77

(2) https://www.volkskrant.nl/nieuws-achtergrond/lees-het-hier-zelf-de-proeve-van-een-regeerakkoord-van-vvd-en-cda~b4ea4d75/

(3) 'Mehr Fortschritt wagen; Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit', Koalitionsvertrag
2021-2025 zwischen der SPD, BÜNDNIS 90/ DIE GRÜNEN und den FDP, Berlin, 2021, p. 15-19: https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800

(4) https://www.nrc.nl/nieuws/2021/12/15/nieuw-kabinet-wil-algoritmewaakhond-oprichten-a4069035

(5) Zie voor een overzicht van de toezichthouders: Bijlage 3 bij de kabinetsbrief van 20 april 2020 over de Initiatiefnota 'Menselijke grip op algoritmen' en het onderzoek 'Toezicht op gebruik van algoritmen door de overheid', Kamerstukken II, 2019/20, 35212, nr. 3.

(6) https://zoek.officielebekendmakingen.nl/blg-957075

(7) Kamerstukken II, 2020/21, 25 268 en 32 761, nr. 192

(8) Nationale ombudsman 'Voor een dichte deur: Een onderzoek naar hoe de Autoriteit Persoonsgegevens omgaat met ongenoegen van burgers over de behandeling van privacyklachten', rapportnr.: 2021/139, Den Haag: 21 december 2021
https://www.nationaleombudsman.nl/system/files/bijlage/Nationale%20ombudsman%20-%20Rapport%20Autoriteit%20Persoonsgegevens%20Voor%20een%20dichte%-20deur.pdf

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Als je niet normaal bent

In Rotterdam werden personen die binnen een bepaald risicoprofiel vielen, verrast met een brief op de deurmat. Daarin stond te lezen dat zij voor een langere periode op willekeurige momenten onderworpen zouden worden aan preventieve fouillering. Een computeralgoritme had voorspeld hoe waarschijnlijk de kans was dat zij de wet zouden overtreden en dat achtte de politie voldoende rechtvaardiging. De rechter maakte gehakt van deze extreem privacyschendende maatregel: er moet namelijk een concrete aanleiding zijn om tot een dergelijke fouillering over te kunnen gaan. En die concrete aanleiding was er hier heel duidelijk niet.

De ouders van het toeslagenschandaal werden op een zwarte lijst gezet omdat zij afweken van de norm door hun achtergrond. Dat werd ingegeven door een algoritme dat onder meer scande op buitenlands klinkende achternamen en dubbele nationaliteiten. Wie op die zwarte lijst terechtkwam, werd in de gaten gehouden met alle gevolgen van dien.

Nikkie de Jager, een wereldwijd beroemde Nederlandse make-up goeroe, werd gedwongen om en plein public uit de kast te komen. Iemand wist namelijk dat zij transgender was en chanteerde haar daarmee. Om de macht uit de handen van deze persoon te halen, besloot ze dan maar zelf naar buiten te treden.

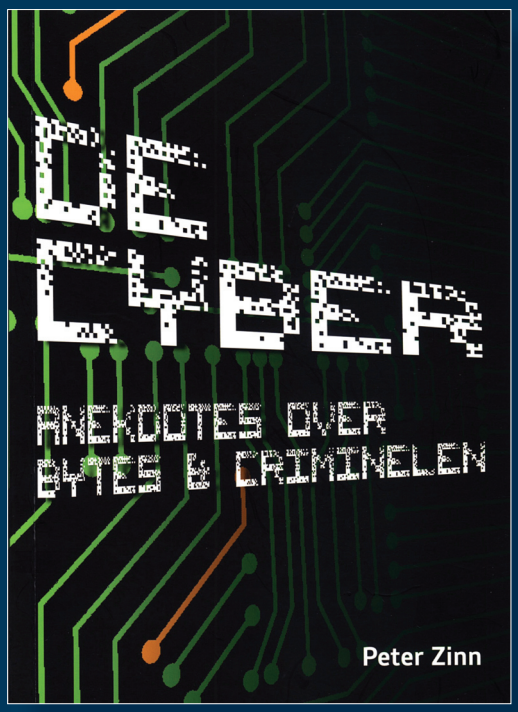
Eindhovens raadslid Mpanzu Bamenga spande een rechtszaak aan tegen de Nederlandse marechaussee omdat hij telkens het slachtoffer werd van etnische profilering als hij reisde via luchthavens. De rechter oordeelde echter dat etniciteit slechts één van de kenmerken is voor de marechaussee om iemand te controleren, en dat dat proportioneel was. En hoewel Bamenga de strijd in de rechtbank verloor, kondigde de marechaussee later aan dat ze besloten had etniciteit niet langer mee te willen wegen. Bamenga won in 2021 een mensenrechtenprijs voor zijn inzet rondom etnische profilering.

Slachtoffers van delicten hebben ook al sinds jaar en dag te kampen met privacyproblemen. Hun naam verschijnt op officiële stukken en in de pers vaak voluit en kenbaar. Adresgegevens en andere communicatiegegevens staan vaak in allerlei documenten zoals een aangifte en stukken verwant aan rechtszaken. Hoewel in 2020 door toenmalig minister Dekker in een kamerbrief het belang van privacy voor slachtoffers wel werd onderstreept, was het geen zelfstandig doel in de Meerjarenagenda Slachtofferbeleid en is tot op heden niet heel duidelijk of er inmiddels voortgang geboekt is met allerhande in de kamerbrief voorgestelde maatregelen.

Afwijken van de norm brengt heel veel kwetsbaarheden met zich mee, en levert vaak in het kielzog ook ongewenste schendingen van de privacy op. Ironisch genoeg beoogt het grondrecht op privacy nu juist ook de belangen van minderheden te beschermen zodat zij niet ondergesneeuwd raken door de sterke meerderheid. Afwijken van de norm is extra belangrijk voor de democratie, het brengt vaak allerlei maatschappelijke misstanden aan het licht. Alleen al daarom zouden mensen die 'niet normaal' zijn wat meer beschermd moeten worden en op zijn minst meer omarmd door de 'normale' meerderheid.

Rachel

Auteur: Lex Borger is security architect, docent bij Tesorion en oud-hoofdredacteur van iB-Magazine. Lex is bereikbaar via lex.borger@tesorion.nl.



Titel boek:	*De Cyber*. Anekdotes over Bytes en Criminelen
Auteur:	Peter Zinn
Taal:	Nederlands
Bindwijze:	Paperback
Aantal pagina's:	200 pagina's
EAN:	9789490969356
Prijs:	€ 24,00

BOEKREVIEW

De Cyber

De Cyber is geschreven door Peter Zinn. Zinn is spreker, ex-politieman en ex-HTC lid. HTC staat voor high tech crime, het team bij de politie dat zich specialiseert in cybercrime aanpakken. Het boek is een simpele, handzame pocket over cyber-techniek en cybercrime, omvat 200 pagina's en is mooi geïllustreerd door Marijke van Veldhoven.

Peter schrijft informatief. Alle onderwerpen die langskomen hebben één of meerdere vrije associaties met 'de cyber' en zijn door hem in één van de drie delen geplaatst. De onderwerpen die behandeld worden staan redelijk goed op zichzelf en worden geïllustreerd met verhalen (anekdotes) die het tastbaar maken. De subtitel Anekdotes over Bytes en Criminelen kan ook gelezen worden als 'ABC', wat het boek *De Cyber* ABC maakt - een encyclopedie.

Drie delen

Het boek bestaat uit drie delen: de setting (techniek en beveiliging), de spelers (verschillende groeperingen) en de acties (cyberaanvallen). De delen zijn behoorlijk vervlochten, zodat je, om een goed overzicht te hebben, ze allemaal door moet werken.

Wat door deze opbouw ontbreekt is een onderliggende boodschap, anders dan dat cybertechniek en -crime niet anders zijn dan andere techniekontwikkelingen en misdaadactiviteiten in de geschiedenis. Peter laat in de opzet van het boek ook weten dat hij mensen graag warm maakt voor security zonder ze bang te willen maken. Daar past dit boek bij. De onderwerpen worden goed gepositioneerd. De anekdotes verrijken de onderwerpen.

Kritische noot

Ik heb een paar kritische opmerkingen:
Het boekt opent met de anekdote die ook gelijk de vreemd-klinkende titel verklaart, het verhaal over minister Opsteltens bezoek aan het HTC-team (pagina 11). Ik had dit verhaal eerder gehoord, maar dan met de kreet: 'De Cybers'. Of het nu enkelvoud of meervoud is, het laat zien dat bij politici de eenvoudige uitleg blijft hangen. In de VS noemde senator Stevens het internet 'A Series of Tubes' (https://en.wikipedia.org/wiki/Series_of_tubes). Ik kan me zo voorstellen hoe zijn equivalente voorstelrondje bij de NSA of ander bureau is gelopen.

Op pagina 61 vertelt Peter een anekdote over Donald Knuth. Een bijzonder begaafde man in de softwarewereld. Hij schreef de encyclopedie *The Art of Computer Programming*. Iemand die zo structureel kan denken dat hij zonder te testen foutloze programma's kon schrijven in een tijd dat programmeren als vak nog uitgevonden moest worden. Zeg maar de uitvinder van 'security by design'. Dus als hij zegt dat hij bang is voor bugs in een programmaatje van 26 regels…

Peter maakt geen onderscheid tussen asymmetrische en symmetrische cryptografie. Gegeven de toon van de rest van het boek is dat op zich geen probleem, hij blijft consequent weg van de technische details. Maar in dit geval is het toch lastig, omdat hij in relatie tot DES verwijst naar de sleutellengte en de grootte van bijbehorende priemgetallen (pagina 171). Dit zal mensen die meer over crypto willen leren verwarren.

Meer boeken over dit onderwerp

De afgelopen drie jaar zijn er aardig wat Nederlandstalige boeken uitgekomen die het kennisgebied cybertechniek, cybersecurity en cybercrime breed beschrijven. Ik heb er vier op mijn boekenplank staan en vergelijk ze met *De Cyber:*

- *Cyberellende was nog nooit zo leuk* van Chris van 't Hof. Chris is een echte insider, die vanuit dat perspectief de boodschap naar buiten brengt. Hij schuwt de technische details niet, maar maakt ze bespreekbaar. En hij doet dit door te schakelen met de spelers aan alle kanten. *De Cyber* is toegankelijker voor niet-technici.
- *Het is oorlog, maar niemand die het ziet* van Huib Modderkolk. Huib is journalist en schreef dit boek als een serie van specials zoals je die in de zaterdag-uitgave van de Volkskrant zou kunnen lezen. Goede journalistiek, nuttig om te lezen, maar het bevat alleen de smeuïge kant, meestal met de focus op de cybercrime. Ten opzichte van *De Cyber* een andere stijl: spannender, maar met een open einde, geen oplossingen.
- *Survivalgids voor de digitale jungle* van Brenno de Winter. Dit is het handboek dat je oppakt nadat je *De Cyber* gelezen hebt en tot de conclusie komt dat je iets moet doen met cybersecurity, maar geen flauw idee hebt hoe of waar je moet beginnen.
- *Unhacked* van Rian van Rijbroek. Dit is het meest omvangrijke boek, maar laat ik gelijk duidelijk zijn: het is een algemene afrader, tenzij je het als een verhalenbundel ziet waarbij de grens tussen fictie en realiteit vloeibaar geworden is en af en toe humoristisch kan zijn. Inhoudelijk staat het vol met cyberincidenten en cybertechniekdetails die sensationeler zijn gemaakt en vaak onvolledig of incorrect zijn. Het is daarmee de tegenpool van *De Cyber.*

Al met al is *De Cyber* een boek dat ik met plezier gelezen heb en zonder problemen iedereen die meer wil weten over informatiebeveiliging kan aanraden. Zeker voor mensen buiten het professionele werkveld, zoals managers, vrienden en familieleden en andere geïnteresseerden.

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

BLOG

Adequate aanpak van antivirus

Op elke computer een antivirusprogramma installeren is geen slecht idee – maar ook geen perfect idee. Hieronder licht ik de voor- en nadelen van diverse aanpakken toe.

Veel antivirusprogrammatuur werkt door te letten op iets kenmerkends dat de broncode van het computervirus in zich heeft. Dit noemen we signature (handtekening) gebaseerd. Natuurlijk zijn alleen bekende handtekeningen te herkennen en deze soort AV-programmatuur loopt dus altijd achter de feiten aan. Zeker wanneer de malware-ontwikkelaars nieuwe varianten van de virussen programmeren. Door 'obfuscatie' veranderen zij de broncode, waarbij de kwaadaardige functionaliteit hetzelfde blijft. Obfusceren kan met geautomatiseerde tools of gewoon met de hand, bijvoorbeeld door een andere programmeertaal te gebruiken of alle variabelen, processen en labels in de broncode een nieuwe naam te geven. De oude handtekeningen (als een soort 'spikes') zijn dan niet meer te signaleren.

Schijnzekerheid

Op sommige websites kun je als eindgebruiker verdachte software uploaden om deze te laten analyseren. Bijvoorbeeld www.virustotal.com meldt of een aantal popu-

laire AV-programma's in de aangeboden versie van de software een virus herkennen. Het is een soort parallelle PCR-test. Ook hier geldt dat een dergelijke scan-website nooit actueler kan zijn dan de individuele voortdurende bijgewerkte handtekeninglijsten van de door hen gebruikte AV-software. Als de in die lijsten gebruikte handtekeningen te kort of te algemeen zijn (bijvoorbeeld: in de broncode van het virus komt de letter A voor), wordt te veel software als virusverdacht aangemeld. Dit geeft veel 'false positives' over 'besmettingen' en leidt daarmee tot onnodige paniek. Langere en specifiekere handtekeningen geven bij een gevonden infectie meer zekerheid dat het werkelijk een bepaald virus is. Maar zeer specifieke handtekeningen hebben, in elk geval bij nieuwe virusvarianten, als bijwerking veel 'false negatives'. In de virusbestrijding zijn die door de gewekte schijnzekerheid nog gevaarlijker.

Boeven testen hun malware ook

Bovendien testen eerdergenoemde boeven (de kwaadwillende ontwikkelaars) hun malware zelf ook bij Virustotal. Om met de testresultaten hun virus net zolang bij te stellen en te schaven totdat het niet meer herkend wordt door de selectie van AV-pakketten bij die scan-website. Als consument ben je dus soms beter af met een onbekend AV-pakket van een kleine, beginnende leverancier. Omdat die een (nieuw) virus dat precies de door Virustotal gebruikte checks weet te omzeilen, wel herkent.

De schijnzekerheid van 'de meervoudige virusscanner zag niks, dus ik ben veilig' kan helaas nog verergeren. Namelijk wanneer Virustotal de selectie door hen gebruikte AV-pakketten ooit zou beperken tot slechts één super-AV-pakket. Consumenten zouden vervolgens wereldwijd ook massaal kunnen kiezen voor dit ene AV-pakket, als 'beste keuze volgens de Consumentenbond'. Dat is zeker zo wanneer internationale overheden daarbij hun onderdanen met boetes, hogere premies en belastingen en gevangenisstraf zouden stimuleren om voor dat ene pakket te kiezen. Ik zeg niet dat een dergelijke monocultuur totaal niet werkt tegen virussen. Maar wel dat hij niet altijd zal blijven werken. Met name niet wanneer een (nieuw) virus opduikt dat juist dat ene - tegen die tijd door iedereen gebruikte AV-pakket - weet te omzeilen.

Blij met eigenwijze mensen

Om het bestaan van een nieuw virus te ontdekken, ben je soms blij dat er nog eigenwijze mensen zijn die een ander AV-programma gebruiken dan de 'global standard'. En die niet op vreemde linkjes klikken, nooit ongevraagde software installeren maar zelf steeds verdacht gedrag van hun computer monitoren en daarop actie ondernemen. Zoals de verdachte computer loskoppelen van het (draadloze) netwerk en het apparaat in complete isolatie of quarantaine plaatsen en dus ook geen 'sneakerinterface' naar andere computers via USB-sticks gebruiken. Ook zijn er gebruikers die zelfs onbaatzuchtig een computer volledig onbeschermd als 'honeypot' aan het internet koppelen. We mogen hen dankbaar zijn, omdat ze helpen om nieuwe virussen te ontdekken. Je vangt immers meer vliegen of tijgerhorzels met honing dan met azijn.

Heuristische AV-aanpak

Er is nog een andere aanpak in de virusbestrijding: AV-pakketten die niet zoeken naar de aanwezigheid van bepaalde handtekeningen, maar juist het gedrag van het virus monitoren. Dit is de heuristische AV-aanpak. Worden meteen na installatie alle mailadressen op de computer opgehaald door een niet-mailpakket? Zijn er veel lees- en schrijfacties naar de harde schijf (of naar het intern geheugen bij 'fileless malware')? Worden daarbij bestanden opgehaald, bewerkt (lees: versleuteld) en meteen daarna opgeslagen, zoals ransomware dat doet? Deze gerichte aanpak van verdacht gedrag is in mijn ogen een betere manier van virusbestrijding. Het is trouwens ook doeltreffender bij security awareness en gedragsverandering, waarover ik al eerder schreef.

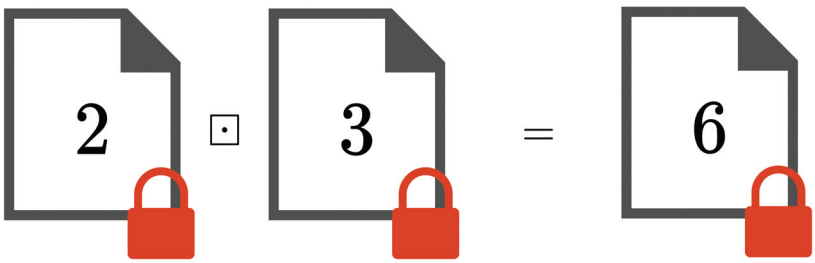
Inderdaad, ook heuristische antivirus-programmatuur kan na verloop van tijd verdacht gedrag gaan missen, wanneer het een totaal nieuwe aanvalstechniek of 'modus operandi' is. Maar als de verdachte gedragingen op voldoende abstracte niveau zijn gedefinieerd, veroudert deze test op virus-activiteit veel langzamer dan een beveiliging gebaseerd op virus-(deel)identiteit. En worden nieuwe virussen met het oude gedrag nog steeds onderkend, zodat tijdig mitigerende actie mogelijk is. En dat is in computervirusbestrijding 'positief' (excusez le mot).

Auteur: Dieuwke van der Ende is werkzaam bij het ministerie van Defensie als Cyber Security Researcher. Ze heeft dit onderzoek gedaan bij TU Delft in samenwerking met TNO. Dieuwke is bereikbaar via dieuwkevdende@gmail.com.

Onderzoek: evalueren beslisboom met privé input data

Op 6 oktober 2021 vond de uitreiking van de Joop Bautz Information Security Award plaats, waar ik de eer had om samen met Bhaskar Dercon, Jeroen Gaiser en Dilara Toprakhisar onze scripties te presenteren. Ik was erg verrast en blij toen ik hoorde dat ik de award had gewonnen! Voor mijn scriptie heb ik onderzoek gedaan naar het evalueren van een beslisboom terwijl de input data, die afkomstig is van meerdere partijen, privé blijft. Hiervoor heb ik gebruik gemaakt van een techniek genaamd homomorfische encryptie.

$$2 \cdot 3 = 6$$



Afbeelding 1 - Homomorfische vermenigvuldiging.

Beslisbomen kennen vele toepassingen. Denk bijvoorbeeld aan de detectie van malware, spam, fraude of het doen van de juiste productaanbevelingen (Portugal et al., 2018; Gibert et al., 2020). Daarnaast kunnen beslisbomen worden toegepast bij toegangscontroles, door te toetsen of iemand toegang mag hebben tot bepaalde systemen of documenten. Een belangrijk voorbeeld daarvan is de medische wereld, waar het voor een goede behandeling van patiënten cruciaal is dat artsen toegang hebben tot hun medische dossiers. Sommige artsen pleiten zelfs voor één Elektronisch Patiënten Dossier (EPD), waarin alle medische dossiers van patiënten te vinden zijn (Pieterman, 2020). Voor een goede implementatie is het van essentieel belang dat er een toegangscontrole is die de huidige context in beschouwing neemt en ervoor zorgt dat er alleen toegang wordt verleend aan de juiste artsen. Alleen zij mogen bij de bestanden die daadwerkelijk nodig zijn voor de huidige behandeling van de patiënt. Het gebruik van beslisbomen is hier een mogelijke oplossing.

Gevoelige data

Beslisbomen hebben voor het maken van keuzes toegang nodig tot data die vaak gevoelig of privé is. Deze data is meestal afkomstig van verschillende organisaties voor wie het delen van gevoelige informatie buiten de organisatie vaak moeilijk of zelfs onmogelijk is. Banken kunnen samenwerken en hun financiële dossiers combineren voor het detecteren van fraude (Sangers et al., 2019) en daarbij gebruikmaken van bijvoorbeeld beslisbomen. Samen kunnen ze meer conclusies trekken dan alleen, maar het delen van financiële data is vaak moeilijk. Ook voor het juist functioneren van een beslisboom als toegangscontrole tot medische dossiers, is gevoelige data nodig van bijvoorbeeld ziekenhuizen, huisartsen en/of spoedposten. Dit kan data zijn over bijvoorbeeld artsen, patiënten en inhoud van de dossiers. Het gebruik van beslisbomen in deze toepassingen kan dus alleen plaatsvinden wanneer de privacy van de input data wordt gewaarborgd.

Collaboratieve setting

Er zijn meerdere onderzoeken gedaan naar het evalueren van beslisbomen waarbij de vertrouwelijkheid van de input data wordt gewaarborgd (Tai et al., 2017; Tueno et al., 2020). Echter, geen van deze oplossingen kan worden gebruikt wanneer de input data vanuit meerdere organisaties afkomstig is. Dit noemen we een collaboratieve setting. Samenwerking bij het evalueren van beslisbomen is steeds meer nodig en is vaak alleen mogelijk als de privacy van de data van alle partijen wordt gewaarborgd. Ons onderzoek zet de eerste stap in de richting van het evalueren van een beslisboom terwijl de input data, dat afkomstig is uit meer dan één bron, privé blijft.

Homomorfische encryptie

Ons werk maakt gebruik van homomorfische encryptie. Dit is een type encryptie dat ervoor zorgt dat berekeningen – wis-

kundige operaties –, gedaan kunnen worden over versleutelde data. Het resultaat is een encryptie van de waarde die de berekeningen zouden hebben over de normale, niet geëncrypte data. Zoals te zien in afbeelding 1 maakt homomorfische encryptie het mogelijk om een vermenigvuldiging van 2 en 3 te doen wanneer deze waarden zijn versleuteld (en dus niet zichtbaar).

Deze versleuteling, of encryptie, is in de afbeelding aangegeven met het rode slot. Het resultaat van deze homomorfische vermenigvuldiging, is een encryptie van de waarde 6. De daadwerkelijke waarde 6 is alleen zichtbaar als iemand over de juiste sleutel beschikt die `het rode slot kan openmaken', ofwel de encryptie kan ontcijferen.

Aangezien beslisbomen bestaan uit meerdere berekeningen of vergelijkingen van stukjes data, kunnen we de input data versleutelen en de berekeningen van de beslisboom homomorfisch uitvoeren. De moeilijkheid hierbij is dat voor het oplossen van onze probleemstelling, nu alle stukjes data versleuteld worden door verschillende partijen. Homomorfische berekeningen, zoals hierboven omschreven, kunnen alleen gedaan worden met data die versleuteld is met dezelfde sleutel.

Drie protocollen

In ons werk zijn drie protocollen voorgesteld om dit wél mogelijk te maken. Deze protocollen maken gebruik van de techniek genaamd `Multi-Key Fully Homomorphic Encryption' of de techniek `Fully Homomorphic Encryption' (Peikert & Shiehian, 2016). Deze eerste techniek maakt het mogelijk om homomorfische berekeningen te doen op data die is versleuteld met verschillende sleutels.
De tweede techniek maakt het mogelijk deze data te combineren door een extra partij te introduceren van wie de encryptiesleutel wordt gebruikt, maar verder geen kennis vergaart wat betreft de input data of de beslisboom.
In het derde protocol wordt een zogenaamde `sleutelwisseling' voorgesteld die ervoor zorgt dat de protocollen minder afhankelijk zijn van deze extra partij.

Conclusie

Alle protocollen zijn geïmplementeerd en met elkaar vergeleken voor wat betreft de complexiteit, runtijd en benodigde communicatie tussen de verschillende partijen. Daaruit kwam naar voren dat de techniek `Multi-Key Fully Homomorphic Encryption' erg complex is, wat resulteert in te hoge, en daarom niet praktische runtijden. De andere twee protocollen zijn daarom het meest haalbaar. Onze implementatie, als we aannemen dat de computaties in parallel gedaan kunnen worden, gaf een hoogst haalbare runtijd in de ordegrootte van dagen. Gelukkig hangt de efficiëntie van onze protocollen direct af van de efficiëntie van de onderliggende encryptieschema's, dus verbetering is niet uitgesloten. Met dit werk is de eerste stap gezet naar mogelijke oplossingen om in een collaboratieve setting een beslisboom privé te evalueren, waarvoor er vele interessante toepassingsgebieden bestaan.

Ben je na het lezen van bovenstaand stuk nieuwsgierig geworden naar de inhoud? Via deze link is de scriptie te downloaden: http://resolver.tudelft.nl/uuid:50073f62-cf87-40d1-bef3-e407b5a5b949.

Referenties

Gibert, D., Mateu, C., & Planes, J. (2020, March 1). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. Journal of Network and Computer Applications, 153. 10.1016/j.jnca.2019.102526

Peikert, C., & Shiehian, S. (2016, October 21). Multi-key FHE from LWE, Revisited. Theory of Cryptography Conference, 217-238. 10.1007/978-3-662-53644-5_9

Pieterman, H. (2020, December 10). Geef huisarts spilfunctie in epd. Medisch Contact. https://www.medischcontact.nl/nieuws/laatste-nieuws/artikel/geef-huisarts-spilfunctie-in-epd.htm

Portugal, I., Alencar, P., & Cowan, D. (2018, May 1). The use of machine learning algorithms in recommender systems: A systematic review. Expert Systems with Applications, 97, 205-227. 10.1016/j.eswa.2017.12.020

Sangers, A., van Heesch, M., Attema, T., & Veugen, T. (2019). Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection. Financial Cryptography and Data Security, 605-623.

Tai, R. K. H., Ma, J. P. K., Zhao, Y., & Chow, S. S. M. (2017, August 12). Privacy-Preserving Decision Trees Evaluation via Linear Functions. European Symposium on Research in Computer Security, 494-512. 10.1007/978-3-319-66399-9_27

Tueno, A., Boev, Y., & Kerschbaum, F. (2020, June 18). Non-interactive Private Decision Tree Evaluation. IFIP Annual Conference on Data and Applications Security and Privacy, XXXIV, 174-194. 10.1007/978-3-030-49669-2_10

COLUMN LEX

Het jaar onder de oppervlakte

We hebben een kwetsbaar jaar achter de rug. Nog niet eerder werden er zoveel zero-days ontdekt met zoveel impact als in 2021. De log4shell kwetsbaarheid in log4j zal nog jaren na-echoën, het maakt bijna dat we vergeten dat er eerder dit jaar nog andere kwetsbaarheden zijn langsgekomen.
Microsoft had een drietal episodes. Allereerst de Microsoft Exchange servers in januari, waarbij vier zero-days gezamenlijk een totale overname van een exchangeserver mogelijk maakten. Een klassieke kill-chain: authentication bypass, privilege escalation tot admin, en twee methodes voor remote code execution. Pas in maart kwamen er patches beschikbaar en waren er al een kwart miljoen exchangeservers gecompromitteerd.

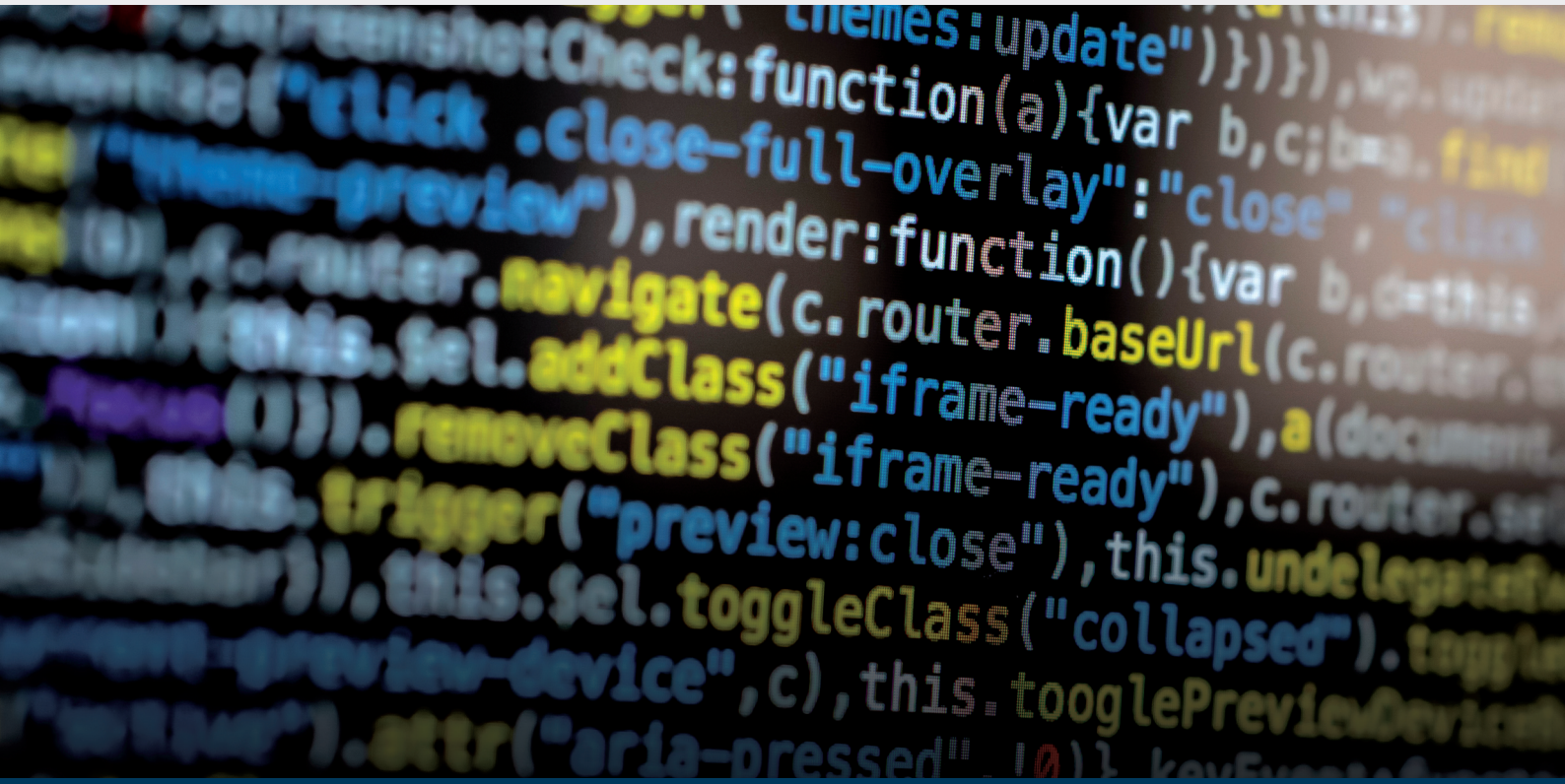
De volgende, een maand later, was PrintNightmare. Het aloude print-spooling systeem in Windows bleek ook kwetsbaar voor remote code execution en privilege escalation. De patches blokkeerden ook (kwetsbare) standaardfunctionaliteit, wat tot extra verwarring leidde. Dit werd meteen gevolgd door HiveNightmare/SeriousSAM. Dit was een configuratiefout in de Windows standaardinstallatie, waardoor de SAM (Security Account Manager) database door gewone gebruikers gelezen kon worden. Dell had ook een vergelijkbare access control kwetsbaarheid in november in hun dbutil driver, die standaard meegeleverd wordt. Het frappante is dat flink wat van deze kwetsbaarheden geen codeerfouten waren, maar eigenlijk voortvloeiden uit bedoelde functionaliteit, die door de algemene internetconnectiviteit uiteindelijk massaal te misbruiken zijn. De functionaliteiten in je software bepalen dus ook de grootte van je aanvalsoppervlakte (attack surface).

Wat gaat het komend jaar dan brengen? Eerst een schot voor open doel: ransomware-aanvallen blijven komen, en ze zullen zich aanpassen door nieuwe tactieken te gebruiken. De COVID-19 pandemie heeft de verschillen in de wereldpolitiek zichtbaarder gemaakt en spanningen gebracht of uitvergroot. Verwacht dus dat nation-state aanvallers meer noodzaak hebben zich te nestelen in de infrastructuur van anderen om te spioneren en potentieel te verstoren. De aanvalsoppervlakte van organisaties is tijdens de COVID-19 pandemie veranderd. Het werken op afstand is de norm geworden binnen organisaties. Zelfs grote bedrijven zweren er nu bij. Dit maakt dat thuiswerkomgevingen onderdeel zijn geworden van deze oppervlakte, met alle IoT-apparaten die daarbij horen. Daarnaast is er meer OT gekoppeld met IT om remote beheerd te kunnen worden, wat potentieel ook weer de oppervlakte uitbreidt. Supplychain beveiliging is al een aantal jaren een aandachtspunt, CISO's moeten meer beveiligen middels afspraken en controles dan dat ze zelf kunnen beveiligen met maatregelen. Preventie is niet langer genoeg. Monitoren van de omgeving en het inrichten van detectie en response processen wordt essentieel. Het effectief gebruik van beschikbare threat intel is belangrijk. Het delen van deze informatie is van belang voor iedereen.

Een andere uitbreiding van de aanvalsoppervlakte is het gebruik van clouddiensten. Vooral de SaaS-vorm van dienstverlening introduceert een vergroting door de uitdaging om de verschillende klanten gescheiden te houden in een multi-tenancy dienst. Ook de onderliggende cloud-API's zelf worden direct aangevallen. De aanvalsoppervlakte is zo bepalend dat deze centraal zou mogen staan in het cybersecurityplan van je organisatie. Allereerst voor de preventie: er is de laatste jaren zoveel gewijzigd in het IT-landschap dat het nodig wordt om te evalueren of we nog werken volgens de beveiligingsprincipes die we altijd al gebruikten in het opzetten van de eigen IT. De principes zijn nog altijd geldig, maar de invulling daarvan moet wellicht heel anders ingestoken worden. De adoptie van een zero-trust architectuur, hardening op dienstniveau en toegangsbeheer blijken een effectieve aanpak te zijn tegen cyberaanvallen. En ook bij de detectie en respons moeten we rekening houden met de aanvalsoppervlakte in de breedste zin. Hiervoor is een goed zicht op de gehele oppervlakte nodig. Je moet kunnen monitoren en valideren dat alles naar behoren werkt. De log4shell kwetsbaarheid in log4j heeft pijnlijk duidelijk gemaakt hoe slecht we inzicht hebben in welke software-libraries waar gebruikt worden en hoe deze afhankelijkheden beheerd moeten worden.

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

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.



Log4shell - een cadeau voor de maatschappij aan het einde van 2021?

Log4shell is een referentie naar een kwetsbaarheid in een Java class Log4j. De wereld werd op 10 december 2021 verrast door het bekend worden van deze kwetsbaarheid, terwijl dit al eerder ontdekt was. Velen dachten: "We hebben wel meer kwetsbaarheden in onze infrastructuur, wat is het probleem?"

Er bestaat een unauthenticated remote code execution kwetsbaarheid in de populaire Java-library 'Apache Log4j 2'. Deze library wordt door veel op Java gebaseerde toepassingen gebruikt voor logging doeleinden. Door de kwetsbaarheid kan een aanvaller een willekeurige code uitvoeren binnen het Java-proces. In het Financieel Dagblad werd dit vergeleken met suiker. Het zit in allerlei producten, soms zonder je medeweten (1). Door deze kwetsbaarheid zijn alle organisaties alert gemaakt van het belang van cybersecurity. Is dit een mooi cadeau of niet?


Chris de Vries


Fook Hwa Tan


Maarten Hartsuijker

Patching is belangrijk, maar niet altijd even makkelijk – Fook Hwa Tan

Het waren drukke dagen voor de kerst, toen veel organisaties hun infrastructuren moesten inventariseren om na te gaan of deze java-library aanwezig was. Velen begonnen in te zien hoe belangrijk het kennen van je eigen IT-omgeving wel niet is. Je kunt niet controleren wat je niet weet. Uitdaging bij deze kwetsbaarheid was ook, dat het niet altijd duidelijk was of de software gebruik maakte van deze java-library. Het was een race tegen de klok om zowel van buiten als van binnen je netwerk af te speuren naar het gebruik van deze programmatuur.

Vervolgens werd je geconfronteerd met het feit dat oudere software mogelijk niet zo kwetsbaar was en dat het slechts om specifieke versies ging. Er kwamen discussies op gang over wat het nut ervan was om deze oude versies te updaten, omdat je nu niet kwetsbaar zou zijn. Soms werd dit zelfs aangedragen als bewijs, dat actueel houden van software soms misschien ook slecht is voor je beveiliging. Neemt niet weg dat in oudere versies van deze software er natuurlijk ook nog andere kwetsbaarheden zaten die je zou willen patchen.

Als laatste verrassing kwam men er na een aantal dagen achter dat de patch ook nog kwetsbaar was en er inmiddels ook weer een nieuwe versie beschikbaar werd gesteld. Wil je na een hectische week patchen, nogmaals alle systemen patchen? Patchen is belangrijk, maar last minute van alles moeten bijwerken is vaak geen doen!

Nog lang last van Log4j – Maarten Hartsuijker

Log4Shell heeft ons allemaal weer even gewezen. En hoewel dat goed is voor ons 'veiligheidsbewustzijn', is een lek als dit natuurlijk een verschrikking. Gelukkig kwamen er snel patches en workarounds beschikbaar. Maar waar deze kwetsbaarheid zich enorm in onderscheidt van de andere kwetsbaarheden, is zijn complexiteit. Daar waar misbruik ervan uitblonk in eenvoud, is het voor veel organisaties verschrikkelijk moeilijk om in te schatten wáár ze precies kwetsbaar voor zijn.
Waar je een belangrijke Windows of Linux update over het algemeen met één druk op de knop doorvoert, moet je er bij Log4j eerst erachter komen of de module ergens verstopt zit. Als je eigen development teams hebt die software bouwen, kunnen de teams dit veelal bij software die nog actief in ontwikkeling is wel snel inschatten. Maar neem je applicaties of software af van derden, dan is dit al veel lastiger. Is log4j aanwezig? Bevat de laatste firmware ook de patch? Deze informatie wordt door leveranciers vaak niet actief noch in detail gedeeld. En als berichten de keten in gaan en ergens diep in het netwerk een applicatie raken van een log4j module erin, dan is het ook eenvoudig om de kwetsbaarheid over het hoofd te zien óf in te schatten wat de impact van de kwetsbaarheid is. We gaan van dit lek nog heel erg lang last hebben.

Bewustworden, bewustzijn en onvermogen – Chris de Vries

Soms ligt het antwoord zo voor de hand en schrijf je 1-2-3 de waarheid op. Dan begin je te twijfelen, verlangzaam je het denken en ga je op zoek naar wijsheid. Ik wil er op zo'n moment weleens een etymologisch of een groot woordenboek der Nederlandse taal op naslaan. Zo ook hier:

- bewustworden: het proces van betekenis toekennen aan gebeurtenissen in de praktijk;
- bewustzijn: het vermogen tot besef, tot weten en erkennen van jezelf en van de dingen;
- onvermogen: de machteloosheid om ondanks het bewustzijn de situatie aan te passen!

En wat heeft dit nu te maken met het Log4j hoor ik u denken? Veel. In december (van vorig jaar) hoorden wij van deze grote dreiging. Ik werd erop geattendeerd door een relatie en vele anderen vernamen het via het nieuws. Ah … het proces van bewustworden!
Vervolgens het besef dat de dingen niet zijn zoals ze horen te zijn (de gevaren) en de start van het zoeken naar oplossingen (`patches' of hardware aanpassingen). Bingo … het bewustzijn naar vermogen te acteren of te laten acteren! En drie: de oplossing implementeren. Eh… welke? Nee toch, sta ik opeens voor mijn onvermogen? Dat hield in mijn geval in dat ik niet in staat bleek om alle mogelijke kwetsbaarheden op te sporen en dat na raadpleging van mijn systeembeheerder het meest effectieve was om mijn iDrac-kabel los te koppelen en aanvullende 'back-ups' te draaien. Conclusie: zo leidt 'awareness' niet altijd tot preventie. Wederom blijkt dat het MKB vaak niet in staat is zelf de dreiging te keren en professionals – naar beste eer en geweten – kunnen trachten dat op te lossen, maar dat evenmin kunnen garanderen. Wat nu…? Een soort klimaatverandering die wij maar lijdzaam hebben te ondergaan? Oftewel spreken wij hier over een 'total system hack', niet te verwarren met de 'total recall' film!

Referentie

(1) https://fd.nl/tech-en-innovatie/1423175/nationale-cyberwaakhond-roept-beveiligers-bijeen-vanwege-wereldwijd-lek-xca2cawKb9w0

15 PvIB reconnect in cyber security

COLOFON

iB is het huisorgaan van het Platform Informatiebeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

HOOFDREDACTEUR
Nicole van Deursen

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

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Raalte

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 2022 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

(Advertorial)

REUZADO INTRODUCEERT DATAVERNIETIGING OP LOCATIE

Reuzado is gespecialiseerd in het veilig inzamelen, vervoeren en vernietigen van data en datadragers. Elke stap in dat proces voldoet aan strenge eisen, is 100% beveiligd en milieuvriendelijk. Zelfs de minuscule, onbruikbare snippers die overblijven na het vernietigen van datadragers worden zoveel mogelijk op duurzame wijze gerecycled. Het is nu ook mogelijk om data en datadragers op het terrein van de klant te vernietigen.

Wat zijn de voordelen:

- Transport is overbodig; voor bepaalde branches een must;
- De klant, of een bevoegde controleur, kan ter plekke vaststellen dat de datadragers en/of data definitief zijn vernietigd;
- Iedere stap in dat proces wordt gedocumenteerd;
- De klant ontvangt van elke vernietigde datadrager een vernietigingsbewijs met serienummer;
- Reuzado garandeert dat vernietiging 100% veilig en volledig heeft plaatsgevonden;
- Het vernietigen van data en/of datadrager wordt altijd door eigen personeel uitgevoerd.

Meer weten?

Meer weten over mobiele datavernietiging of de andere diensten van Reuzado ICT Services? Neem dan contact met ons op via e-mail (circulair@reuzado.nl) of telefonisch via 023 5519821. De medewerkers leggen graag uit wat er mogelijk is. Reuzado staat voor transparante communicatie, glasheldere offertes en 100% veilige datavernietiging.

Over Reuzado

Reuzado, Esperanto voor 'hergebruik', is dé expert voor alles op het gebied van ICT. Het bedrijf is ISO 9001 gecertificeerd en alle werkzaamheden worden verricht conform DIN 66399. Op dit moment wordt gewerkt aan zowel ISO 14001 als ISO 27001 certificering en Weeelabex/Cenelec 50625. Voor meer informatie: https://reuzado.nl/

TSTC

ICT en Security Trainingen

ADVANCE YOUR CAREER WITH SECURITY IN 2022

CSA - Certified SOC Analyst
GSEC - Giac Security Essentials
GPEN - Giac Penetration Tester
EDRP - Disaster Recovery Professional
EHF - Ethical Hacking Foundation
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v11
CPENT - Certified Penetration Testing Professional

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 weer klassikaal of Live Online te volgen