INFORMATIEBEVEILIGING MAGAZINE

DOSSIERS

Goed wachtwoordmanagement & wat als het faalt!?

Europese soevereiniteit in de schijnwerpers

Belangrijk vernieuwde regelgeving

JAARGANG 26 - 2026 - EDITIE 2

INFORMATIEBEVEILIGING MAGAZINE

Op zoek naar verbinding

Het IB Magazine van PvIB zoekt nieuwe redactieleden. Heb je passie voor informatiebeveiliging en wil je meebouwen aan hét magazine dat vakgenoten verbindt? Schrijf je graag of denk je mee over onderwerpen? Dan pas je perfect in ons team!

Ervaring is mooi meegenomen, maar vooral jouw motivatie telt. Samen zorgen we voor een sterk en relevant magazine, dóór en vóór professionals.

Nieuwsgierig?
Mail ons via ibmagazine@pvib.nl – we maken graag kennis!

PvIB
Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Tim Deahl
Alex Dingemanse
Maarten Hartsuijker
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
Fook Hwa Tan
Chris de Vries
Zoëlle Yusufi

BLADMANAGEMENT
Congres- en Organisatiebureau Interactie BV
Zeynep Turkan
ibmagazine@pvib.nl

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Horapark 9
6717LZ Ede
+31 85 799 0233
secretariaat@pvib.nl
www.pvib.nl

Heb je vragen, opmerkingen of suggesties, mail dan naar ibmagazine@pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2026 bedraagt € 123,- (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

Redacteur zijn, is dat nou leuk?

Chris de Vries

Het redactiewerk is een vak van uitersten. Soms is het hard werken wanneer bijdragen uitblijven, maar de laatste jaren worden we vaker verrast door spontane inzendingen van bevlogen auteurs. Het mooist is ons werk wanneer we in themanummers en dossiers verschillende facetten van een onderwerp kunnen belichten, verrijkt door onverwachte ontmoetingen met vakmensen die we in het dagelijks leven zelden spreken.

In dit nummer keert de rubriek 'Achter Het Nieuws' na een jaar van afwezigheid terug. En we pakken direct uit met het thema Vrijheid. Vijf redacteuren reageren op een scherpe voorzet over onze tijdsgeest: democratie versus tirannie, de macht van geld en — specifiek voor ons vakgebied — digitale soevereiniteit. Denk hierbij aan Open Source-oplossingen die ons losmaken van Big Tech en onze privacy waarborgen. Een thema om eens goed op u te laten inwerken.

Daarnaast besteden we uitgebreid aandacht aan het dossier 'Wachtwoorden en bedreigingen'. Naast professionele visies op digitale hygiëne en de aanvalstechniek ClickFix, leest u het openhartige verhaal van een ondernemer die zijn bloeiende bedrijf door een hack vernietigd zag worden. Een relaas over vallen, opstaan en de weg van het 'nu' naar de toekomst.

VERDER IN DIT NUMMER:

BIO2: Auteurs van het Ministerie van BZK lichten toe wat deze vernieuwing betekent voor het volwassenheidsniveau van informatiebeveiliging bij de overheid.

Soevereine smartphones: Ronald Eygendaal onderzoekt in hoeverre Europese toestellen écht onafhankelijk zijn.

Columns: Persoonlijke inzichten en pareltjes van Lex Borger, Rachel Marbus en Nicole van der Meulen.

Wij danken alle redacteuren, columnisten en auteurs voor hun onvolprezen medewerking aan dit nummer. We nodigen u als lezer uitdrukkelijk uit om te laten weten wat u waardeert, wat beter kan, of waar u zelf als potentieel auteur aan zou willen bijdragen.

Ons magazine verschijnt in een roerige tijd van oorlog en veranderende maatschappelijke waarden. We sluiten daarom graag af met een passend *citaat van George Bernard Shaw: "Vrijheid betekent verantwoordelijkheid. Daarom zijn de meeste mensen er bang voor."*

Veel leesplezier en graag tot de volgende uitgave.

Chris

Rectificatie IB.1-2026

In aansluiting op het artikel van Petter Glenstrup inzake: "NIS2-compliance is een voortdurend proces en geen reden tot paniek" (IB.1-2026 pagina 14 t/m 15) zijn wij verzocht de contact persoon (zoals vermeld onder de auteurgegevens) te wijzigen in "Clare Loveridge, Vice President & General Manager EMEA bij Arctic Wolf, die bereikbaar is onder het e-mail adres: clare.loveridge@arcticwolf.com".

IN DIT NUMMER

Auteur: Merijn de Jonge is oprichter en CEO van MindYourPass.
Hij is bereikbaar via: merijn.de.jonge@mindyourpass.com

Eigen digitale hygiëne

een worsteling, zelfs voor security-professionals

We hebben in cybersecurity de neiging om steeds verder omhoog te kijken: naar beleidskaders, nieuwe authenticatiemiddelen en architecturen die het werkveld moeten moderniseren. Maar als je de onderzoeken erop naslaat, blijft het probleem vrijwel hetzelfde. De meeste incidenten beginnen nog steeds bij iets wat iedereen kent en waarvan iedereen weet dat het mis kan gaan: accounts en wachtwoorden. Het is de basishygiëne die al jaren onderwerp is van rapporten en die in werkelijkheid nauwelijks verbetert.

Security-specialisten weten dit natuurlijk als geen ander. Maar zelfs binnen security-teams is het beheer van accounts en wachtwoorden vaak minder op orde dan we hardop durven toe te geven. Niet omdat professionals zich niet bewust zijn van de risico's, maar omdat de hoeveelheid digitale identiteiten niet meer te overzien is en het onderhoud ervan volledig bij individuen is komen te liggen. Het is een bekend spanningsveld: je weet precies wat verstandig is, maar je doet het zelf lang niet altijd.

In dit artikel kijk ik daarom niet naar gebruikers of naar organisaties, maar naar onszelf. Wat zegt het over ons vakgebied dat zelfs vakgenoten moeite hebben met hun eigen digitale hygiëne? Wat zegt het over de techniek die we bouwen, de verwachtingen die we scheppen en het gedrag dat we van anderen verlangen? En vooral: wat kunnen we leren door weer eens bij de basis te beginnen.

De onoverzienbaarheid van digitale identiteiten

Wie zijn eigen digitale 'leven' in kaart probeert te brengen, wordt al snel overdonderd door de grote hoeveelheid accounts die hij of zij in de jaren heeft opgebouwd. Zelf heb ik bijvoorbeeld 402 accounts in mijn wachtwoordmanager staan. De gemiddelde professional heeft tientallen tot honderden accounts, verspreid over werk, privé, oude hobby's, vergeten diensten en tools die ooit één keer nodig waren. Dat aantal groeit gestaag door, zonder dat er ooit een moment van opschoning tegenover staat.

Er ontstaat daarmee een situatie die moeilijk te verenigen is met het idee van persoonlijke verantwoordelijkheid. Van iedereen vragen dat hij of zij tientallen of honderden wachtwoorden uniek, sterk en up-to-date houdt, klinkt redelijk zolang je het abstract bekijkt. Maar zodra je de werkelijke aantallen ziet, wordt duidelijk dat het nauwelijks werkbaar is. Dat geldt voor collega's die weten wat de risico's zijn en al helemaal voor eindgebruikers die weinig affiniteit hebben met beveiliging. Kennis blijkt in de praktijk dus geen garantie voor consistent gedrag.

De vraag is niet of iemand zorgvuldig met die identiteiten om wil gaan, maar of het überhaupt mogelijk is om dat te doen. Het antwoord daarop is: "Nauwelijks", terwijl daar wel veel risico's liggen.

Wat waren ook alweer de risico's?

We kennen allemaal de bekende rapporten: 'Data Breach Investigations Report' van Verizon; Microsoft 'Digital Defense Report'; CrowdStrike 'Threat Report'; ENISA 'Threat Landscape'; en de 'Cost of a Data Breach Report' van IBM. Allemaal zeggen ze hetzelfde: aanvallers beginnen zelden met complexe technische aanvallen. Ze beginnen met iets eenvoudigs: gestolen wachtwoorden.

Zodra een wachtwoord ergens is uitgelekt, vindt het snel zijn weg naar de 'dark web' waar aanvallers het kunnen kopen. Met geautomatiseerde scripts worden de combinaties van e-mailadressen en wachtwoorden uitgeprobeerd op andere - belangrijkere - diensten. Het hergebruiken van wachtwoorden zorgt er dus voor dat één lek direct kan leiden tot toegang op meerdere plekken.

Ondanks verwoede pogingen om deze risico's in te dammen, groeit het probleem. In het laatste Microsoft Digital Defense Report staat dat in de eerste helft van 2025 het aantal 'identity-based attacks' met 32% toenam. De reden hiervoor is AI. Criminelen ruiken hun kans schoon, want met AI kunnen ze inlogpogingen steeds overtuigender nabootsen. Signalen zoals timing, apparaatprofiel en locatie helpen dan minder goed om verdachte activiteiten te herkennen.

Het risico blijft dus onverminderd groot, en we weten ook allemaal wat de financiële gevolgen kunnen zijn van een geslaagde cyberaanval; we gebruiken deze getallen immers allemaal om cybersecurity hoger op de agenda van de board te krijgen.

Maar toch voelt het alsof we de struisvogeltactiek toepassen. "We hebben een wachtwoordmanager / SSO / MFA /... dus dit probleem hebben we afgedekt," wordt vaak gezegd. Maar is het probleem daarmee wel echt opgelost?

Wat zijn ook alweer de oplossingen?

Wachtwoordtrainingen

De klassieke oplossing: het personeel leren hoe ze goede wachtwoorden bedenken. Er wordt uitgelegd waarom het belangrijk is een sterk wachtwoord te kiezen; dat "admin" of "welkom123" beter niet gekozen kan worden; en hoe je wél een sterk wachtwoord kan bedenken en onthouden.

En die trainingen werken ook: mensen bedenken na zo'n training aantoonbaar betere wachtwoorden (1). Of vooral: één aantoonbaar beter wachtwoord, en die wordt daarna overal gebruikt. Dan ben je dus nog steeds niet van het probleem af.

Wachtwoordmanager

Omdat mensen dus niet zoveel wachtwoorden kunnen bedenken en onthouden werd de wachtwoordmanager uitgevonden. Daarvan is het idee: laat de software sterke wachtwoorden genereren, bewaar ze veilig, vul ze automatisch in en voorkom zo dat één wachtwoord zich als een olievlek verspreidt over tientallen accounts. Voor veel professionals voelt het als het enige werkbare middel om het groeiende aantal accounts te beheren.

Alleen en dit weten we onbewust allemaal: niemand gebruikt de wachtwoordmanager, op een enkeling met veel zelfdiscipline na. En dus zijn we terug bij af.

SSO & MFA

SSO (Single Sign-On) en MFA (Multi-Factor Authenticatie) worden vaak genoemd als het antwoord op dit probleem. En in theorie klopt dat ook. Door gebruikers minder wachtwoorden te laten beheren en elke inlog te koppelen aan een extra verificatiestap, verklein je de afhankelijkheid van individuele credentials.

Veel organisaties zien hierin een manier om het risico beter te beheersen: één centraal account (SSO), minder wachtwoordgedoe en een extra laag controle (MFA). Op papier levert dat overzicht op en vermindert het de kans dat gestolen wachtwoorden direct bruikbaar zijn.

Voor de goede orde: voor veel applicaties werkt dit (bijna) perfect. Namelijk de apps die deze mogelijkheid van inloggen aanbieden.

Nieuwe technologische oplossingen

Wat we in feite aan het bouwen zijn is een systeem met "n+1" oplossingen. Echter, het wordt voor eindgebruikers steeds lastiger om te doorzien via welk systeem ze bij welke applicaties moeten inloggen. En ook voor leveranciers wordt de "license to operate" steeds kostbaarder en tijdsintensiever. Naast wachtwoorden, moet je nu ook SSO, MFA, biometrisch, passkeys en andere vormen van inloggen ondersteunen. Dat is prima voor een enterprise, maar lastiger voor een webwinkel gespecialiseerd in modelauto's.

Professionals die IT goed begrijpen zullen hier weinig over nadenken, maar voor de gemiddelde medewerker wordt het al snel verwarrend. En zolang een groot deel van de industrie afhankelijk blijft van wachtwoorden, ontstaan er situaties waarin de techniek wel mogelijkheden biedt, maar niemand kan garanderen dat die mogelijkheden overal hetzelfde werken. Dat maakt de druk op het individu groter dan redelijk is.

Dat is lastig voor security professionals, want ook al zijn veel van ons zich bewust van de risico's, ook wij hergebruiken soms hetzelfde wachtwoord en al helemaal voor Henk van boekhouding. We lijken vaak te vergeten dat security niet hun werk is. Dus ja, we kunnen ze vertellen over de risico's, maar het is lastig om alles te onthouden.

Inloggen bij Topdesk om een factuur te downloaden... Hoe ging dat ook alweer? Ah ja, het wachtwoord staat in de wachtwoordkluis. Hoe kwam ik daar ook alweer? Hmm... Wachtwoord werkt niet. Herstel wachtwoord. Recovery code? Wat was dat nou ook alweer? Weet je wat: ik reset het wachtwoord wel gewoon. Nieuw wachtwoord: Mijn-kat-luna21.

Wachtwoorden blijven er voorlopig nog

Het echte probleem is dus: er is géén uniform systeem dat op dit moment wachtwoorden op grote schaal kan vervangen. En zelfs, als dat er wel was, dan gaat het nog steeds om ongelofelijk veel aanpassingen die gedaan moeten worden.

Op dit moment zitten er in Nederland 275.000 websites in de database van MindYourPass. Dat betekent dat daarop ingelogd kan worden met wachtwoorden. Op passkeys.com (2) staat nu een lijst van 173 websites die passkeys ondersteunen - wereldwijd. Waarschijnlijk is dat een onderschatting en is de werkelijke lijst langer, maar zelfs met een factor 10 hebben we het nog steeds over een fractie van de websites.

Kortom, als we helemaal van wachtwoorden af willen, dan is dat net zo impactvol als wanneer we alle huizen in Nederland van het gas af zouden willen halen.

Is dat een probleem?

Dat we voorlopig dus nog niet van wachtwoorden af zijn, hoeft op zichzelf geen probleem te zijn. Het principe is eenvoudig: een geheim dat alleen jij kent geeft je toegang tot een account. Dat concept is al tientallen jaren hetzelfde en werkt in de basis nog steeds. Sterker nog, een uniek en lang wachtwoord blijft een van de meest betrouwbare manieren om een identiteit te beschermen, zolang het geheim ook echt geheim blijft. Het probleem zit dus niet in het idee van een wachtwoord, maar in de manier waarop we er in de praktijk mee moeten omgaan: niet één wachtwoord, maar tientallen tot honderden.

Welke verantwoordelijkheid voor ons vakgebied?

Dan blijft de vraag waar dit ons brengt, wat zegt dit alles over ons vakgebied zelf? Dat de mens een belangrijke, zo niet de belangrijkste, factor blijft in het toepassen van techniek. En dat de oplossingen die wij als sector graag noemen nog vooral toekomstmuziek zijn, terwijl de risico's, zoals Microsoft laat zien, nu spelen.

En als we, als security experts, eerlijk zijn naar onszelf toe dan weten we al jaren dat wachtwoorden kwetsbaar zijn; dat gebruikers moeite hebben met digitale hygiëne; en dat training en nieuwe technieken géén structurele veranderingen brengen. We gedragen ons wel zo. In security doen we vaak alsof eindgebruikers irrationeel zijn, terwijl we eigenlijk van hen irrationele dingen vragen.

Hackers zijn de lachende derde. Ze hoeven alleen gebruik te maken van de zwakste plek die al jaren hetzelfde is: gestolen of hergebruikte wachtwoorden, vaak gekoppeld aan accounts die nooit meer zijn opgeruimd.

Daarom is het te makkelijk om te zeggen dat mensen het probleem zijn. Zolang wachtwoorden bestaan, ligt het werk vooral bij ons: mensen ontlasten, inzicht geven, veilige keuzes standaard maken en zo min mogelijk overlaten aan individuele discipline. Niet door te hopen dat iedereen zich perfect aan beleid houdt, maar door toe te geven dat het systeem nog niet aansluit op hoe mensen in de praktijk werken.

Dat levert geen heroïsche eindconclusie op, maar wel een eerlijke:

1. alles rondom het inloggen door de gebruiker moet eenduidiger van aard en daardoor minder foutgevoelig worden.
2. maak het voor tooling gemakkelijker om inlog-procedures adequaat te ondersteunen.

Referenties

(1) https://mindyourpass.io/nl/artikelen/mindyourpass-gemeenten-benchmark-2024-hoe-veilig-zijn-de-wachtwoorden

(2) http://passkeys.com

COLUMN LEX

De onzichtbare legacy-dreiging

De moderne system administrator is opgegroeid met Microsoft 365, cloud-identiteiten, conditional access en zero-trust. Authenticatie draait om Kerberos, OAuth, SAML of tokens. Er is echter nog een authenticatieprotocol uit een 'ver verleden' dat vrijwel in elke omgeving nog steeds aanwezig is. In cyberaanvallen kan ervoor gezorgd worden dat dit gebruikt wordt, en dat gebeurt zonder dat iemand het merkt.

Het draait hier om NTLM, dat is hét authenticatieprotocol van Microsoft uit de jaren negentig. Het was ontworpen voor kleine, relatief veilige netwerken. Inmiddels is het protocol structureel zwakker dan moderne alternatieven en wordt het regelmatig misbruikt in cyberaanvallen en kan gezien worden als structurele kwetsbaarheid.

NTLM ondersteunt geen sterke wederzijdse authenticatie en is gevoelig voor bekende aanvalstechnieken, zoals: relay-aanvallen en pass-the-hash. Dat betekent dat een aanvaller, zodra hij toegang heeft tot één systeem, NTLM kan gebruiken om zich verder te verspreiden. In ransomware-incidenten speelt NTLM regelmatig een rol bij laterale beweging tussen systemen, escalatie van privileges en toegang tot kritieke servers.

Microsoft verving NTLM door Kerberos bij de introductie van Active Directory in Windows 2000. Kerberos bood sterkere cryptografie, betere schaalbaarheid en ondersteuning voor gedistribueerde netwerken, met meerdere domeinen en trusts. Kerberos was al een open standaard en maakte veiligere, efficiënte en beter beheersbare enterprise-authenticatie mogelijk. Kerberos werd al gebruikt in Unix-netwerken en zelfs op sommige mainframes.

Vervolgens verdween NTLM langzaam uit beeld – in de praktijk en in opleidingen. Als je met moderne omgevingen werkt, kom je NTLM nauwelijks tegen. Dat komt omdat Kerberos nu al 25+ jaar de standaard is in Active Directory; cloud-omgevingen gebruiken NTLM niet en nieuwe systemen en certificeringen focussen op moderne authenticatie.

Het probleem is dat NTLM nog wel onzichtbaar actief is. Het wordt automatisch gebruikt als fallback, wanneer Kerberos niet werkt. Daardoor kan een omgeving er jarenlang gebruik van maken zonder dat iemand het merkt. NTLM duikt alleen op in erfgoed: legacy-applicaties, oude servers en apparaten, systemen die niet domain-joined zijn en in scripts via hun IP-adres worden benaderd.

Microsoft neemt zijn tijd om NTLM weg te werken. Ze hebben aangekondigd dat NTLM in 'de toekomst' standaard wordt uitgeschakeld in Windows. Dat betekent dat die onzichtbare afhankelijkheden zichtbaar gaan worden. Dat zal vooral zijn bij een update, migratie of implementatie van een nieuwe techniek. Dan moet de organisatie onder tijdsdruk beslissen hoe deze afhankelijkheden opgelost moeten worden. Ondertussen kunnen hackers nog steeds NTLM blijven misbruiken.

Het is dus belangrijk dat je zicht hebt op het verborgen NTLM-gebruik. Heb je dat niet, dan loop je het risico op storingen, legacy-systemen die plots niet meer werken en extra werkdruk door spoedoplossingen die aangebracht moeten worden. Begin met NTLM-auditing aan te zetten op je domain controllers. In vrijwel elke organisatie waar auditing wordt ingeschakeld, blijkt NTLM nog ergens actief te zijn. Vaak op plekken waar niemand het verwacht. Analyseer vervolgens de bronnen van het NTLM-verkeer. Dat zijn de systemen die aangepakt moeten worden.

NTLM is geen acuut probleem dat morgen alles platlegt, maar wel een verzwakking van je security-fundament. Door er nu inzicht in te krijgen en het gefaseerd af te bouwen, voorkom je zowel security-risico's als toekomstige operationele verrassingen.

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

Auteurs: Rob Mellegers, Executive Director bij Securance.
Bereikbaar via: rob.mellegers@securance.com

Inzicht door meten van wachtwoordkwaliteit

Het traditionele wachtwoord is nog steeds een zwakke schakel in digitale beveiliging. Een groot deel van de cyberaanvallen, die succesvol zijn, starten met het verkrijgen van een wachtwoord door een hacker. Gelukkig komen er steeds meer alternatieven voor of uitbreidingen op wachtwoorden om in te loggen, die veiliger en gebruiksvriendelijker zijn dan het bedenken en onthouden van complexe wachtwoorden. Ook zijn er meer wachtwoordkluizen die een complexe string kunnen genereren en opslaan.

Hoe stel je echter vast dat gebruikers in alle gevallen een kwalitatief goed wachtwoord gebruiken dan wel tools en middelen, die beschikbaar zijn, ook daadwerkelijk gebruiken? En als je dat goed kunt controleren, wat ga je vervolgens doen om het risico van misbruik van een slecht wachtwoord te voorkomen? In de afgelopen 5 jaar is op regelmatige basis en op verschillende klantlocaties het gebruik van wachtwoorden gemeten en is onderzocht of alternatieve oplossingen inderdaad leiden tot goed wachtwoordgebruik.

Tijdens de afgelopen controles werd geconstateerd dat er wachtwoordkluizen tot beschikking stonden alsook andere alternatieven zoals: Passkeys, biometrische authenticatie, Multi-Factor Authenticatie (MFA), SSO en op hardware gebaseerde authenticatie.

Echter, bij deze eerste meting werd eveneens vastgesteld dat minder dan 2% van de respondenten geen wachtwoordkluis gebruikten, terwijl die wel beschikbaar werd gesteld door de organisatie. Enerzijds omdat gebruikers het lastig vonden om het in te richten, anderzijds omdat ze het lastig vonden om het wachtwoord vanuit de kluis op te halen. Daarbij tevens vaststellende dat vanuit die werkplekken meer dan 900 clouddiensten werden aangesproken, daarbij een zwak wachtwoord gebruikende om zich te authentiseren. In meer dan 80% van die gevallen werd ook geen MFA toegepast.

Door toepassing van verschillende meettechnieken is het mogelijk om inzicht te krijgen in het risico voor de organisatie. De metingen kunnen informatie geven over de lengte van het wachtwoord of het wachtwoord al eens eerder is gebruikt of gestolen of dat het wachtwoord niet uniek is dan wel onderdeel uitmaakt van een zogenaamde Dictionary (woordenboek). Een versleutelde versie van het wachtwoord is dan opgenomen in een zogenaamd woordenboek. Als de versleutelde variant overeenkomt met die uit het woordenboek, dan is het oorspronkelijke wachtwoord ook hetzelfde.

Meten van wachtwoordkwaliteit is geen controle, maar behoort onderdeel te zijn van het risicomanagementproces

Van Technisch meten naar bestuurlijk inzicht

Voor CISO's is het meten van wachtwoordkwaliteit pas waardevol wanneer de uitkomsten vertaald kunnen worden naar concrete risico's, bestuurlijke keuzes en aantoonbare verbetering. Denk daarbij aan tools als Hashcat, John the Ripper, Mindyourpass of zxcvbn voor het meten van wachtwoorden uit webapplicaties. In de praktijk zien we dat veel organisaties blijven hangen in beleid en bewustwording, terwijl objectieve metingen aantonen dat structurele zwakheden blijven bestaan, omdat de bestuurlijke keuzes niet gemaakt worden.

Een bezwaar dat vaak wordt aangevoerd met betrekking tot het meten van wachtwoorden is dat het voelt als controle op medewerkers. In werkelijkheid is het tegendeel waar: het doel van meten is het kwantificeren van organisatierisico. Net zoals een kwetsbaarheidsscan of een configuratie-audit geen oordeel geeft over technisch of functioneel beheerders, zegt een wachtwoordmeting ook niets over een individuele gebruiker. Een zwak wachtwoord is op zichzelf geen incident, maar vergroot de kans op misbruik. Door wachtwoordkwaliteit te combineren met risicobeoordeling - van: hergebruik, het mogelijk negeren van bekende datalekken en daarnaast het belang van de achterliggende applicatie (en 'assets') - ontstaat een volwassen risicomodel. Hiermee kan een organisatie prioriteren; niet elk zwak wachtwoord is even kritisch.

De rol van cloud en identiteitsfederatie

De sterke groei van cloudapplicaties vergroot het probleem exponentieel. Waar organisaties traditioneel zicht hadden op een beperkt aantal interne applicaties, zien we nu honderden en in sommige gevallen duizenden externe SaaS-diensten. Zonder centrale meting ontstaat schijnveiligheid: beleid is formeel op orde, echter feitelijk niet afdwingbaar.

Uit meerdere meetmomenten blijkt dat awareness campagnes slechts tijdelijk effect hebben. Gebruikers vervallen na verloop van tijd terug in oud gedrag, zeker wanneer gebruiksgemak belangrijker wordt dan abstracte dreigingen. Structurele verbetering vraagt daarom om technische borging, niet enkel en alleen gedragsbeïnvloeding.

Een toekomst zonder wachtwoorden?

Hoewel passwordless authenticatie sterk in opkomst is, zullen wachtwoorden de komende jaren nog niet volledig verdwijnen. Legacy-applicaties, federatieve koppelingen en externe leveranciers blijven afhankelijk van klassieke authenticatie. Juist daarom blijft het meten van wachtwoordkwaliteit relevant, ook in een passwordless strategie.

Conclusie:

Het structureel meten van wachtwoordkwaliteit biedt securityteams een krachtig instrument om abstracte dreigingen te vertalen naar meetbare risico's. Niet om gebruikers te corrigeren, maar om bestuurders, CISO's en auditors te voorzien van feitelijke stuurinformatie. Wie niet meet, stuurt op aannames en dus op kwetsbaarheid. Realisatie van dat vereist noodzakelijkerwijs een overzicht van alle entiteiten waar een wachtwoord wordt gebruikt als authenticatiemechanisme. Begin niet te groot en start bijvoorbeeld met webapplicaties en/of clouddiensten en plan daarna de rest van de keten in, zoals: werkplekken, netwerkcomponenten en data. Zorg dat daarbij een classificatiemodel zorgt voor de prioriteit van het te meten onderdeel.

Auteur: Xander Koppelmans is initiatiefnemer van het e-learning platform: MKB cybertraining.nl (https://kbcybertraining.nl/). Hij schrijft en spreekt vanuit eigen ervaring over een catastrofale hack en is bereikbaar via: info@xanderkoppelmans.nl

Van cybercrime en veiligheid heb ik geen verstand

Dat hoef ik ook niet, want dat is mijn vak niet.

Ik zit met mijn bedrijf in de communicatiesector of wat we vroeger een reclamebureau met foto- en filmstudio noemden. Zoals een bakker goed is in brood bakken en een timmerman in kozijnen zetten, is mijn specialisme het maken van mooie (foto)grafische communicatie en videoproductie. Samen met mijn team doe ik dat al meer dan 25 jaar en niet zonder succes. Bijna 1200 klanten waarvan 10 multinationals huren ons in en de resultaten liggen als verpakkingen in de schappen van de supermarkten en onze videoproducties zijn dagelijks te zien op TV. Daar ben ik echt trots op.

En zoals ik al zei, van automatisering heb ik veel minder verstand en van cybercriminaliteit al helemaal niet, bovendien is er in 25 jaar ondernemen op dat vlak nog nooit iets gebeurt. Blijkbaar doe ik het al goed!? Er zijn best veel dingen waar ik als ondernemer geen verstand of tijd voor heb zoals pensioenen, verzekeringen en de boekhouding. Die dingen besteed ik dan ook uit aan specialisten, "mijn mannetjes"; zo ook voor de automatisering en beveiliging.

Mijn eigen focus en primair doel als dienstverlenend bedrijf is maken van mooie dingen en die - in fijne samenwerking met mijn team en opdrachtgevers - netjes foutloos en op tijd te leveren. Daar is mijn automatisering ook primair op ingericht. Snelle servers en computers, goed internet en geen zandlopertjes in beeld; inloggen en gaan zonder haperingen! Een ander doel is om iedereen binnen mijn team in een goede sfeer en met een lach op het gezicht hun werk te kunnen laten doen, want die lach, die liefde, die vind je terug in de kwaliteit van het geleverde werk.

Wij creëren met al die foto- en videobestanden enorme hoeveelheden unieke data die goed gemanaged moet worden. Dus wij hebben meerdere servers (in de afgesloten brandveilige serverruimte) met RAID-geschakelde disks en daarachter nog back-up servers die 24/7 kopieën draaien van ons "onderhanden werk". Eenmaal voltooide projecten gaan van de servers af op losse harddisks. Van elk project weer 2 kopieën (ons archief) om te voorkomen dat er kostbare data verloren gaat als er een harddisk valt.
Voor de computers en hardware hebben we al jaren een vaste leverancier en daarnaast heb ik een systeembeheerder in Amsterdam die de boel onderhoudt en update, mijn "mannetjes" zogezegd.

Beveiliging hoort daar natuurlijk ook bij, dus ja we hebben een firewall, antivirussoftware en allemaal onze eigen unieke wachtwoorden om in te loggen en die wisselen elke maand … wat een hel. Ik kan in mijn eigen bedrijf alleen op mijn eigen PC werken, omdat ik simpelweg de wachtwoorden van de andere stations niet weet. Maar ja, als ik het als eigenaar al niet weet, dan is dat vast wel heel veilig…

De Hack

Dan worden we op een donderdagmorgen om half elf in de ochtend toch gehackt!

Onze systeembeheerder had de dag ervoor gebeld dat onze servers een beetje vol liepen en hij vroeg of er wat bestanden overgezet konden worden naar het losse harddiskarchief. De volgende morgen meteen iemand erop gezet en die kwam tot de vreemde ontdekking dat 2 van de servers niet vol maar juist bijna leeg waren, geen bestanden meer. Toen we samen keken zagen we de bestanden van de andere 2 servers verdwijnen. Meteen systeembeheer gebeld om te vragen of zij zelf misschien al dingen aan het verzetten waren maar het antwoord was nee, dit doet iemand anders, iemand van buitenaf, jullie worden gehackt!

Heel eerlijk? Ik moest eerst lachen en kon het niet geloven. Wij gehackt? Een bureautje op een industrieterrein in de Zeeuwse periferie? Hoe dan, wie dan, waarom dan?

Meteen daarna in de actiemodus gesprongen en zonder overleg meteen de stekkers uit al de servers getrokken en de boel stil gelegd onder het motto: "Dit moet nu stoppen!" Die middag heb ik het team vrijaf gegeven en de volgende morgen kwam de systeembeheerder om de back-ups terug te zetten om vervolgens tot de ontdekking te komen dat de back-ups ook verdwenen waren. Met 90 lopende orders en deadlines was er ineens nagenoeg niets meer terug te vinden, 80% van alle bestanden weg. Geen werk, geen planning, geen telefonie, geen mail het bedrijf was digitaal van de aardbodem verdwenen.

We zijn vervolgens met onze mobieltjes klanten gaan bellen om te zeggen wat er gebeurd was en dat de leveringen vertraagd zijn. Niet iedereen was blij of begripvol om dat te horen, als ketenpartner ontwricht je direct ook de workflow van iedereen voor én achter je.

Wat was er gebeurd?

Onze servers zijn ook van buitenaf te benaderen voor de

Dan stopt alles en kijkt iedereen naar jou. Wat ga je doen, hoe ga je deze crisis oplossen?

mensen die vanuit huis werken maar ook de freelancers (tekstschrijvers, fotografen e.d.) en klanten die bestanden willen uploaden.

Onze servers blijken via die ingang te zijn aangevallen door een bruteforce-aanval. In essentie proberen de hackers dan in te loggen op je server door domweg wachtwoorden te proberen. Eerst de meest voor de hand liggende wachtwoorden zoals 1234567, QWERTY en Welkom01! Daarna met werkelijk vele andere wachtwoorden.

Je kan op mijn servers maar 3x inloggen en als dat 3 maal fout is, dan word je automatisch voor een tijdje geblokkeerd. Maar die inlogpogingen gaan geautomatiseerd en wel met duizenden pogingen per seconde en deze inlogpogingen komen steeds van andere gestolen of gehackte adressen. In de logbestanden vinden we inlogpogingen van kinderdagverblijven, pannenkoekenhuizen, scholen, werkelijk van alles! En alle inloggers mogen het 3x proberen. Vroeg of laat en in mijn geval na 4,5 uur, vinden ze het juiste wachtwoord en zijn ze binnen.

Daarna zijn ze met een automatisch script alle bestanden van alle systemen gaan verwijderen en dat zagen wij dus live gebeuren. Waarom? Je kan het ze niet vragen. Wij hebben de stekkers eruit getrokken dus misschien was het te doen om ransomware of zo, maar dat zullen we mede door het stekker-trekken nooit weten.

Kosten

Als ondernemer dacht ik direct "Oei dit gaat geld kosten. Deadlines gemist, klant gaat daarom niet betalen, systeembeheer gaat een hoop uren maken en ik lig stil en verlies productie-uren. De directe schade was al snel 250.000 euro en die is niet verzekerd. Maar daar bleef het niet bij.
Sommige projecten lopen soms wel jarenlang, zoals de aanleg van snelwegen en spoorwegtracés, waar wij de registratie van verzorgen maar ook de opbouw van beeldbanken. Daar zijn nog geen offline archief back-ups van, want dat is nog steeds "onderhanden werk". Niet handig.
Dat werk kan je niet meer opnieuw reconstrueren, die snelweg ligt er inmiddels al. Veel ander werk kan wel opnieuw gemaakt worden dus nadat de systemen weer opgestart zijn gaan we vol gas, maandenlang opnieuw maken wat weg is. Nieuwe foto's maken, modellen en locaties opnieuw inhuren, advertenties en brochures opnieuw opbouwen. Na 4 maanden boek ik wederom een schadepost van 250.000 euro aan dubbel werk, wat niet nog eens betaald gaat worden.

Als ondernemer ben je een deel van je eigen team

Gewoonlijk zat ik hele dagen op de weg om opdrachten bij klanten op te halen en door te spreken. In de studio realiseert je team op basis van jouw briefings de mooiste producten, die je dan later met veel plezier en trots gaat presenteren. Maar niet als je gehackt bent.

Dan stopt alles en kijkt iedereen naar jou. Wat ga je doen, hoe ga je deze crisis oplossen? Jouw relaties, jouw team, iedereen heeft vragen waar jij zo snel geen antwoorden op hebt en jouw eigen specialisten-netwerk weet het ook niet. Jouw accountant, IT-partner en Arbodienst kan je daarbij niet helpen. Dit is immers niemands vak, niemands expertise, hier ben je nog nooit geweest en crisismanagement op deze schaal heb je in 25 jaar nog nooit hoeven doen. Hoe snel krijg je het werk toch bij de klanten, hoe stel je ze gerust, wat doe je met de automatisering om incidenten in de toekomst te voorkomen, hoe breng je de sfeer terug in jouw team nu ze ook ineens boze telefoontjes krijgen van mensen die teleurgesteld zijn? Allemaal dingen die ten koste gaan van het normale dagelijkse werk en dus ook direct ten koste van acquisitie en omzet.

En niet in de laatste plaats, hoe blijf je zelf overeind in dit

geweld? Je staat er mee op en gaat er mee naar bed en werkt alle weekenden door om "het" weer goed te krijgen. Daar betaalt je lijf, je gemoedsrust maar ook jouw gezin een lelijke prijs voor. In mijn geval val ik na 10 maanden voor de 2e keer flauw bij het tankstation langs de snelweg en kom bij de huisarts vandaan met de diagnose burn-out. Ik eindig in bed met 3 maanden lang 18 uur per dag slapen. Tel die schade gerust op bij wat een hack je kost.

Gevolgschade

Kosten van eventueel losgeld, de IT en securitypartner, eventuele boetes (datalek) en de herbouw van bestanden begrijpt iedereen wel. Dat is te overzien en meestal nog net te betalen. Waar maar weinigen aan denken: ziekte en uitval van jezelf en jouw medewerkers, want die krijgen ook de volle laag en zijn hier - na een half jaar klachten en gedoe - niet langer meer tegen bestand. Ze worden bang, onzeker en jouw beste krachten komen na een jaar ellende aan jouw bureau staan met de mededeling: "Ik heb een andere baan!"

Waar ook niemand aan lijkt te denken is de zorg bij de klanten. Offerte-aanvragen en omzetten lopen hard terug bij een stijgende overhead. Niet in de laatste plaats, omdat de klanten jou veel minder zien, omdat je zo druk bent met het crisismanagement van de hack. De imagoschade die jouw onderneming oploopt is gigantisch en duurt meerdere jaren. En daar gaat je bedrijf uiteindelijk aan kapot.

The End

Anderhalf jaar na de hack telde ik al 1,5 miljoen niet verzekerde schade en dat was te veel voor mijn bedrijf. Zo heb ik 2 jaar na de hack, net als 60% van alle succesvol gehackte bedrijven, mijn eigen bedrijf moeten sluiten. Oprecht de slechtste periode van mijn leven. Mijn levenswerk verloren, mijn klanten in de problemen, mijn team werkloos, bedrijfspand en huis worden door de bank verkocht en mijn bestaansrecht als mens en ondernemer is heel ver te zoeken. En nee, het huwelijk van 18 jaar heeft het ook niet gehouden.

Nieuwe ronde, nieuwe kansen

Bijna iedereen vroeg me, je gaat jouw bedrijf toch wel opnieuw opstarten? Het antwoord moet nee zijn. Ik heb er de energie niet meer voor om weer een team samen te stellen en 25 jaar werk over te doen. Dit zit in jouw lijf en gaat er niet meer uit. Die periode is definitief voorbij. Ik ben lezingen gaan geven om ondernemers en instellingen te waarschuwen voor dit grote maatschappelijke gevaar en ik ben met een mooie groep topbedrijven MKB Cybertraining.nl gestart.

Een e-learning platform waar het MKB haar hele team voor heel weinig geld snel bewust en bekwaam maakt voor de grootste uitdaging waar we allemaal samen voor staan en waar we te weinig kennis van hebben. Ondernemend Nederland heeft echt hulp nodig, of je dat nou beseft of niet.

Hulp in de vorm van technische oplossingen die het veilig werken makkelijker maken, maar ook in de vorm van training en bewustwording van al onze medewerkers. Want die ene secretaresse of uitzendkracht die per ongeluk toch op die link klikt, gaat met schuldgevoel naar huis dat ze hun leven lang met zich meedragen.

Epiloog

Ik ben weer opgekrabbeld, ben gezond en uit de problemen, heb weer een huis en een fijn bedrijf. Maar het trauma blijft nog even.

Nu besef ik pas goed dat ik - en alles om mij heen - maximaal met internet verbonden is en is het eigenlijk een wonder dat ik niet eerder of vaker gehackt ben. Ik bezit mogelijk bij 150 bedrijven en websites over accounts met e-mailadressen en wachtwoorden! Alles in mijn bedrijf praat met internet! Van de deurbel tot de printer, van de slagboom tot de digitale weegschaal, die m'n secretaresse even van thuis meegenomen heeft. In onze onwetendheid denken we het goed te doen, echter hebben wij heel veel deuren wijd open staan. Waarom u nog niet gehackt bent? Nou vermoedelijk omdat hackers ook met personeelstekort kampen en niet omdat u het zo geweldig goed geregeld heeft.

Iemand vroeg mij laatst: "Als je nu moet aangeven hoe zwaar een brand, inbraak of een cyberaanval weegt, hoe zou je die dan waarderen?" Mijn antwoord was inbraak met een 3 (gewoon spul vervangen en de voordeur repareren), brand een 7 (meer gedoe en is meer ontwrichtend, maar net als inbraak ook verzekerd) en cyber een 11… maximaal ontwrichtend voor je bedrijf, jezelf, je team en alles daaromheen. Vreemd dat we ons dat onvoldoende beseffen. Er is werk te doen, doe het vandaag.

Auteur: Arnoud Bruinsma is oprichter van BSM Business Security Management BV. Daarnaast is hij meer dan 20 jaar actief in het werkveld van cybersecurity en cybercrime. Hij is bereikbaar via: a.bruinsma@bsm.nl

ClickFix: een opvallend effectieve aanvalstechniek

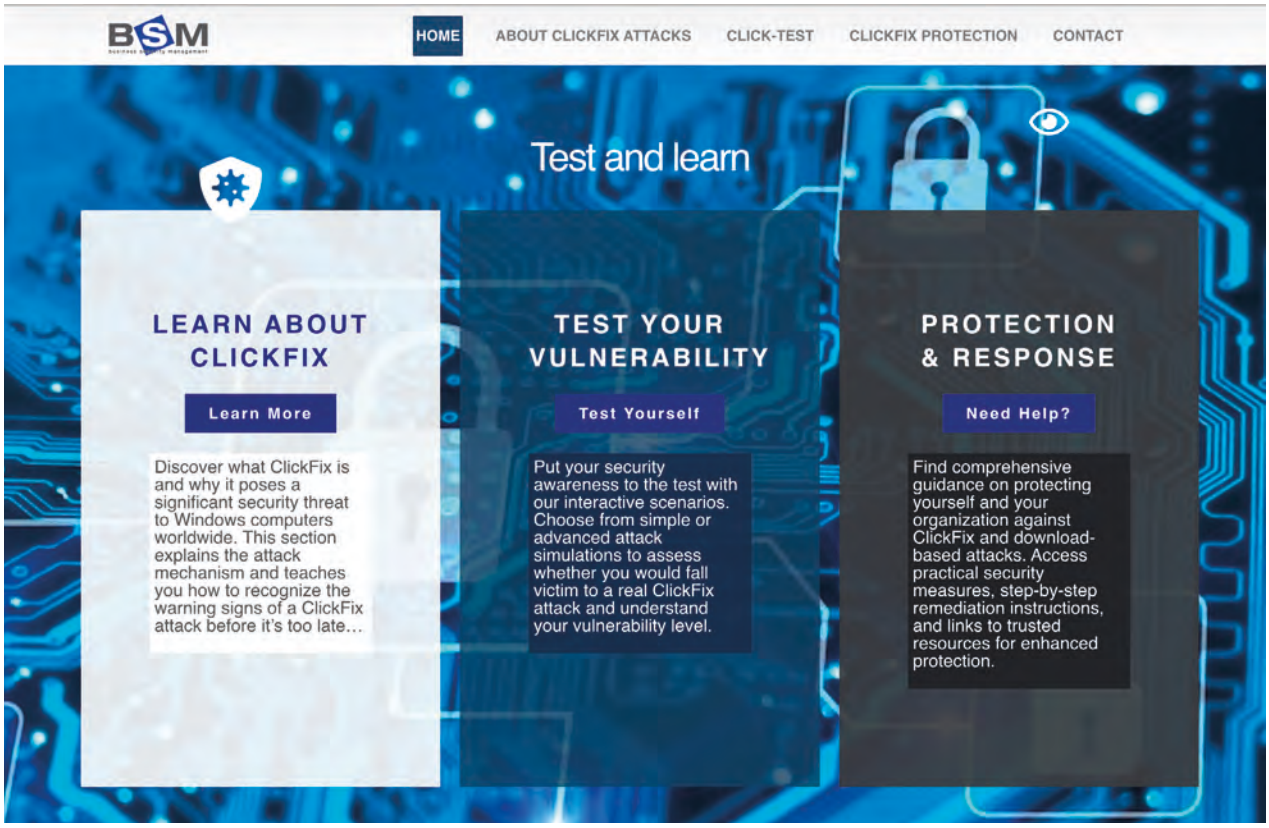
Sinds 2024 is een aanvalstechniek in opkomst die zich onderscheidt door eenvoud, effectiviteit en het vermogen om traditionele beveiligingsmaatregelen te omzeilen. Deze methode — bekend onder de naam ClickFix — maakt geen gebruik van zero-days of complexe exploits, maar combineert geraffineerde social engineering met legitieme systeemfunctionaliteit. In 2025 en 2026 is deze techniek verantwoordelijk voor een aanzienlijk aandeel in succesvolle malware-infecties wereldwijd.

In dit artikel wordt uiteengezet hoe ClickFix werkt, waarom bestaande beveiligingsmaatregelen vaak tekortschieten, hoe organisaties hun kwetsbaarheid kunnen testen en welke technische en organisatorische maatregelen de risico's kunnen beperken.

Social engineering als aanvalsvector

ClickFix-aanvallen creëren een geloofwaardige situatie waarin de gebruiker wordt verleid om zelf handelingen uit te voeren. Voorbeelden hiervan zijn: meldingen over vermeende browserupdates, foutmeldingen van ogenschijnlijk legitieme Microsoft- of Google-diensten, documentfouten die aanvullende stappen vereisen, nep-CAPTCHA-verificaties en beveiligingswaarschuwingen over een vermeend gecompromitteerd account. De verspreiding vindt vaak plaats via gecompromitteerde websites waarop de aanvalsketen is geplaatst, al wordt ClickFix regelmatig gecombineerd met phishing e-mails die de gebruiker naar zo'n pagina leiden.

De kern van de aanval bestaat uit één ogenschijnlijk onschuldige handeling: een klik op een webpagina of HTML-opgemaakte tekst. Omdat de gebruiker vervolgens zélf — onbedoeld — het script uitvoert, wordt veel werkplekbeveiliging eenvoudig omzeild. ClickFix maakt daarmee misbruik van een fundamentele zwakte in veel beveiligingsarchitecturen. Kenmerkend voor deze aanval is dat er geen exploit



Afbeelding 1: homepage click-fix.nl

wordt gebruikt en dat er geen softwarekwetsbaarheid wordt misbruikt. Een volledig lege Windows 11 laptop is voldoende om ClickFix-aanvallen te laten slagen.

ClickFix-aanvallen maken misbruik van legitieme systeemfunctionaliteit en gebruikersgedrag, waardoor traditionele beveiligingsmaatregelen vaak geen effectieve bescherming bieden.

De verschuiving is duidelijk: de aanval verplaatst zich van technische kwetsbaarheidsexploitatie naar gedragsmanipulatie. Dit deed zich eerder voor bij Adversary-in-the-Middle (AiTM)-phishingaanvallen. Het verschil is echter dat ClickFix niet alleen inloggegevens kan compromitteren, maar dat het potentieel direct volledige controle over de werkplek kan opleveren. Daarmee slaat de aanval meerdere traditionele stappen in de aanvalsketen over, zoals: exploitontwikkeling, privilege escalatie via kwetsbaarheden en klassieke malware-delivery. Dit maakt ClickFix risicovoller dan klassieke phishing, omdat één succesvolle interactie voldoende is om volledige controle over de werkplek te verkrijgen.

Gecontroleerd "spelen met virussen"

Om de werking van ClickFix beter te begrijpen, hebben wij onderzocht of we een ClickFix-aanval zelf konden nabootsen in een gecontroleerde testomgeving. Daarbij wilden we niet alleen het aanvalsscenario reproduceren, maar ook analyseren in hoeverre bestaande securitytooling dergelijke aanvallen detecteert of blokkeert.

Tijdens dit onderzoek ontstond het idee om een publieke testomgeving te ontwikkelen. Het resultaat is een voorbeeldwebsite die – vergelijkbaar met het bekende EICAR-testbestand voor antivirussoftware – gebruikt kan worden om ClickFix-scenario's veilig te simuleren.

De website stelt securityprofessionals en organisaties in staat om hun eigen werkplekken te testen en tegelijkertijd inzicht te krijgen in de werking van deze aanvalstechniek. Gebruikers kunnen het scenario in een gecontroleerde omgeving ervaren, waardoor zowel technische detectie als gebruikers-

Afbeelding 2: basic flow

bewustzijn kan worden geëvalueerd. Via https://click-fix.nl kan iedere organisatie haar eigen werkplekken eenvoudig testen.

De testscenario's

Via deze website wordt (momenteel in het Engels) uitgelegd hoe ClickFix werkt, welke tegenmaatregelen mogelijk zijn en als belangrijkste onderdeel drie verschillende testscenario's doorlopen. De meest eenvoudige test — de Basic Security Test — simuleert een eenvoudig maar effectief ClickFix-scenario. Hoewel de gemiddelde IT-professional deze aanval snel zal herkennen, blijkt dat veel reguliere Windows-gebruikers inmiddels gewend zijn geraakt aan het uitvoeren van ongebruikelijke handelingen, zoals CAPTCHA-verificaties. Waar men voorheen afbeeldingen van motoren of bruggen moest selecteren, wordt nu gevraagd bepaalde toetscombinaties uit te voeren. De essentie van de aanval is dat één klik op een webpagina ongemerkt een script naar het klembord kan kopiëren, zonder dat de gebruiker zich daarvan bewust is. Wanneer u na het uitvoeren van de Basic Security Test een pop-up ziet met de melding "Your PC is hackable", dan is uw werkplek technisch kwetsbaar voor dit type aanval en is het raadzaam aanvullende maatregelen te overwegen.
Naast de basistest — die uitsluitend een onschuldige pop-up toont — zijn ook een Advanced Test en een Download Test ontwikkeld. Deze varianten zijn eveneens ongevaarlijk, maar ingrijpender van opzet en testen aanvullende beveiligingslagen van de werkplek. Daarom is vooraf acceptatie van de gebruiksvoorwaarden vereist.

De Advanced Test demonstreert hoe - via een in PowerShell op de achtergrond gestreamd uitvoerbaar bestand - code kan worden uitgevoerd. In de testomgeving wordt vervolgens, als bewijs van een geslaagde aanval, de camera gestart en een foto gemaakt, die de computer niet verlaat, waarna de webpagina met de poll wordt geopend. De derde variant vereist dat de gebruiker zelf een bestand downloadt en uitvoert. Deze test biedt waardevolle inzichten voor securityprofessionals, zoals komen er downloadwaarschuwingen of niet? Hoe reageert de gebruiker op downloadwaarschuwingen? Op welk beveiligingsniveau (netwerk, browser, AV) wordt de test geblokkeerd? Is het mogelijk om een uitvoerbaar bestand uit te voeren vanuit de downloadmap?

Topje van de ijsberg

In onze praktijk als cybercrime-onderzoekers en operationeel securitytesters hebben wij de afgelopen maanden vastgesteld dat een groot deel van alle onderzochte werkplekken kwetsbaar zijn voor ClickFix. Daarnaast blijkt uit gesprekken met medewerkers, en met securityspecialisten, dat de kennis over deze aanvalsmethode beperkt is en dat het risico mogelijk structureel wordt onderschat. Een interessant aspect van ClickFix is dat deze aanval zich grotendeels onttrekt aan traditionele antivirusdetectie, omdat de gebruiker zelf – via legitieme functionaliteit – de aanval activeert. Daarmee wordt feitelijk een beveiligingsmechanisme omzeild zonder dat er direct sprake is van een klassieke exploit. Hoewel de techniek relatief nieuw lijkt, laat onderzoek zien dat ClickFix zich in korte tijd razendsnel heeft ontwikkeld en inmiddels ook wordt toegepast in grootschalige cybercrimecampagnes en zelfs in statelijke spionageoperaties. De onderstaande tijdslijn laat zien hoe snel deze aanvalsmethode zich heeft ontwikkeld:

Tijdslijn van ClickFix-aanvallen

Oktober 2023 — eerste waarnemingen
Onderzoekers signaleren vroege varianten van wat later ClickFix-achtige aanvallen worden genoemd. De techniek bestaat al, maar krijgt nog weinig aandacht.

Maart 2024 — naam "ClickFix" verschijnt
Securitybedrijf Proofpoint introduceert de term ClickFix, nadat de tactiek wordt waargenomen in phishingcampagnes van initial-access-broker TA571. In dezelfde periode observeert Microsoft de ClickFix-campagnes die zij volgen onder de aanduiding Storm-1607.

Mei 2024 — eerste grootschalige campagnes
Storm-1607 verstuurt tienduizenden phishingmails naar organisaties in de VS en Canada. De aanvallen leveren

onder andere DarkGate-malware af en tonen dat de methode op grote schaal inzetbaar is.

Oktober–november 2024 — adoptie door statelijke actoren
De techniek wordt ook gebruikt in spionagecampagnes. Onder meer statelijke actoren zoals APT28 (Rusland) en MuddyWater (Iran) passen ClickFix toe in gerichte phishing-operaties. Tegelijk verschijnen kant-en-klare builders op cybercrimefora.

Januari 2025 — Noord-Korea sluit aan
Onderzoekers detecteren dat Kimsuky (TA427) ClickFix gebruikt in spionagecampagnes. Daarmee wordt de techniek binnen korte tijd toegepast door meerdere statelijke actoren.

Eerste helft 2025 — sterke wereldwijde groei
Onderzoek van ESET laat zien dat het gebruik van ClickFix-achtige technieken met meer dan 500% is toegenomen. Nieuwe varianten verschijnen, waaronder macOS-gerichte campagnes en afgeleiden zoals FileFix.

ClickFix tegengaan

De voorgaande analyse laat zien hoe ClickFix-aanvallen misbruik maken van legitieme systeemfunctionaliteit en gebruikersgedrag. In dit afsluitende deel worden enkele praktische verdedigingsmaatregelen besproken.

De mens
Gebruikers leren in de praktijk doorgaans meer door te doen dan door te lezen. Wanneer een realistische doorloop of simulatie met een gebruiker wordt uitgevoerd, ontstaat er een veel duidelijker besef van het risico van bijvoorbeeld de Windows-R - toetscombinatie. Als deze toetscombinatie binnen de organisatie niet of nauwelijks wordt gebruikt, kan het risico in de basis al aanzienlijk worden beperkt. Bewustwording en gedragsverandering vormen daarmee een essentieel onderdeel van de verdediging tegen ClickFix.

De techniek
Het is belangrijk om te begrijpen dat gangbare digitale hygiënemaatregelen – zoals: het installeren van antivirus-software, het toepassen van MFA op alle accounts, het tijdig updaten van besturingssystemen en applicaties en het maken van back-ups – op zichzelf géén bescherming bieden tegen ClickFix. Maatregelen die wél effectief kunnen zijn, richten zich met name op het beperken van misbruik van legitieme systeemfunctionaliteit. Zo kan het uitschakelen van de Windows R toetscombinatie het risico aanzienlijk verkleinen, net als het blokkeren van het uitvoeren van scripts. Daarnaast kan het beperken of volledig blokkeren van PowerShell en opdrachtpromptgebruik bijdragen aan het verminderen van de aanvalsmogelijkheden. Ook het blokkeren van scriptuitvoer via e-mail kan een belangrijke rol spelen in het voorkomen van ClickFix-aanvallen.
Voor bescherming tegen geavanceerdere varianten kunnen aanvullende maatregelen worden overwogen. Daarbij valt te denken aan het toepassen van application whitelisting en het blokkeren van het uitvoeren van applicaties vanuit tijdelijke mappen of de downloadmap. Verder kan het ontwikkelen van detectiemechanismen voor het injecteren van kwaadaardige scripts in het klembord helpen om deze aanvallen eerder te herkennen en te stoppen. Ook kan onderzocht worden of het mogelijk is om het kopiëren van scripts naar het klembord te detecteren via eigen detectiescripts of – bij voorkeur – via endpoint-beveiligingssoftware die ClickFix als serieuze dreiging herkent en blokkeert.

Tot slot

Met de website click-fix.nl beschikt u over een praktische testomgeving om uzelf, uw organisatie en uw klanten te toetsen op kwetsbaarheid voor dit type aanval. Door de test zelf te ervaren wordt sneller duidelijk hoe eenvoudig gebruikers tot het uitvoeren van een kwaadaardig script kunnen worden verleid. Wij stellen het zeer op prijs als u na afloop van een test de poll op https://click-fix.nl/poll invult. De resultaten helpen ons om een beter beeld te krijgen van de werkelijke impact van ClickFix-achtige aanvallen en van de mate waarin bestaande beveiligingsmaatregelen deze technieken herkennen of blokkeren. Mocht u oplossingen tegenkomen die deze aanval wél detecteren of voorkomen, dan horen wij dat uiteraard graag. Op basis van de ervaringen en resultaten die de komende periode worden verzameld, hopen wij in een volgend artikel verder in te gaan op de effectiviteit van bestaande beveiligingsmaatregelen en mogelijke verbeteringen.

Referenties

Proofpoint – introductie en analyse van de ClickFix-techniek (TA571)
https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
Proofpoint – ClickFix verspreidt zich snel in phishingcampagnes
https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
Proofpoint – statelijke actoren gebruiken ClickFix (APT28, MuddyWater, Kimsuky)
https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix
ESET Threat Report – sterke wereldwijde groei van ClickFix-aanvallen
https://www.eset.com/us/business/threat-report/
Eicar testvirus: https://eicar.org

Auteurs: Erik Becker en Kees van der Maarel, zij zijn beleidsmedewerkers BIO2 bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Erik is te bereiken onder erik.becker@minbzk.nl

BIO2: een hoger IB volwassenheidsniveau voor de hele overheid

In september is de nieuwe Baseline Informatiebeveiliging Overheid (BIO2) vastgesteld in het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). De BIO2 is als normenkader hét informatiebeveiligingsfundament voor de overheid. In dit artikel lichten de makers van de BIO2 toe wat er verandert, hoe de BIO2 tot stand is gekomen, hoe de doorontwikkeling eruit zal zien, wat de BIO2 voor organisaties betekent en hoe deze zich verhoudt tot de aanstaande Cyberbeveiligingswet (Cbw).

Eén standaard voor de hele overheid

Waar voorheen iedere overheidslaag zijn eigen baseline had, is er sinds de komst van de BIO in 2018 één normenkader voor alle gemeenten, provincies, waterschappen en de Rijksoverheid. Het gebruik van één normenkader voor de gehele overheid kent een aantal voordelen; zo versterken we de informatiebeveiliging door betere afstemming binnen de ketens, verlichten we de administratielasten, sluiten we beter aan bij internationale regelgeving en verminderen we de onderhoudskosten.

Alle overheden zijn aan de hand van hun eigen implementatiepad aan de slag gegaan met de BIO. De wereld heeft echter sindsdien niet stilgestaan. Ontwikkelingen in nieuwe aanvalstechnieken, verdere professionalisering van de cybercrime industrie en voortdurende cyberaanvallen vanuit statelijke actoren, maken dat het noodzakelijk is om de informatiebeveiliging van overheden continu te verbeteren (1). Waar in het verleden veel aandacht uitging naar preventie hebben we nu detectie, response en herstel extra aandacht gegeven in de BIO2, om robuust en veerkrachtig incidenten en crises te lijf te gaan. Dit vereist een hoger volwassenheidsniveau; een gedegen managementsysteem (ISMS) om risicogedreven tot maatregelen te komen die passen bij de processen en dreigingen van de organisatie.

Daarnaast was de herziening van de BIO nodig in het kader van de Europese NIS2-richtlijn, die in Nederland wordt vertaald in de Cyberbeveiligingswet (Cbw). De BIO2 geeft straks als normenkader invulling aan de zorgplicht, één van de plichten van de Cbw die de sector overheid krijgt op het gebied van informatiebeveiliging.

Een risicogerichte focus

De BIO2 weerspiegelt de internationale beveiligingsnormen (NEN-EN-ISO 27001 en NEN-EN-ISO 27002) en we hebben de oude indeling met drie Basisbeveiligingsniveaus (BBN's) vervangen door een explicieter risicogerichte benadering. Hiermee kunnen overheidsinstanties maatregelen afstemmen op basis van specifieke risico's zonder vast te zitten aan drie vaste basisbeveiligingsniveaus.

Door de meer risicogerichte focus van de BIO2 konden we een aantal overheidsmaatregelen verlichten. Door de verplichte doorwerking van de NIS2-richtlijn op de BIO2 zijn ook een aantal overheidsmaatregelen verzwaard. Waar de beheersmaatregelen uit de ISO-standaard risicogebaseerd moeten worden toegepast, zijn overheidsorganisaties verplicht om de overheidsmaatregelen uit de BIO2 toe te passen om zo een basisniveau aan informatiebeveiliging te garanderen en samenwerking te bevorderen. Hiermee zijn organisaties er echter nog niet. Op basis van de risico's moeten uit de ISO27002 aanvullende maatregelen worden geselecteerd om de veiligheid te borgen. Hierbij kunnen organisaties zelf passende standaarden selecteren, denk bijvoorbeeld aan de Cybersecurity Implementatierichtlijn (CSIR) voor de beveiliging van Operationele Technologie (OT) of de NEN 7510 voor zorginformatie.

Community-gedreven aanpak

De ontwikkeling van BIO2 vond plaats binnen de BIO-werkgroep, een samenwerkingsverband waarin alle overheidslagen (gemeenten, provincies, waterschappen, uitvoeringsorganisaties en het Rijk) zijn vertegenwoordigd. De nieuwe BIO is het resultaat van het verwerken van de feedback uit een breed uitgezette evaluatie van de vorige BIO bij bestuurders en cybersecurityexperts (2), workshops met de CISO's van de vier overheidslagen, een mapping van de NIS2-eisen (3), brede afstemming in de BIO-werkgroep en een online internetconsultatie via GitHub. Binnen de werkgroep hebben we inhoudelijk overeenstemming bereikt over deze versie van de BIO2.

Met deze aanpak gaan wij verder richting de toekomst! Informatiebeveiliging is immers geen statische activiteit. Nieuwe inzichten rond dreigingen of ervaringsgegevens kunnen aanleiding geven tot aanpassing van en/of aanvulling op de BIO2. Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) zal de BIO2 samen met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de verschillende overheidslagen gaan beheren.

Uitgangspunten bij dit beheer zijn:

- Continuering van de community-gedreven ontwikkeling van de BIO2;
- Een twee-jaarcyclus die is afgestemd op de uitvoeringscyclus van organisaties die de BIO2 implementeren;
- Afstemming met diverse specialismen om wijzigingen te controleren op haalbaarheid en toetsbaarheid.

Zelfregulering en wettelijke verankering

In lijn met de acties onder de Nederlandse Cybersecurity Strategie (NLCS) gaan we de BIO2 opnemen in de verplichtingen die voortvloeien uit de Nederlandse vertaling van de Europese NIS2-richtlijn; de Cyberbeveiligingswet (Cbw). De BIO2 zal dienen als normenkader voor de zorgplicht die de sector overheid krijgt op het gebied van informatiebeveiliging. Het

hanteren van de BIO2 waarborgt een uniforme en gecoördineerde aanpak van cyberbeveiliging. De bekendheid van de BIO2 zorgt voor een 'zachtere landing' van de Cbw en lagere regelgeving bij de verschillende overheidsorganisaties.

Begin maart 2026 hebben we de BIO2 versie 1.3 gepubliceerd in de Staatscourant (4). In deze nieuwe versie zijn, vanwege de relatie met de ministeriële regeling voor de Cbw, nog beperkte aanpassingen gedaan om inconsistenties te verwijderen, verduidelijkingen toe te voegen en teksten meer in lijn te brengen met de Cbw. Ook zijn een drietal overheidsmaatregelen uitgezonderd van de Cbw verplichting, omdat deze niet binnen de scope van de wet vallen (die zich beperkt tot de beveiliging van netwerk- en informatiesystemen). De versie 1.3 vervangt de versie 1.2 die in het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) van 23 september 2025 is vastgesteld. De ministeriële regeling onder de Cbw zal voor de verplichting van de overheidsmaatregelen uit de BIO2 rechtstreeks verwijzen naar deze Staatscourantpublicatie.

Als onderdeel van deze wettelijke verankering dienen organisaties zich over hun naleving van de BIO2 te verantwoorden. De toezichthouders onder de Cbw zijn de **R**ijksinspectie **D**igitale **I**nfrastructuur (**RDI**) voor de gemeenten, provincies, gemeenschappelijke regelingen, de ZBO's en het Rijk; en de **I**nspectie **L**eefomgeving en **T**ransport (**ILT**) voor de waterschappen. Aanvullend zullen ook andere toezichthouders overstappen op de nieuwe BIO, voor gemeenten kun je bijvoorbeeld denken aan de **E**enduidige **N**ormatiek **S**ingle **I**nformation **A**udit (**ENSIA**)-verantwoording over **S**tructuur **u**itvoeringsorganisatie werk en **i**nkomen (**Suwinet**) en de Basisregistratie Persoonsgegevens. Een minstens even belangrijke verantwoording is die richting de eigen bestuurder. Onder de Cbw krijgen bestuurders duidelijkere verplichtingen op het gebied van informatiebeveiliging en het is belangrijk dat ze op de hoogte zijn van de risico's en welke stappen er ondernomen moeten worden om deze effectief te beheersen.

Vanaf de besluitvorming in het OBDO en tot de inwerkingtreding van de Cbw hanteren de provincies, waterschappen en het Rijk de BIO2 als verplichtende zelfregulering. De gemeenten gaan de BIO2 ook toepassen als richtinggevend kader, maar de BIO versie 1.04 blijft voor hen gelden als verplichtende zelfregulering tot de inwerkingtreding van de Cbw, in de loop van 2026. Voor de tussenliggende periode maken de betrokken partijen in samenwerkingssituaties afspraken over de implementatie van de BIO2. Hierin geldt dat de stem van de (hoofd)opdrachtgever bepalend is voor welke BIO versie leidend is.

De BIO2 blijft ook na de inwerkingtreding van de Cbw gelden als verplichtende zelfregulering voor overheidsorganisaties die niet onder de Cbw vallen. Dergelijke organisaties bij de Rijksdienst, zoals het Ministerie van Defensie en de AIVD blijven gebonden via een besluit dat via de Ministerraad is vastgesteld (5). Verplichtende zelfregulering blijft ook van kracht voor overheidsmaatregelen die buiten de scope van de Cbw vallen.

Aan de slag

Bij de implementatie van de BIO2 liggen er voor iedere organisatie uitdagingen die kosten en inspanningen met zich meebrengen. De steeds grotere afhankelijkheid van digitalisering en de toegenomen dreiging vanuit statelijke actoren maken het van groot belang dat deze uitdagingen worden opgepakt. De veranderende geopolitieke werkelijkheid laat de verschillende overheidsonderdelen helaas weinig ruimte voor aarzeling. We moeten nu een been bijtrekken om de basisveiligheid op orde te brengen en daar zal capaciteit voor vrijgemaakt moeten worden. Bestuurders zijn hierin eindverantwoordelijk. Zij moeten, samen met de CISO, de implementatie van de BIO2 uitvoeren.

Om organisaties te helpen deze stap te maken hebben wij het CIP gevraagd een implementatiebegeleidingscampagne te organiseren, deze is in september 2025 gestart. Iedere maand worden er verschillende activiteiten georganiseerd en handreikingen gedeeld die organisaties helpen de BIO2 te implementeren. Ook vanuit de verschillende koepelorganisaties is ondersteuning beschikbaar. Voor vragen kunt u terecht op de website van: bio-overheid.nl

Tot slot

Wij willen vanaf deze plaats nogmaals iedereen hartelijk bedanken die input heeft aangeleverd of op een andere manier betrokken is geweest bij de totstandkoming van de BIO2. We kijken uit naar een voortzetting van de goede samenwerking en wensen alle organisaties veel succes met de implementatie!

Referenties

(1) Zie bijvoorbeeld de **N**ederlandse **C**yberSecurityStrategie (**NLCS**) 2022-2028 en het **C**yberSecurity**B**eeld **N**ederland (**CSBN**) 2024

(2) https://www.rijksoverheid.nl/documenten/rapporten/2022/11/17/evaluatie-baseline-informatieveiligheid-overheid

(3) https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/mapping-nis2-maatregelen/

(4) Zie Staatscourant. 2026, 7416

(5) Zie Staatscourant. 2019, 26526.

COLUMN PRIVACY

Mr. Rachel Marbus

Oh jee, daar komt de AP

Wie een klein beetje het klappen van de zweep kent, weet dat elke organisatie van een beetje omvang op goed moment te maken krijgt met de privacytoezichthouder. Autoriteit Persoonsgegevens schrijft onder meer brieven. Dat deed zij onlangs nog over cookies en hoe dat beter moet worden ingericht. Ongeveer 300 organisaties in Nederland kregen dit schrijven op de mat. Zo nu en dan bellen ze naar de Functionaris Gegevensbescherming (FG) om opheldering te vragen over een gemeld datalek. En ja, het kan ook voorkomen dat er een officieel onderzoek wordt gestart omdat er iets mis lijkt te zijn met privacy. Dat is natuurlijk best even schrikken, en wat dan?

Het is een open deur van jewelste: raak vooral niet in paniek. Hou het hoofd koel. Vergis je niet, het is heel menselijk dat er paniek gevoeld wordt en in de praktijk zie ik dit bijna altijd gebeuren. Haal eerst even adem, doe een pas op de plaats. Bekijk wat AP precies van je wil, vaak zul je zien dat al op een informele manier wat informatie opgehaald wordt door de toezichthouder. Dan is een cruciale start ervoor te zorgen dat jouw privacyspecialisten, waaronder in ieder geval de FG, goed meegenomen worden en overal van op de hoogte zijn. Richt een intern onderzoek in om alle feiten boven tafel te krijgen, dat gaat je enorm helpen om eventuele vragen makkelijk en goed te kunnen beantwoorden.

Het kan natuurlijk gebeuren dat uit je eigen onderzoek al blijkt dat het toch niet helemaal goed is gegaan. Dan is je volgende stap om te zien wat je kunt doen om negatieve gevolgen voor de privacy van personen in te perken en als er verder onvolkomenheden geconstateerd zijn, schrijf op hoe je die gaat oplossen en maak een reële planning daarvoor. Het hebben van een goede analyse van de situatie en een plan van aanpak om eventueel gevonden issues op te lossen, maakt dat AP ziet dat je privacy serieus neemt en – niet geheel onbelangrijk – je helpt er jezelf mee en vooral ook de mensen die getroffen zijn door een inbreuk op hun privacy.

Helemaal ongeschonden zul je er wellicht niet uitkomen. Maar wie laat zien het juiste te willen doen, staat er direct wat beter op. Voorkomen is altijd beter natuurlijk, maar weet ook dat het soms niet altijd mogelijk is om een privacy-incident te voorkomen, hoe je daarna handelt zal cruciaal zijn. En vergeet niet, als alle stof weer neergedaald is, dat je even samen gaat zitten. Hebben we alles goed gedaan? Liep het proces met AP van onze kant gesmeerd? Wat hebben we geleerd hiervan? En, hoe kunnen we die geleerde lessen weer terug onze organisatie inbrengen?

En heel misschien zeg je dan een volgende keer niet 'Oh jee, daar komt de AP', maar 'Oh hey, daar heb je de AP!' – maar misschien is dat laatste wel wat veel gevraagd, want hoe dan ook, blijft het vaak toch een spannende aangelegenheid.

Rachel

Auteurs: M. (Marlou) Snelders (Digitalisering en Cybersecurity bij FME, de ondernemersorganisatie voor de technologische industrie) en P.T. (Paul) Borghouts (Extern Projectmanager, in opdracht van FME) en bereikbaar via e-mail: marlou.snelders@fme.nl of paul.borghouts@fme.nl

Het Digital Product Passport

• een kans voor transparantie en duurzaamheid
• een uitdaging voor cybersecurity

Je koopt een wasmachine. Met een simpele scan van de QR-code op het apparaat zie je meteen waar de onderdelen vandaan komen, hoe je dit apparaat het beste kunt onderhouden, en hoe je het aan het einde van zijn levensduur kunt recyclen. Dit is de belofte van het Digital Product Passport (DPP). Vanaf 2027 wordt het DPP per productgroep stapsgewijs ingevoerd via gedelegeerde handelingen als onderdeel van de Ecodesign for Sustainable Products Regulation (ESPR) binnen de European Green Deal. Het doel? Producten langer laten meegaan, reparatie en hergebruik stimuleren en de volledige levenscyclus transparanter maken.

Achter deze belofte schuilt echter een complexe realiteit. Want het DPP is geen simpel compliance vinkje, maar vraagt om fundamentele systeemverandering. Productdata moet digitaal, gestructureerd en langdurig beschikbaar zijn. In de praktijk gaat het hier om koppelingen met Enterprise Resource Planning (ERP),Product Lifecycle Management (PLM), Product Information Management (PIM), Mobile Device Management (MDM) en service-systemen. Voor bedrijven die nu nog grotendeels werken in Excel, is dit een enorme stap. Tegelijkertijd markeert het DPP een bredere verschuiving in Europees beleid. Waar regelgeving voorheen met name afzonderlijke domeinen adresseerde, zoals milieu, veiligheid of digitale veiligheid, verschuift de focus nu steeds meer naar de hele levenscyclus van het product zelf.

Een systeem in ontwikkeling

Het DPP moet uitgroeien tot betrouwbare bron van gestandaardiseerde productinformatie. Deze moet toegankelijk zijn voor consumenten, bedrijven en toezichthouders. Afhankelijk van de productgroep kan het gaan om informatie over materialen, herkomst, energieprestaties, onderhoud, certificeringen en recycling. Technisch gezien bestaat de architectuur uit een unieke identifier (zoals een QR-code), een verwijzing naar het EU-register (toegangspoort, portaal en identifier beheer), en decentrale dataopslag bij bedrijven of dienstverleners. De data blijft dus bij de bron, het EU-register verwijst ernaar.

Veel onderdelen van het DPP-stelsel zijn nog in ontwikkeling. Dit vormt een uitdaging voor implementatie. Denk aan datastructuren, opnamecriteria, rollenmodellen, beveiligingseisen en archiveringstermijnen. Daarnaast vergroot de veelheid van betrokken actoren: fabrikanten, importeurs, distributeurs, installatiebedrijven, machinebouwers, onderhoudspartijen, consumenten, markttoezichthouders, douane en recyclingbedrijven; de complexiteit. Het DPP moet functioneren in deze volledige keten en voldoen aan uiteenlopende eisen. Zonder duidelijke governance over eigenaarschap van het centrale register, verantwoordelijkheden bij downtime, escalatie en herstelroutes bij verstoringen alsook transparante besluitvorming over technische updates, standaarden en migraties; bestaat het risico dat bedrijven afhankelijk worden van een centrale EU-infrastructuur waarvan de operationele continuïteit en capaciteit niet voorspelbaar is. Zodat in het slechtste geval de markttoegang in gevaar komt. Zo dreigt het DPP een kostbaar en risicovol verplichtingssysteem te worden, in plaats van een instrument dat duurzaamheid en concurrentiekracht stimuleert.

Wildgroei en ketendoorwerking

In de praktijk ontstaat al een wildgroei van partijen die pretenderen oplossingen aan te kunnen bieden, terwijl de exacte eisen nog niet vastliggen. Sectoren die nog lange tijd geen DPP hoeven te leveren worden er nu al door klanten om gevraagd. Dit zorgt voor haastige, onvolledige en niet gestandaardiseerde noch toekomstbestendige implementaties.

Het DPP moet fungeren als een "single source of truth" voor gereguleerde productinformatie. Maar om dat waar te maken is een strikte technische scheiding nodig tussen publieke en niet publieke lagen. Publieke data (voor brede toegang) moet veilig ontsloten kunnen worden zonder toegang tot bedrijfsgevoelige informatie. Dit vraagt om afzonderlijke API-punten, dataclassificatie en beveiligde authenticatie en autorisatie voor niet publieke informatie. Zonder die scheiding ontstaat er een risico op onbedoelde openbaarmaking van intellectueel eigendom of strategische bedrijfsinformatie. Iets wat al helemaal in deze tijd, te allen tijde voorkomen moet worden.

Cybersecurity: van randvoorwaarde naar kernrisico

De schaal en openheid van het DPP maken cybersecurity tot een fundamenteel vraagstuk. Waar traditionele productdocumentatie vaak statisch en intern was, moet DPP-informatie dynamisch, extern toegankelijk en langdurig beschikbaar zijn. Dit creëert een aantal concrete dreigingsscenario's:

1. Denial-of-Service Aanvallen(DDoS): omdat DPP-data via online systemen toegankelijk moet zijn, kunnen aanvallen op bedrijfsservers of het centrale register directe impact hebben op beschikbaarheid. In het ergste geval kan dit leiden tot vertragingen in logistieke processen of markttoegang.
2. Datamanipulatie: onjuiste of gemanipuleerde productinformatie kan leiden tot verkeerde beslissingen, recalls of reputatieschade. De integriteit van data wordt daarmee cruciaal.
3. Identiteitsmisbruik: zonder robuuste authenticatie en autorisatie kunnen kwaadwillenden valse productpaspoorten aanmaken of bestaande gegevens aanpassen.
4. Economische spionage: zelfs openbare DPP-data kan waardevolle inzichten bieden in supplychains, productieprocessen of volumes. Aggregatie van deze informatie kan concurrentiegevoelige kennis blootleggen.

Het DPP vergroot daarmee het aanvalsvlak aanzienlijk: niet alleen grote bedrijven, maar ook kleinere leveranciers en MKB-bedrijven worden onderdeel van een publiek toegankelijk digitaal netwerk. Kwetsbaarheden bij één partij kunnen daarbij doorwerken in de hele keten, bijvoorbeeld wanneer onjuiste of gemanipuleerde productdata zich verspreidt naar afnemers, toezichthouders of andere systemen.

De kwetsbaarheid van decentralisatie

Het gedecentraliseerde karakter van het DPP zorgt ervoor dat bedrijven zelf controle houden over hun data en het systeem schaalbaar en flexibel blijft. Tegelijkertijd zorgt het voor grote uitdagingen. Elke eigenaar moet namelijk zorgen dat: de data continue beschikbaar is, wordt beschermd tegen ongeautoriseerde toegang en/of dataverlies en zij is verantwoordelijk voor correct versiebeheer. Voor veel organisaties is dit een flinke stap. Met name het MKB beschikt vaak niet over middelen voor: geavanceerde monitoring/detectie, DDOS-bescherming of zelfs maar een redundante infrastructuur.

Security-by-Design en proportionaliteit

Veilige implementatie vraagt om security-by-design en secure-by-default. Dus end-to-end encryptie, sterke authenticatie (minstens MFA), logging en monitoring en pentesting. Systemen moeten standaard veilig geconfigureerd zijn, zonder dat bedrijven complexe keuzes moeten maken. Dit is met name belangrijk voor kleinere organisaties, waar security-expertise beperkt is. Daarnaast is proportionaliteit cruciaal. Niet alle DPP-informatie is tijdkritisch. Als eisen rond beschikbaarheid en performance te zwaar worden (bijvoorbeeld 24/7 uptime), dreigt het DPP een kostbaar IT-systeem te worden dat de bedrijfsvoering belemmert in plaats van ondersteunt.

Data-opslag: een onderschatte uitdaging

Naast cybersecurity brengt het DPP een fundamenteel datavraagstuk met zich mee: "Hoe lang en door wie moet productinformatie worden bewaard?." Veel producten in de technologische industrie hebben een levensduur van 15 tot 50 jaar. Dat betekent dat data mogelijk decennialang beschikbaar moet blijven. Tegelijkertijd is nog onduidelijk

- wat de exacte bewaartermijnen zijn,
- wie verantwoordelijk is bij faillissement of overname,
- hoe om te gaan met verouderde bestandsformaten,
- hoe digitale handtekeningen en certificaten worden onderhouden.

Daar komt bij dat het niet alleen gaat om kerngegevens, maar ook om uitgebreide documentatie zoals handleidingen, revisies en onderhoudsinformatie. De opslag- en beheerkosten kunnen daardoor aanzienlijk oplopen. Een belangrijk principe uit de industrie is hier relevant: "wie gegevens nodig heeft, bewaart ze.", Een mooi uitgangspunt maar het is onrealistisch om deze verantwoordelijkheid bij eindgebruikers of consumenten te leggen, en evenmin wenselijk om fabrikanten onbeperkt verantwoordelijk te maken voor langdurige dataopslag van informatie die zij zelf niet meer gebruiken. Een meer realistische benadering ligt in een model waarbij fabrikanten, ketenpartners en digitale infrastructuren gezamenlijk zorgdragen voor beschikbaarheid en toegankelijkheid van data. Daarbij verschuift de focus van permanente opslag naar betrouwbare toegang, bijvoorbeeld via federatieve data-uitwisseling en gestandaardiseerde systemen. Zonder duidelijke afspraken over deze verantwoordelijkheden en de inrichting van data governance, dreigt het DPP niet alleen technisch complex, maar ook economisch onhoudbaar te worden, en druist het bovendien tegen de principes van data minimalisatie in.

Conclusie: balans tussen ambitie en uitvoerbaarheid

Het Digital Product Passport heeft de potentie om een sleutelrol te spelen in de transitie naar een duurzame en circulaire economie. De belangrijkste uitdaging ligt in het vinden van balans:

- tussen transparantie en bescherming van bedrijfsinformatie,
- tussen beschikbaarheid en proportionaliteit,
- tussen innovatie en uitvoerbaarheid.

Zonder duidelijke kaders voor governance, security, data-opslag en serviceniveaus dreigt het DPP uit te groeien tot een complex en kostbaar verplichtingssysteem. Met de juiste randvoorwaarden kan het echter juist een katalysator worden voor veilige, efficiënte en toekomstbestendige digitale waardeketens. Het DPP heeft het potentieel om het Europese concurrentievermogen te versterken. Het creëert kansen voor nieuwe markten en diensten rondom productdata, traceability en circulariteit, stimuleert innovatie in waardeketens en maakt nieuwe businessmodellen mogelijk, zoals: reparatie, hergebruik en lifecycle management. Tot slot, biedt het DPP een strategische kans voor Europa om grondstoffen en leveringszekerheid te versterken. Door beter inzicht in materiaalstromen en productdata, maakt het hoogwaardig hergebruik, reparatie en recycling mogelijk. Dit vermindert de afhankelijkheid van primaire grondstoffen en externe leveranciers en draagt bij aan het sluiten van materiaalcycli binnen Europa. Juist in een tijd van geopolitieke spanningen en schaarste aan kritieke grondstoffen vormt dit een belangrijk onderdeel van strategische autonomie. De komende jaren zijn daarmee bepalend. Niet alleen voor de technische uitwerking van het DPP, maar vooral voor het vertrouwen van bedrijven in dit nieuwe digitale fundament van de Europese industrie. Dat ontstaat alleen als het DPP op een realistische en bedrijfseconomische manier wordt geïntroduceerd en niet misbruikt wordt voor andere doeleinden. In dat geval kan het uitgroeien tot een katalysator voor zowel de groene als de digitale transitie, én tot een strategisch voordeel voor de Europese industrie.

Waar kun je terecht voor samenwerking, informatie en ondersteuning?

Het Centre of Excellence for Digital Product Passports (CoE-DPP) is een open initiatief onder leiding van TNO, als onderdeel van het Centre of Excellence for Data Sharing & Cloud. Het heeft als doel om de leidende hub te zijn voor ontwikkeling, standaardisatie en implementatie van het DPP in Nederland, gefinancierd door het ministerie van Economische Zaken en Klimaat. Het CoE-DPP zal de komende tijd use cases en informatie publiceren die u ondersteuning biedt bij het aanpakken van vraagstukken rondom het DPP.

Het CIRPASS-2-initiatief is een door de Europese Commissie gefinancierd project dat zich richt op de verdere ontwikkeling en opschaling van het Digital Product Passport in Europa. Aan de hand van 13 pilots zal het initiatief werkende DPPs demonstreren en het zal de opbouw en uitrol in verschillende productsectoren faciliteren. Daarnaast kunt u er brede informatie en updates over het DPP verkrijgen.

Lees daarnaast hier de gehele sectoranalyse en whitepaper van FME: https://www.fme.nl/system/files/publicaties/2026-03/FME%20Brochure%20DPP%20industry%20view_Digitaal.pdf

COLUMN NICOLE

Want ik behoud graag mijn eigen stem

Op de dag van de Odido-hack stond ik in Abcoude te presenteren voor een groep hoogopgeleide vrouwen, allemaal geïnteresseerd in cybersecurity. "Met de hack van vandaag is jouw onderwerp wel heel actueel," zeiden ze bijna in koor.

Ik wilde hen niet teleurstellen. Maar ik was niet gekomen om te praten over buitgemaakte gegevens. Mijn onderwerp: deepfakes en voice cloning. Bedreigingen die veel relevanter zijn dan het zoveelste bedrijf dat persoonsgegevens lekt.

Want experts noemden de gestolen Odido-data "goud waard voor criminelen" en spraken van één van de grootste datalekken ooit. Ik vraag me af in welke wereld zij leven. Deze gegevens liggen waarschijnlijk allang op straat. Zelfs met een IBAN, geboortedatum en adresgegevens moet een crimineel nog flink aan de slag — en heeft hij een actieve rol van het slachtoffer nodig. De paniek over dit datalek doet me denken aan iemand die alarm slaat over een lekke kraan, terwijl het hele huis onder water staat.

Want terwijl wij ons druk maken over gelekte IBAN-nummers, is de dreiging allang verdergegaan. Criminelen hoeven geen gegevens meer te stelen om geloofwaardig over te komen. Ze kunnen jouw stem namaken op basis van een paar seconden audio van social media. Je gezicht in een video plaatsen. Bellen met de stem van je dochter die in tranen beweert dat ze een ongeluk heeft gehad. Geen datalek vereist.

Dit is geen sciencefiction. Bedrijven verliezen miljoenen aan deepfake-videogesprekken met nep-CEO's. Ouderen worden opgelicht door gekloonde stemmen van hun kleinkinderen. Politici worden gediscrediteerd door video's waarin ze dingen zeggen die ze nooit hebben uitgesproken.

Toch besteden beleidsmakers hun energie aan AVG-boetes voor datalekken. Media schrijven verontwaardigde artikelen over falende IT-beveiliging. En wij knikken mee — alsof het beveiligen van een database het antwoord is op een wereld die allang verder is getrokken.

Vorig jaar zijn mijn uitstrijkgegevens gelekt, samen met die van duizenden andere vrouwen. Ik heb er geen nacht minder om geslapen. Deepfakes en voice cloning geven mij wél slapeloze nachten. Niet alleen vanwege de directe dreiging, maar omdat ze het fundament aantasten van hoe wij als mensen met elkaar communiceren en elkaar vertrouwen.

Dat is het gesprek dat we zouden moeten voeren. Over hoe we waarheid en authenticiteit waarborgen in het AI-tijdperk. Over een wereld waarin je niet meer kunt vertrouwen op wat je ziet en hoort.

Want ik behoud graag mijn eigen stem.

Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com

Auteur: Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via, ronald@eygendaal-assist.nl

Europese, soevereine smartphones voor security en privacy

Smartphones draaien bijna allemaal op Android (Google) of iOS (Apple), die veel gebruikersdata verzamelen. Smartphones zijn essentieel voor communicatie, de maatschappij, de overheid, bedrijven en kritieke infrastructuur. In tijden van geopolitieke spanningen (bijvoorbeeld: VS-China handelsconflicten, cyberdreigingen) wil Europa kwetsbaarheden verminderen. Afhankelijkheid van buitenlandse OS'en (Operating Systemen) vormt een risico: een update of 'kill switch' kan miljoenen apparaten uitschakelen. Logisch dat er vraag is naar een Europese alternatief, wat beter aansluit bij strenge EU-regels zoals de GDPR, DSA, NIS2. Een alternatief zonder dat het data naar buitenlandse servers stuurt of onder buitenlandse wetten komt te vallen. Een alternatief wat past bij de wens voor digitale soevereiniteit in Europa.

Maar wat verstaan we eigenlijk onder soeverein? Komt dan hard- en software uit Europa? En hoe zit met de processoren? Zijn er dan Europese alternatieven voor de processors van MediaTek uit Taiwan? of voor de processoren van het Amerikaanse Qualcomm?

Een eenvoudig onderzoekje leert dat de fabrikanten, die zogenaamd een soevereine smartphone fabriceren, bijna allemaal een processor van MediaTek aan boord hebben. De meeste fabrikanten focussen zich op de software en de data uitwisseling van en naar Google alsook naar de cloud. Omdat er voor de hardware en processoren niet echt alter-

natieven zijn, focussen we in dit artikel op de Europese fabrikanten ongeacht voor welke van deze onderdelen ze soeverein zijn. Maar ook, is de fabrikant echt Europees met soms een niet-Europese eigenaar erachter?

Voor echte "Europese soevereiniteit" (zoals vaak bedoeld in EU-tech-discussies: productie + data + controle + eigenaar binnen EU) voldoen de meeste fabrikanten niet helemaal

Europese smartphone fabrikanten gebruiken verschillende versies van het besturingssysteem. Het OS (Operating System) is de essentiële software die alle hardware aanstuurt. Het vormt de brug tussen jou en het apparaat (telefoon, tablet, computer). Dankzij het OS kun je apps gebruiken, bestanden beheren en taken uitvoeren. Vaak blijft de aanpassing van fabrikanten beperkt tot nét dat beetje extra. Hieronder een overzicht.

Volla

Volla Systeme GmbH, een Duits bedrijf uit Remscheid, ontwikkelt en assembleert smartphones met een sterke focus op privacy en onafhankelijkheid. Hun toestellen (zoals de Volla Phone Quintus, X23 en oudere modellen) komen standaard met Volla OS, een 'de-Googled' versie van Android gebaseerd op het open-source Android Open Source Project (AOSP). Maar ook Volla heeft MediaTek onder de motorkap.
https://volla.online

SHIFT

SHIFTphones worden ontwikkeld en deels geassembleerd in Duitsland, met nadruk op ethische productie, fair supply chains en ecologische materialen (bijvoorbeeld geen coltan). Hun toestellen zijn standaard uitgerust met ShiftOS, een aangepaste Android-versie. Van ShiftOS existeren verschillenden varianten: ShiftOS-G (met Google-diensten) of ShiftOS-L (Google-free, zonder Play Services). Ook bij SHIFT komen processoren en een groot deel van hardware van elders.
https://www.shift.eco/en/

Punkt

Het Zwitserse Punkt onthult de MC02, hun eerste privacy-gerichte smartphone met Apostrophy OS. Apostrophy OS is een custom, Google-vrije versie gebaseerd op Android Open Source Project (versie 13) en GrapheneOS (open-source, privacy-focused). Geen Google Play Services standaard; apps via GMS Wizard (voor compatibiliteit met Android-apps) of sideloaden. Bij Punkt komen processoren en een deel van hardware van elders op de wereld.
https://www.punkt.ch

Jolla

Jolla is een Fins bedrijf dat gespecialiseerd is in privacygerichte besturingssystemen en ontwikkelde Sailfish OS, het enige Europese mobiele besturingssysteem dat al meer dan tien jaar wereldwijd wordt toegepast op smartphones. Net als Android is Sailfish OS gebaseerd op Linux en kunnen er Android-apps worden geïnstalleerd. De selectie van geschikte hardware is nog kleiner dan bij GrapheneOS, dat alleen draait op Pixel-apparaten. Dus ook hier geen soevereine processoren en hardware.
https://commerce.jolla.com/

TESLA

Tesla is een Europees consumentenelektronicamerk van de in Belgrado, Servië gevestigde Comtrade Group. Het merk bouwt voort op een lange regionale traditie en biedt tv's, huishoudelijke apparaten, airco's, smartphones en meer. Tesla produceert o.a. Android-smartphones gebaseerd op Android Open Source Project (AOSP), met hardware en procesoren uit Azië.
https://tesla.info/en/phones/explr9/

Gigaset

Gigaset's productie en ontwikkeling vinden plaats in hun fabriek in Bocholt, Duitsland, maar heeft VTech Holdings Limited in Hong Kong als eigenaar. De smartphones die ze maken zijn gebaseerd op het open-source Android Open Source Project (AOSP) en de Processoren komen van de Amerikaanse fabrikant van halfgeleiders Qualcom.
https://www.gigaset.com

MPTech

MPTech (genoteerd aan de NewConnect-beurs van Warschau) is een toonaangevende Poolse fabrikant van consumentenelektronica en maakt deel uit van de TelForceOne Capital Group. Het bedrijf voert merken zoals: myPhone, HAMMER en VENTUS. MPTech ontwikkelt Android-apparaten met volledige Google Mobile Services (GMS) en werkt nauw samen met de Taiwanese chipontwerper MediaTek en het Chinese UNISOC. Het bedrijf is actief in heel Europa en richt zich op betaalbare, innovatieve technologische oplossingen.
https://www.mptech.eu/en

Nothing

Het Engelse Nothing Technology Limited werd door een Chinees-Zweedse ondernemer opgericht, het heeft naast het hoofdkantoor in Londen kantoren in: Shenzhen, China - ter ondersteuning van de productie en de toeleverings-keten - en in Tokio. Het is dus een Europees merk met Aziatische productie, vergelijkbaar met veel andere Europese merken.
https://nothing.tech

CROSSCALL

De fabrikant is het Franse bedrijf CROSSCALL, opgericht in 2009 met het hoofdkantoor gevestigd in Aix-en-Provence en is 100% Frans. De smartphones worden ontworpen in Frankrijk en vervaardigd in China en draaien op Android One. Processoren komen van de Amerikaanse fabrikant van halfgeleiders Qualcomm.
https://www.crosscall.com/

Fairphone

Fairphone is een Nederlands bedrijf, dat duurzame smart-phones maakt, maar de assemblage vindt plaats in een Chinese fabriek (Hi-P International in Suzhou) om te voldoen aan hun hoge ethische en ecologische standaarden, waarbij ze zich richten op eerlijke grondstoffen en betere werkomstandigheden in de keten. De smartphones van het bedrijf worden geleverd met besturingssysteem Android maar via samenwerkingen zoals met de /e/ Foundation kan de telefoon ook voorzien worden van alternatieve op Android gebaseerde besturingssystemen. Processoren komen van de Amerikaanse fabrikant van halfgeleiders Qualcomm.
https://www.fairphone.com/nl

Murena

Murena is een Frans bedrijf dat zich richt op privacy vrien-delijke smartphones en clouddiensten door Google-diensten te vervangen met open-source alternatieven, bekend als /e/OS, om digitale surveillance te bestrijden. Ze bieden een volledig ecosysteem, inclusief telefoons met het geïnstalleerde /e/OS (zoals de Fairphone, Pixel, SHIFT, CMF en eigen modellen) en privacy-georiënteerde cloud-opslag, e-mail en agenda. De focus ligt op het geven van controle over persoonlijke data door alle ingebouwde trackers te verwijderen. Maar ook bij Murena komen smart-phones en hardware van elders en zijn dus maar beperkt soeverein.
https://murena.com/

HDM

Het Finse HDM (Human Mobile Devices) is de grootste Europese smartphone fabrikant met eigen productielijnen in Hongarije én is maker van Nokia-telefoons. HDM maakt op zijn smartphone gebruik van Android One. Dat is een kale versie van het besturingssysteem Android. Telefoons met Android One krijgen snel en regelmatig beveiligingsup-dates. Processoren komen van de Amerikaanse fabrikant van halfgeleiders Qualcomm.
https://www.hmd.com

We zijn maar een "beetje" Soeverein

Kortom, voor Europese soevereine smartphones – met meer controle, privacy, risicoreductie en versterking van waarden & economie – moet er nog veel gebeuren. Europa importeert vrijwel alle processoren, hardware en onderdelen voor smartphones van buitenaf. Europa heeft circa 10% aandeel in de wereldwijde chipproductie (2025-2026), maar dit gaat bijna volledig naar automotive -, industriële -, power - en specialty chips. Er zijn geen Europese fabrieken voor de modernste nodes (zoals 3 nm of kleiner), cruciaal voor high-end smartphone-SoC's. Door politieke keuzes focust de European Chips Act (inclusief TSMC Dresden op 12-28 nm) op auto, AI en industrie – niet op smartphones.

Europese bedrijven en ontwikkelaars bouwen actief aan privacy-vriendelijke alternatieven zoals /e/OS, Ubuntu Touch, Volla OS en Sailfish OS. Deze open-source mobiele ecosystemen respecteren privacy, stimuleren onafhanke-lijke ontwikkeling en verminderen afhankelijkheid van Amerikaanse techgiganten.

Toch blijft er veel versnippering en een gebrek aan samen-werking tussen de projecten. Zonder sterke sturing en coördinatie vanuit Brussel blijft de soevereine smartphone een nicheproduct. Alleen met de juiste politieke keuzes (zoals het plaatsen van Europese subsidies voor deze sector op de agenda van de EU, alsook de politieke keuze om een Europese halfgeleider fabrikant te realiseren) en voldoende maatschappelijke druk kan dit veranderen. Dan kan Europa écht stappen zetten naar digitale soevereiniteit in smartphones.

INFORMATIEBEVEILIGING MAGAZINE

Draag bij aan de toekomst

Sluit je aan bij het PvIB-bestuur

Wil jij bijdragen aan de toekomst van informatiebeveiliging in Nederland? Sluit je aan bij het bestuur van PvIB.

Als bestuurslid werk je samen met een betrokken netwerk van professionals, denk je mee over de koers van de vereniging en draag je actief bij aan kennisdeling en verbinding binnen het vakgebied.

Geïnteresseerd?
Zet je expertise in en maak impact binnen de community.
Stuur een e-mail naar secretariaat@pvib.nl; wij maken graag kennis.

Achter Het Nieuws

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

Disclaimer: *het navolgend artikel deel uitmakende van de rubriek "Achter Het Nieuws" is met in acht genomen zorgvuldigheid samengesteld op basis van persoonlijke notities, waarnemingen en interpretaties opgedaan uit artikelen en bijeenkomsten en bedoeld als algemene informatie. De rubriek beoogt de redacteuren in discussie te laten treden met de auteur en daarmee lezers van deze rubriek over de grenzen van ons vak heen te laten kijken alsook nieuwe gedachten en/of visies ter kennis te nemen.*

De hier aangehaalde uitspraken, stellingen, mededelingen e.d. van derden zijn op persoonlijke titel weergegeven. Ondanks de betrachte zorgvuldigheid kan niet worden ingestaan voor de juistheid, volledigheid en actualiteit van de aangeboden informatie.

Noch mag men van geciteerde personen - dan wel de organisaties waarvoor zij werken - officiële dan wel formele standpunten of meningen uit dit artikel afleiden. Hetzelfde geldt voor het Platform voor Informatie Beveiliging en haar bestuur.

Eventuele omissies, vergissingen of fouten verzoeken wij u kenbaar te maken via: Ibmagazine@pvib.nl.

Vrijheid

is dat Virtuele Realiteit, voorspelbaarheid, media en scherm?

De Amerikaanse hoogleraar (Yale University, New Haven – 1701 opgericht) Timothy Snyder bezocht Nederland en lichtte zijn visie op democratie en tirannie toe tijdens een interview op het "internationaal literatuurfestival Den Haag: writers unlimited" (1). Diens visie doet een beroep op een actieve houding van progressief gerichte mensen.

Zijn visie en ervaring in het Amerika van nu is, dat het gepropagandeerde libertarisme (2) de wegvoorbereider is van fascisme en dictatuur. Moeten wij niet bewust worden en de waarschuwing zien voor mechanismen die parallellen vertonen met onze geschiedenis van 1933-1945?!

Libertarisme wenst de overheid af te schaffen. Het verafschuwt en wantrouwt sociale, collectieve regelingen. De heer Snyder formuleert het hard, dat de afkeer van gezondheidszorg en sociale voorzieningen gebaseerd is op racisme, mede op het verkeerde inzicht dat niet-witte Amerikanen frauderen, en witte-Amerikanen niet.

Zoals zo vaak bij dit soort ontwikkelingen worden er fictieve fronten gecreëerd. Nationalisme centraal gesteld en het extreem kapitalisme (welstand voor slechts de enkeling) de hemel in geprezen. Het lijkt dus tijd te zijn om oppositie te voeren.

Hoe speelt dit mee binnen ons vakgebied? Snyder benoemt dat niet expliciet, maar indirect herken ik veel wat ook ons aangaat. Hij heeft het over leven binnen de niet-3D-realiteit van alledag, vertaalt naar ons begrip van "Virtuele Realiteit (bijvoorbeeld TV/AR/ER/agentic AI)". AI dit gebaseerd op de noodzaak van voorspelbaarheid (LLM, statistieken). En dat terwijl onvoorspelbaarheid essentieel is voor vrijheid!

En zo komen wij uit bij de lancering van Nvidia's NemoClaw infrastructuur tijdens GTC 2026, welke de basis moet worden van elk AI-agent. Als je zijn 18 minuten presentatie volgt (3) dan zie je de triljarden bytes - en waarschijnlijk veel meer - aan data (AI als kerninfrastructuur met autonome agenten, digital twins en AI-aangestuurde fabrieken) alsook dollars bij dit bedrijf binnenstromen. De volgende Amerikaanse monopolie en het gevaar voor de "niet-Amerikaanse soevereiniteit".

De media-inspanning is indrukwekkend. Amerikaanse cultuur (?) domineert onze media en onze schermen. Zij degradeert vrijheid tot iets negatiefs, zelfs tot een negatief recht, zoals Snyder toelicht: er hoeven dan geen voorwaarden voor vrijheid geschapen te worden. Denk aan de aanval van de Amerikaanse techgiganten op de AI Act, waardoor de Europese Unie genoodzaakt ziet dat sociaal en collectief recht actief af te zwakken om Trump, de techgiganten en Amerika maar niet boos te maken.

Media die, in tegenstelling tot het leven in de werkelijkheid, geen tot nauwelijks herinneringen bij ons opbouwt; dat wat juist essentieel is voor het mens zijn. Mediaverslaving laat de geschiedenis meer en meer vergeten. In de periode van 1933 tot en met 1945 was de imposante rol van de bioscoop en de radio herkenbaar, dat als menner van het volk. Onwaarheden werden waarheden en de harde werkelijkheid werd naar de achtergrond zo niet uit zicht verplaatst. Media, die in bepaalde context, dan een krachtig middel zijn voor manipulatie en beeldvorming. Zeker constaterende dat de Amerikaanse technologie- & mediabedrijven een grote dominante positie innemen en de cloud- & data-infrastructuur daar een grote rol in gaan spelen. In hoeverre moeten wij ook nu vrezen voor een dergelijke stroming, maar dan met moderne technologie en een dataverzameling die zijn weerga niet kent.

Er zijn techgiganten en wetenschappers die het hebben over de waardeloosheid van bewaarde data. Die de discussie oproepen dat veel meer data moet worden vernietigd om niet aan data-obesitas te bezwijken. Vanzelfsprekend hebben zij het dan over onze data, niet hun eigen bestanden. Daarnaast, wie zei/schreef ook al weer: "Dat wat op het web (lees: computer, cloud e.d.) staat, staat er voor altijd!"?

Snyder geeft dan ook aan dat men veroordeeld wordt te leven "in het nu" en dan dus zonder kennis van de geschiedenis. Deze opsluiting "in het nu" is de basis voor manipulatie en het leven in een schijnwerkelijkheid. Extreme & kortstondige media-aandacht maakt dat iets belangrijker lijkt dan het in werkelijkheid is. Iets groeit van een minuscule gebeurtenis uit tot een boven proportionele ramp. Zo worden hypes (gebaseerd op bigtech-marketing of andere reclamestunten) een aan jezelf aan je schoenveters optrekkende, zichzelf versterkende motivatie oftewel drijfveer en politieke dogma's. Erover nadenkende, "Waar zien wij dat nu gebeuren?".

Het denken in concepten is het noodzakelijke tegenwicht. Het Rijnlands denken (4) (verfoeid door de liberalen c.q. het extreem kapitalisme, extreem rechtse partijen en nationalisten) is een dergelijk concept. In het Amerikaans denken gaat echter een gevaarlijke bedreiging schuil, zo schreef de 3e president van de Verenigde Staten, Thomas Jefferson (1802): *'I believe that banking institutions are more dangerous to our liberties than standing armies. If the American people ever allow private banks to control the issue of their currency, first by inflation, then by deflation, the banks and corporations that will grow up around the banks will deprive the people of all property until their children wake up homeless on the continent their fathers conquered.'*. Zo zien huidige critici ten aanzien van deze financiële concentraties zorgelijke parallellen.

Kijkende naar onze tijd, onze geopolitieke spanningen en ICT; dan zien wij, dat:
- banken de valuta beheersen *(denk aan Nederlandse banken die Amerikaanse debit- & creditkaarten en in plaats stellen van hun eigen betaalkaarten.*
- dat wij nu stagflatie (hoge inflatie, economische groei traag en werkloosheid hoog) waarnemen, waar eerst inflatie (algemene prijsstijging van goederen en diensten oftewel sec muntontwaarding) heerste;
- naast de banken bedrijven zijn ontstaan die over meer vermogen en werkkapitaal beschikken dan menig soeverein land in de wereld *(bezie hoe de Amerikaanse multinationals over en weer met vermogen – in de vorm van participaties & 'joint ventures' – schuiven en elkaars eigen vermogen – nominaal, maar niet intrinsiek – naar onmetelijke hoogte brengen, met Elon Musk als eerste mogelijke biljonair (> 1.000 miljard USD) op basis van een nieuw beloningsplan van Tesla (5),(6))*, zijn eigen onderneming;
- de collectieve overheidsbezuinigingen (Angelsaksisch van aard) & oplopende belastingen, die het grond- en eigen woningbezit nagenoeg alleen ten gunste laat komen van buitenlandse corporaties (zoals uit Amerika, Engeland, Duitsland) en de 'happy few' (7) en
- ten slot AgenticAI (NemoClaw), de door de deeloverheden nog steeds gehandhaafde, bekritiseerde en onbehoorlijke algoritmen, de uitbesteding van digitale burgerdata met voorbijgaan aan de privacyregels en dat alles vanwege het gemak en het niet bereid zijn tot offers (aangestipt door Peter Pannekoek in diens Oudejaarsconference 2025, 31 december 2025 – 22:24 uur, wellicht de onwil van het brengen van offers veroorzaakt door morele gierigheid).

Heel passend, bij dit alles, de door de **N**ederlandse **V**ereniging van **B**eëdigde **I**nformaticadeskundigen (**NVBI**) georganiseerde bijeenkomst over "digitale soevereiniteit" op 18 maart jl. in Amsterdam. Presentaties werden gegeven door:
- Björn Håkansson, sr. Business Development Manager / TNO,
- Jeroen Veldhorst, mede-oprichter en Algemeen Directeur / ContainerInfra B.V.,
- Kees Verhoeven, tech-expert, onafhankelijk adviseur en oud politicus (2e Kamerlid) en
- André de Groot / **D**e **N**ederlandsche **B**ank (**DNB**).

Ieder van de presentatoren hield een korte presentatie en op basis daarvan vond interactie met de anderen en de gasten plaats. Een laagdrempelig en vlot verlopend geheel waarbij behoorlijke diepgang werd gerealiseerd. Navolgend een persoonlijke interpretatie van de essentie.

André de Groot

Zijn werkzaamheden omvatte o.a. de Digital Operational Resilience Act (DORA) en het rapport over digitale afhankelijkheid. Hij begon zijn presentatie met de stelling dat men het proces van de digitale soevereiniteit heeft laten lopen, maar dat dit niet betekent dat het een verloren strijd zou zijn.

De belangrijkste redenen voor uitbesteding was, dat lokale datacenters veel werk met zich brengen en vereist dat kennis wordt bijgehouden. Verder dat de cloud de opties bood van schaalbaarheid en lagere kosten. Echter, de V.S. bleek uiteindelijk toch duurder te zijn dan verwacht. In 2019 kwam de ECB met haar 'guideline' concentratierisico's. Urgentie & impact werden destijds nog laag ingeschat daardoor niet veel resultaat geboekt. De Europese wens m.b.t. urgentie & middelen woog uiteindelijk veel lager dan de ervaren noodzaak tot uitbesteding.

In de daaropvolgende discussie waren enkele constateringen:
- veel kennis is in Europa aanwezig;
- de markt pakt het inmiddels op en
- DNB beoordeelde veel in relatie tot de 'risk appetite'.
  De aanbevelingen die gedaan werden wogen niet op tegen de hoge mate van zekerheid bij de Amerikaanse partijen en dat de Bedrijfscontinuïteit van de BigTech nu eenmaal hoog uitviel.

Jeroen Veldhorst

Hij begon ermee dat soevereiniteit uiteindelijk gebaseerd moet zijn op technische realiteit. IT gaat uiteindelijk over risico & impact alsook over ongemak en snelheid. Dus alles hangt samen met: juridische -, operationele -, strategische – en financiële risico's. Hij licht dat toe door risico & governance te koppelen aan architectuur & technologie en vervolgens met engineering realiteit. Zijn conclusie: digitale soevereiniteit ontstaat wanneer risico, architectuur en engineering op elkaar aansluiten.

Hij propageert dan ook open-standaarden. Open source, portable, geautomatiseerd met een ontkoppelde infrastructuur & applicatie om dan alternatieven in te schakelen op basis van de open-standaarden. Hij gaat dan ook voor "infrastructuur als code" bestaande uit declaratief beheer, meerdere Europese en Nederlandse aanbieders, waarbij infrastructuur goed beschreven dient te zijn, echter niet afgestaan! Hij mikt verder op GitOps beheer en wederom "deploy als code". Combineer dat met een 'self-hosted GitLab' en bewaak gedurende het gehele ontwikkelproces de transparantie & reproduceerbaarheid.

Hij wijst op het belang dat het IT-landschap inzichtelijk is (betekent: data, diensten & applicaties / locaties en leveranciers / verantwoordelijke teams en externe partijen); prioritering van kritieke afhankelijkheden (wat is bedrijfskritisch, waar zit het risico van 'vendor lock-in' en wat zijn de exit mogelijkheden?); om vervolgens erop te wijzen dat niet alles zelf gedaan hoeft te worden, dat er voldoende aanbieders in Europa en Nederland te vinden zijn.

Zijn conclusies:
- autonomie is een strategische keuze;
- alles als code;
- open-standaarden & open source en
- uiteindelijk 'security & compliance by design'.

In de discussie kwam aan de orde dat veel bedrijven niet alle beschikbare services nodig hebben, vaak zijn 20 – 40 services voldoende. Soevereiniteit wordt als 'mindset' gezien en dat betekent vooral: 'in control' zijn. Zo is het een realiteit dat hyperscalers groot zijn en blijven vanwege het geïnvesteerde vermogen. Dus niet alles zelf willen doen, maar weten wie aan welke knoppen zit. De aanwezigen spreken uit dat het inderdaad jammer is dat er in Nederland geen minister is aangesteld met digitalisering als prioritair aandachtsgebied.

Kees Verhoeven

Jammer genoeg komen de beste spullen uit de V.S. en werkt ook het schaalvoordeel voor hen. Elementen, zoals: het diep in de systemen zitten en een agressieve houding; maken dat onze afhankelijkheid zo groot is. Dan hebben wij het niet alleen over de V.S., maar ook andere derden. Kees Verhoeven constateert dan ook dat wij in plaats van afhankelijkheid moeten streven naar verbondenheid. Het druk zet-

ten op die wederkerige verbondenheidsrelatie doet dan over en weer gelijkelijk pijn.

"Wat kan je zelf doen?", is dan ook de vraag en daarbij komt de door de heer Aslander, elders, gestelde en in deze discussie geciteerde vraag: "Wat is de door ons zelf gelegde basis voor de afhankelijkheid?". Reactie: echte onafhankelijkheid is pas realiseerbaar als er door ons andere bestandsformaten worden ingezet.

Afsluitend legde Kees Verhoeven twee stellingen voor:
1. grote woorden staan daden in de weg!
2. Trump is het probleem niet!

Björn Håkansson attendeerde op de cloud ontwikkelingsopties. Kees Verhoeven wees op de kleine initiatieven, welke er al zijn, zoals het Nederlands taalmodel. Wij hebben echter geduld nodig. Jeroen Veldhorst vroeg zich af wat wij nu echt nodig hebben en Kees respondeerde dat de huidige situatie wel erg uniek is. André de Groot wees erop dat de aard van de risico's veranderd is, nu is meer sprake van systeemrisico's. Een antwoord op de eerste vraag is m.i. niet echt gegeven.

Trump zou inderdaad niet echt het probleem zijn was de eerste reactie op de tweede stelling. Het probleem zou veel meer liggen in de veel langere ontwikkelingstijden (x3) voor Europese leveranciers aangaande hard- & software. Wij zouden een te lage offerbereidheid hebben aldus conferencier Peter Pannekoek. De conclusie luidde, dat geld de kritische factor is, dat in Amerika het extreem kapitalisme en de ego (Hoofdredacteur: narcisme?!) de boventoon voert. Als positief signaal wordt aangehaald dat het Europees Galileo GPS project de onafhankelijkheid van de V.S. heeft weten te realiseren en zelfs op punten kwalitatief beter is. Vanuit Europa moet gewerkt worden aan één toekomst, waarbij kosten niet leidend mogen zijn. Wel moeten wij bewust zijn van het Chinese risico met betrekking tot de lage kostprijs (dumping).

Björn Håkansson

`Cloud is central to digital sovereignty / autonomy'! TNO draagt de visie uit dat specifiek de technologie omtrent data opslag bepalend zal zijn voor het creëren van nieuwe controle punten of aanpassing van bestaande controle punten, welke laatste door tegenstanders als knelpunten benut kunnen worden. TNO is dan ook diep geïnvolveerd in het Europese cloud-landschap. In een tabel liet TNO zien hoe zij op de korte en langere termijn inspeelt op gebruikers-, overheids- en industriestrategieën.

Zijn stelling luidde: "Is innovatie belangrijk voor het versterken van digitale soevereiniteit? En hoe dan? Welke rol moet de overheid hierin spelen?".

Hierop ontstond een levendige discussie. Ten aanzien van het eerste punt werd geconstateerd dat schaalgrootte dan essentieel is. In de V.S. is dat simpel, binnen Europa moet daaraan gewerkt worden. André de Groot gaf aan dat er geld nodig zal zijn alsook een industriepolitiek. Echter, soevereiniteit mag niet een doel op zichzelf zijn.

Over het hoe waren de meningen verdeeld. Geld is nodig, maar eerder nog een goed functionerend eco-systeem. Dat vanuit de Europese unie, maar niet dat het leidt tot Europese kampioenen, die vervolgens weer een te grote (markt)macht krijgen. Ja, het kost geld, levert risico's op en dus moet de overheid inspringen. Let wel, de marktwerking moet intact blijven, Nederland zou daarin een Europese toppositie kunnen bekleden. Een voortrekkersrol dus voor de overheid, daarnaast een brede regelgeving en dat ook voor AI wat moet leiden tot meer kansen.

De verdere zaaldiscussie ging meer in op concrete detailzaken en specifieke procedures c.q. casussen zoals Odido, cybercrime losgelden. Voor dit "Achter het nieuws" item minder relevant.

Nu het woord aan de redacteuren: hoe staan zij tegenover de consequenties van Snyder's uitspraken gekoppeld aan de concrete analyses en suggesties tijdens de NVBI-bijeenkomst?

Maarten Hartsuijker

In een wereld waarin onze agenda's voller zijn dan onze inboxen, klinkt "leven in het nu" als een aantrekkelijk streven. Maar precies dat motto – dat we massaal omarmen om onze hectiek te overleven – verandert in een gevaarlijke valkuil zodra het gaat om informatiebeveiliging en digitale soevereiniteit. Want wie alleen in het nu leeft, verliest al snel uit

het oog waar morgen de regie
over de digitale fundamenten van onze samenleving ligt.

Europa beschikte ooit over een krachtige eigen digitale infrastructuur, maar heeft zichzelf verslaafd gemaakt aan de snelle suikers van de cloud. Enterprise- en infra-architecten verzekerden hun besturen jarenlang dat er altijd een exit-strategie klaarstond, dat we "morgen weer konden stoppen" als het nodig was. Maar zoals bij elke verslaving bleek de terugweg een stuk lastiger dan de
verleiding. Terwijl wij druk zijn met optimaliseren, outsourcen en automatiseren, bouwen Amerikaanse techgiganten aan ecosystemen die zo omvangrijk zijn dat ze bijna vanzelfsprekend lijken. "America First" hoeft niet te betekenen dat de rest van de wereld automatisch "second" is, maar door onze digitale ruggengraat uit handen te geven, maken we die rangorde wel erg
gemakkelijk waar.

Informatiebeveiliging draait uiteindelijk om controle: controle over data, risico's en afhankelijkheden. En controle kun je niet uitbesteden. Dat Amerikaanse cloudoplossingen "uiteindelijk toch duurder bleken dan verwacht" is dan ook geen incident, maar een symptoom van een dieper probleem: we hebben gemak boven autonomie gekozen. En gemak is een slechte raadgever in security.

Digitale soevereiniteit vraagt om een lange adem, technische investeringen en politieke moed. Open standaarden, Europese cloudalternatieven en transparante architecturen zijn geen luxe, maar voorwaarden voor een veilig digitaal Europa. Niet om ons af te sluiten, maar om gelijkwaardig te blijven.

Misschien moeten we dus iets minder "leven in het nu" en iets meer "bouwen aan later". Want vrijheid – zowel digitaal als maatschappelijk – is geen momentopname. Het is een infrastructuur. En infrastructuur moet je zelf in handen houden, anders leef je niet in het nu, maar in iemand anders' toekomst.

Fook Hwa Tan

Geen grote woorden, maar een grote lijn

Er is een Chinees gezegde: het beste moment om een bos te planten was jaren geleden. Het op één na beste moment is nu. Dat is precies de positie van Europa. De digitale weerbaarheid die we vandaag nodig hebben, hadden we eerder moeten opbouwen. Dat is niet gebeurd. Te vaak kozen we voor snelheid, gemak en schaal. Te weinig voor strategische veerkracht.

Daarom moet het debat over digitale soevereiniteit niet blijven steken in incidenten of sentiment. Dit vraagt visie. En visie zonder strategie is vooral theater.

De realiteit is helder. Europa kan vandaag niet op alle digitale terreinen direct op hetzelfde niveau concurreren. Niet in schaal. Niet in kapitaal. Niet in marktmacht. Juist daarom is luid roepen om abrupte ontkoppeling geen verstandige koers. Dat is geen strategie, maar ongeduld.

De betere lijn kennen we al. In het debat over China schoof de taal op van decoupling naar de-risking. Dat was verstandig. Niet alle banden verbreken, wel kritieke afhankelijkheden verminderen. Niet jezelf isoleren, wel zorgen dat je kunt blijven functioneren als de omstandigheden kantelen.

Diezelfde strategische logica moeten we nu ook digitaal toepassen. Bouw aan open standaarden. Eis portabiliteit. Ontwerp voor uitwisselbaarheid. Investeer in Europese capaciteit waar het ertoe doet. Maak exit-scenario's serieus. Kies niet voor afhankelijkheid uit gewoonte, maar voor weerbaarheid uit overtuiging.

Soevereiniteit is dan ook geen roep om afsluiting. Het is een langetermijnstrategie. Een kwestie van richting, ontwerp en discipline. Het bos staat er nog niet. Maar wie vandaag verstandig plant, bepaalt wel hoe het Europese digitale landschap er morgen uitziet.

Leo van Koppen

Perfect storm op de vrijheid

In ons vakgebied gaat het altijd weer over risico's, we nemen alleen nog maar besluiten gebaseerd op een risico-inventarisatie. Risico's, die worden afgemeten aan waarschijnlijkheid van optreden en mogelijke impact die het kan hebben op de bedrijfsvoering of persoonlijke situatie. Steeds weer opnieuw moeten we risico-inventarisaties uitvoeren, omdat nieuwe kwetsbaarheden en dreigingen zich aandienen.

Het dreigingsbeeld is een terugkerend onderdeel geworden in onze manier van denken. Met de komst van de Trump en het onderliggende MAGA gedachtegoed is het dreigingsbeeld behoorlijk gewijzigd. Soevereiniteit is nu het keyword in ons vakgebied geworden, want het bepaalt in belangrijke mate alle drie de BIV-factoren, van oudsher de uitgangspunten van informatiebeveiliging.

Hoe botst Snyders visie op vrijheid nu met de dagelijkse praktijk van informatierisico's? Timothy Snyder is een wetenschapper met een uitgesproken visie op vrijheid. Hij definieert vrijheid in termen van soevereiniteit (zonder autonomie geen vrijheid), onvoorspelbaarheid (ruimte voor creativiteit en verandering), mobiliteit (bewegen door ruimte en tijd), feitelijkheid (toegang hebben tot de waarheid/bescherming tegen manipulatie) en solidariteit (collectiviteit, democratie en gelijkheid).

Als we door onze oogharen Snyders visie op vrijheid in relatie tot onze ervaringen met anderhalf jaar Trump/MAGA bekijken, dan is het duidelijk dat dit op alle aspecten conflicteert. De impact van Trump 's beleid met de geopolitieke en economische gevolgen zet ook onze vrijheid onder druk. Maar naast Trump zijn er natuurlijk ook enorme technologische ontwikkelingen met name op het vlak van de IT, OT en AI. De impact daarvan is nog niet helemaal te overzien, maar zal op z'n minst heel groot zijn.

Daarbij hebben we onszelf nog niet zo lang geleden massaal aan het cloud-infuus van Big Tech gelegd. Tot overmaat van ramp heeft Big Tech tijdens de inauguratie van de president de liefde verklaard aan Trump. Met als gevolg dat Big Tech een redelijk vrij speelveld zal krijgen en de dominantie van Big Tech negatief zal doorwerken op zaken als soevereiniteit en solidariteit. Kortom de negatieve effecten op de vrijheid zullen elkaar gaan versterken.

Hoeveel ellende kan je tegelijkertijd overkomen? Het doet mij denken aan een "perfect storm".
Samenvattend de risiconiveaus bij de elementen van Snyders vrijheid:

- Soevereiniteit (cloud-infuus van big Tech)= Zeer Hoog (ZH)
- Onvoorspelbaarheid (Trump) = ZH
- Mobiliteit (MAGA) = ZH
- Feitelijkheid (MAGA/Trump) = ZH
- Solidariteit (MAGA/Trump/Big tech) =ZH

Of schets ik nu een te fatalistisch scenario?

Alex Dingemanse

De architectuur van vrijheid: Soevereiniteit door encryptie en standaarden

De discussie over digitale soevereiniteit, zoals aangestipt door Timothy Snyder en de experts van de NVBI, raakt de kern van ons vakgebied. Als we kijken naar de toekomst van informatiebeveiliging in 2026, zien we een cruciaal spanningsveld: de behoefte aan de enorme rekenkracht van AI-infrastructuren zoals Nvidia's NemoClaw versus de noodzaak om de regie over onze eigen data te behouden.

Een aanvullend perspectief op dit debat is dat soevereiniteit niet noodzakelijkerwijs synoniem hoeft te zijn met het fysiek bezitten van de hardware. In het moderne cybersecurity-landschap kijken we steeds vaker naar een model waarbij we de voordelen van schaalbaarheid en innovatie uit de VS kunnen benutten, zonder de controle over de inhoud op te offeren. Dit wordt wel de "soevereiniteit door architectuur" genoemd.

De wiskundige grens
Waar Snyder waarschuwt voor de onzichtbare macht van algoritmen en datahonger, ligt voor ons als security-experts een kans in de techniek zelf. Echte digitale onafhankelijkheid wordt in 2026 niet meer alleen bepaald door waar een server staat, maar door wie de sleutel heeft.

Door zwaar in te zetten op technologieën zoals:

- Confidential Computing: waarbij data zelfs tijdens de verwerking in de cloud versleuteld blijft voor de provider.
- Bring Your Own Key (BYOK): waarbij de cryptografische controle strikt binnen de Europese jurisdictie blijft.
- Zero Trust Architecture: waarbij geen enkele infrastructuur, Amerikaans of Europees, inherent wordt vertrouwd zonder continue verificatie.

Verbondenheid in plaats van isolatie
Zoals tijdens de NVBI-bijeenkomst werd gesuggereerd, is volledige onafhankelijkheid in een verbonden wereld complex. Een pragmatische koers is het streven naar 'wederkerige verbondenheid'. Dit betekent dat we gebruikmaken van de hoogwaardige beveiligingscapaciteiten en AI-tools van wereldspelers, maar dat we onze systemen zo ontwerpen dat we op elk moment kunnen overstappen.

Open standaarden en "infrastructure as code", zoals Jeroen Veldhorst bepleit, zijn hierbij essentieel. Het stelt ons in staat om de 'vrijheid van beweging' te behouden. Als we onze diensten modulair en portable bouwen, verkleinen we het risico op een vendor lock-in en versterken we onze positie aan de onderhandelingstafel.

Vrijheid is inderdaad een infrastructuur, maar eentje die in de 21e eeuw grotendeels uit software en protocollen bestaat. Onze taak als analisten is om een veilig digitaal fundament te bouwen dat bestand is tegen politieke verschuivingen. Door encryptie en open standaarden als onze primaire verdedigingslinie te gebruiken, creëren we een soeverein Europa dat niet geïsoleerd is, maar juist krachtig en autonoom opereert binnen het mondiale speelveld.

Het "bouwen aan later" begint bij het nu technisch onmogelijk maken dat onze data door derden gemanipuleerd of onteigend kan worden, ongeacht op wiens cloud de bits en bytes toevallig landen. Om een soevereine cloud-architectuur te realiseren die gebruikmaakt van wereldwijde schaalbaarheid zonder de controle te verliezen, moeten we de focus verplaatsen van de locatie naar de beheerlaag.

Tim Deahl

Digitale autonomie begint bij wendbaarheid

"Mensen accepteren verandering alleen wanneer die noodzakelijk is — en zij herkennen die noodzaak meestal pas in tijden van crisis."

Toen Jean Monnet (1888-1976) — een van de architecten van de Europese eenwording — dit in de jaren '70 opschreef, keek hij terug op een continent dat zich onder druk van crisis had leren organiseren. Europese samenwerking was geen abstract ideaal, maar een antwoord op noodzaak. Diezelfde logica dringt zich vandaag opnieuw op. Waar de Europese Unie ooit ontstond uit de wens om vrede duurzaam te borgen door economische zekerheid, groeit nu de roep om strategische autonomie. Ditmaal niet alleen tegenover staten, maar ook tegenover de dominante positie van technologiebedrijven als Google, Amazon en Meta. De vraag raakt daarmee niet alleen technologie, maar ook soevereiniteit, democratie en controle over de digitale infrastructuur van Europa.

Digitale autonomie klinkt vaak als een groots politiek project, iets van lange adem en ver buiten de dagelijkse secu-

rityпraktijk. Maar voor securityprofessionals begint die beweging juist in het klein: in de keuzes die vandaag worden gemaakt, in de vragen die wel — of juist niet — worden gesteld, en in de mate waarin afhankelijkheid zichtbaar wordt gemaakt.

Die eerste stap is inzicht. Niet in abstracte termen, maar in de concrete werking van jouw eigen organisatie. Wat gebeurt er als een identity provider uitvalt en niemand nog kan inloggen? Wat als logging en monitoring via één externe dienst lopen en plots wegvallen? Of als de control plane van een cloudomgeving tijdelijk niet beschikbaar is, waardoor deploys en wijzigingen stilvallen? Veel securityteams begrijpen dreigingen tot in detail, maar hebben hun afhankelijkheden minder scherp. Juist daar ligt naar mijn mening een gemiste kans. Wat niet zichtbaar is, kan ook niet worden gestuurd. Autonomie begint met het expliciet maken van die afhankelijkheden — en dat is iets wat elke securityprofessional vandaag al kan doen.

De volgende stap zit in ontwerpkeuzes. Niet door bestaande technologie direct te vervangen, maar door te voorkomen dat systemen onnodig vast komen te zitten. Autonomie groeit zelden door een radicale breuk, maar door het behouden van opties. Dat betekent werken met open standaarden waar mogelijk, vermijden dat data of functionaliteit slechts binnen één platform bruikbaar is, en bewust omgaan met configuraties die alleen in één ecosysteem werken. Je hoeft morgen niets te migreren, zolang je maar voorkomt dat je overmorgen geen keuze meer hebt.

Daarnaast ligt er een rol in het actief verkennen van alternatieven. Niet als ideologisch statement, maar als voorbereiding. Europese aanbieders en open source oplossingen ontwikkelen zich snel, maar blijven vaak buiten beeld zolang niets ons dwingt om anders te kijken. Door ze nu al te volgen, kleinschalig te testen en op te nemen in het gesprek, ontstaat er iets dat essentieel is voor autonomie: keuzevrijheid. En keuzevrijheid is uiteindelijk een vorm van veiligheid.

Een cruciale verschuiving is, om geopolitieke afhankelijkheid expliciet onderdeel te maken van risicomanagement. Niet als bijzaak, maar als volwaardig risico naast klassieke cyberdreigingen. Wat is de impact als een leverancier, door geopolitieke druk of veranderende wetgeving, zijn dienstverlening aanpast? Hoe ziet continuïteit eruit als toegang tot kritieke systemen tijdelijk wordt beperkt? Dit zijn helaas geen hypothetische scenario's meer, maar de realiteit. Door dit soort vragen structureel mee te nemen, verandert afhankelijkheid van een impliciete aanname in een bestuurbaar risico.

Tot slot vraagt digitale autonomie om wendbaarheid — niet alleen in technologie, maar ook in processen. Incidentrespons, changemanagement, toegangsbeheer en samenwerking met leveranciers moeten flexibel genoeg zijn om mee te bewegen wanneer omstandigheden veranderen. Waar systemen of processen verstarren, verdwijnt de ruimte om te kiezen. En zonder keuzevrijheid is autonomie een illusie.

Autonomie ontstaat daarmee niet door een rigide breuk met bestaande technologie, maar door het systematisch vergroten van onze vrijheid van handelen. Zoals Monnet al scherp zag, komt verandering vaak pas onder druk. De vraag is alleen of securityprofessionals wachten tot die druk onvermijdelijk wordt — of dat we er vandaag al mee beginnen.

Referenties

(1) Zie https://www.bnnvara.nl/joop/artikelen/timothy-snyder-herover-de-vrijheid-nu-ze-vernietigd-wordt

(2) Een politieke filosofie, die individuele vrijheid en zelfbeschikking als kernwaarden ziet, welke de vrije markt – lees extreem kapitalisme – als enige juiste ordening ziet en daarmee de hoogste welvaart gecreëerd ziet. Zij baseren zich daarbij op de term 'libertas' wat "vrijheid" betekent.

(3) Zie https://www.youtube.com/live/kRmZ5zmMS2o en https://nvidianews.nvidia.com/news/nvidia-announces-nemoclaw

(4) Rijnlandse denken ook wel Europees organiseren kan u terugvinden in het boek: "Nieuw Europees organiseren. Organiseren op basis van vakmanschap, verbinding en vertrouwen."; auteurs: Jaap Jan Brouwer & Jaap Peters, ISBN: 978-90-8965-024-5, 1e druk 02.2011

(5) https://www.msn.com/nl-nl/geldzaken/nieuws/hoe-elon-musk-de-eerste-biljonair-ter-wereld-zou-kunnen-worden/ar-AA1M6Rff

(6) https://www.man-man.nl/elon-musk-biljonair-binnen-drie-jaar/

(7) Voor een ontluisterend verhaal over de wooncrisis en de machinerie van de volkshuisvesting, zie: https://www.ftm.nl/volkshuisvesting en https://carlijnkingma.com/DOCUMENTARY van Carlijn Kingma, cartograaf van de maatschappij.

ZET VANDAAG DE STAP NAAR BETERE CYBERVEILIGHEID.

In een digitale wereld waarin risico's zich sneller ontwikkelen dan ooit, heeft uw organisatie behoefte aan experts met betrouwbare kennis. Deze kennis helpt u veilig en toekomstbestendig te blijven. Door de overname van de Security Academy in 2025 bundelt DNV toonaangevende cybersecuritykennis met jarenlange ervaring in risicobeheersing. Cursussen zoals Identity & Access Management en Security Essentials zijn hierdoor direct toepasbaar in uw organisatie.

Zet vandaag de stap. Samen helpen we u om uw informatie, systemen en reputatie duurzaam te beschermen. Met onze cursussen voorkomt u dat dreigingen uitgroeien tot schade en blijft uw organisatie beschermd.

Bekijk het complete aanbod op **dnv.nl/cybersecurity**

Identity & Access Management Woerden of online | 3 dagen | EUR 2350

Security Essentials Woerden of online | 1 dag | EUR 895

Security Behaviour Foundation Woerden | 2 dagen | EUR 1647

DNV

Scan de QR-code en ontdek het cursusaanbod op dnv.nl