iB
INFORMATIEBEVEILIGING
jaargang 17 - 2017
#2

BLOCKCHAIN

Blockchain: van hype naar hymne?

Alles wat je moet weten over blockchain

0-day aanvallen op de blockchain

Interview Aart Jochem

Certificeren? Dan moet u voldoen aan de norm. DNV GL toetst u snel en goed. Maar iedereen houdt van opstekers, niet van standjes. Daarom kijken we bij certificering ook naar wat goed gaat en zelfs nog beter kan. Op die gebieden die voor uw bedrijf of organisatie belangrijk zijn. Aandachtspunten waarop u zélf beoordeeld wilt worden. Certificering die net even verder voert. Want verbetering zit in een klein hoekje.

U kunt ons bereiken via 010 2922 700 of www.dnvgl.nl

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers

SAFER, SMARTER, GREENER

DNV·GL

BLOCKCHAIN

Wellicht een verrassing voor u? Wel Lex, maar een andere Lex dit keer. Dat heeft alles te maken met een nieuwe aanpak, die we binnen de redactie van uw lijfblad IB-Magazine dit jaar hebben opgestart. Elke uitgave krijgt één van de redacteuren als trekker, en de bedoeling is om onze veel te weinig geprezen hoofdredacteur Lex B. wat te ontlasten. Dit keer is het mijn beurt, en we gaan gelijk van start met een uitgave die vooral over het thema blockchain gaat. Reinier van der Drift vertelt ons wat dat nou precies is, en wat je er zoal mee zou kunnen gaan doen, hij vergelijkt het zelfs met een nieuwe dot.com revolutie. Er wordt volop gewerkt aan Proof of Concepts, onder andere bij ING [1] en ook binnen de Nederlandse overheid zijn de nodige projecten opgestart [2]. Het hoeft echter niet altijd over financiële toepassingen te gaan, Refugee E-Dentity was een winnend project bij de recente Dutch Blockchain Hackaton [3]. De vraag is of het wel allemaal zo veilig is, Harld Röling plaatst een aantal kritische kanttekeningen bij de ontwikkelingen. Ook laten we een aantal experts aan het woord over het thema blockchain.
Voor het veilig implementeren van blockchain zijn goed opgeleide security specialisten nodig, maar hoe weet je wat je in huis haalt? Jan Wessels en Olaf Streutker delen hun gedachten over het nieuwe kwalificatiestelsel voor IB'ers (QIS) en hoe dit bij enkele grootbanken geïmplementeerd wordt. Naast de bekende columns en een boekreview hebben we in dit blad ook een interview met Aart Jochem, die terug kijkt op zijn ervaringen bij GovCERT en NCSC.
Vanaf deze plaats wil ik graag Bart Jacobs van harte feliciteren met de hem toegekende SURF Security & Privacy Award 2017, een welverdiende erkenning voor al het werk dat Bart heeft verzet om onze BV Nederland veiliger te maken.

Tot slot: zoals u wellicht al heeft bemerkt, experimenteert de redactie nu ook met digitale uitgaven van ons lijfblad. We horen graag wat u daar van denkt, hoe u de digitale uitgave leest en beoordeelt, en uiteraard staan we open voor uw suggesties en verbeterpunten. E-mail ons op ibmagazine@pvib.nl.

Lex Dunn, redacteur

[1] www.telegraaf.nl/digitaal/27668799/__ING_doet_geslaagde_test_met_blockchain__.html
[2] www.linkedin.com/hp/update/6239839738530971649
[3] http://agconnect.nl/artikel/winnend-blockchain-idee-online-id-voor-vluchtelingen

In dit nummer

BLOCKCHAIN: VAN HYPE NAAR HYMNE?

Wat is blockchain en hoe kun je het gebruiken?

Sinds de DotCom-periode is geen technologie meer zo gehypet als blockchain-technologie. Blockchain-adepten noemen het een nog fundamentelere technologie dan TCP/IP was voor het internet. Wat is blockchain-technologie, waar is het voor bedoeld en vooral, wat zal dan die fundamentele maatschappelijke verandering zijn?

The Internet of Everything needs a Ledger of Everthing
The blockchain is a truly open, distributed, global platform that fundamentally changes what we can do online, how we do it, and who can participate. Call it the world wide ledger.

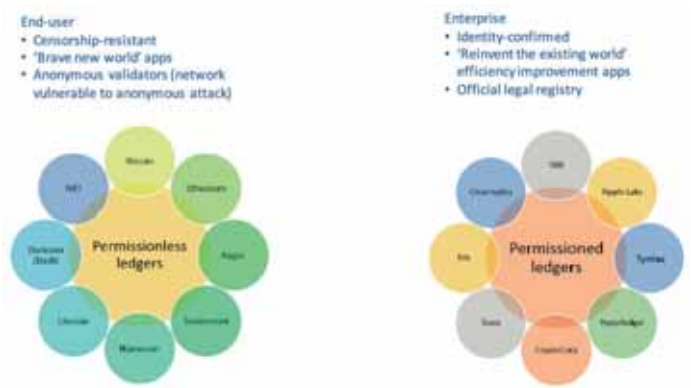
- Don & Alex Tapscott [1]

Er is niet één blockchain

Er wordt veel gepraat over 'de blockchain', alsof er maar één blockchain bestaat. Echter, er zijn verschillende soorten blockchains. Elk met een eigen signatuur en bijbehorende consensusprotocollen, die ontworpen zijn voor bepaalde use-cases. De Bitcoin-blockchain en het bijbehorend 'proof of work' consensusprotocol bijvoorbeeld, lossen het zogenaamde 'double spend'-probleem op bij digitaal geld. Het zorgt ervoor dat eenzelfde digitale munt niet twee keer kan worden verhandeld of uitgegeven. Het zijn met name cryptocurrencies waarmee blockchain-technologie bekend geworden is en waarvan Bitcoin veruit de populairste en het meest bekend is. Cryptocurrencies gebruiken overwegend publieke blockchain-technologie.

Naast publieke blockchains zijn er ook private blockchains. Een andere term die je in dit verband vaak hoort is 'permissionless' en 'permissioned' blockchains, ook wel ledgers genoemd.

Public & permissionless betekent dat de actoren en de hardware waarop de blockchain draait onbekend c.q. anoniem zijn. Private-permissioned ledgers daarentegen draaien op bekende en beheerde hardware en de actoren/deelnemers zijn geïdentificeerd en geauthenticeerd door bijvoorbeeld een KYC- (know your customer) of andere onboarding procedure.



T. (0215). Consensus as a service: a brief report on the emergence of permissioned, distributed ledger systems htttp://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distribute-ledgers.pdf

Permissioned ledgers

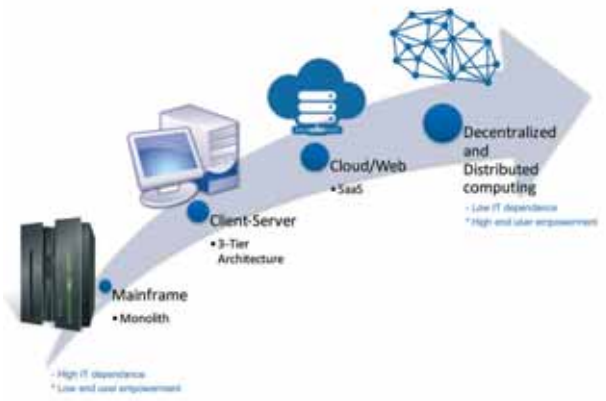
Er zijn ook private-permissioned blockchain-technologieën die zonder cryptocurrencies werken. Bijkomend voordeel voor het bedrijf is dan dat de CFO niet gedwongen wordt om niet-gereguleerd geld in z'n financieel overzicht op te nemen. Veelal kunnen dit soort systemen enorme transactievolumes verwerken.

Een ding hebben alle blockchains gemeen; ze zijn ontworpen om de noodzaak voor de Trusted Third Party (TTP) in ketens of processen te elimineren. De blockchain vormt dan het trustcenter. Daardoor ontstaat optimalisatie in de keten/het proces en wordt vertrouwen op een hoger plan getild en kan het gebruikt worden om processen verder te automatiseren (smart contracts).

De ontwikkeling van netwerkarchitectuur

De afgelopen decennia heeft de netwerkarchitectuur verschillende ontwikkelstadia gehad, elk met hun eigen karakter qua informatiebeveiliging. Het ging van een gecentraliseerd model, via een client-server model naar het huidige cloudcomputing-model. Dit laatste zou je ook een gecentraliseerd model kunnen noemen. De ontwikkeling wordt mogelijk gemaakt door een drietal factoren;

1. **Dalende kosten hardware**
2. **Stijgende rekenkracht**
3. **Virtualisatie**



Distributed computing

Volgens Peter Levine, partner bij Venture Capital bedrijf Andreesen Horowitz, is het einde van het cloudcomputing-tijdperk al weer in zicht [2]. Zijn stelling is dat in 2020 naar een volledig gedistribueerd model wordt gegaan onder invloed van Internet of Things en machine-learning. Hij noemt dit Edge Computing. Dit is geheel in lijn met de ontwikkeling van blockchain-technologie als vitaal onderdeel in gedistribueerde computing.

Qua informatiebeveiliging kan voor de verschillende stadia van netwerk architectuur het volgende model gehanteerd worden:

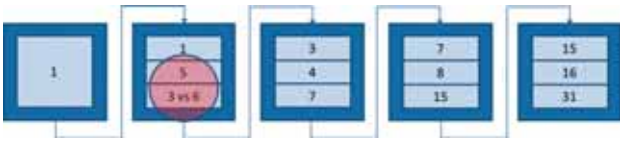
Soort	kwetsbaarheid	Niveau kwetsbaarheid	Kosten Informatiebeveiliging
Mainframe	-	Admin	--
Client/Server	++	Admin, end-user hardware (patch)	++
Cloud computing	+	Admin end-user	+
Distributed and Edge computing	--	enduser	-

Kwetsbaarheden

Volgens dit model dalen de kosten voor informatiebeveiliging bij een gedistribueerd model, omdat de invloed van onder andere de admin, als trusted third party, wordt verminderd.

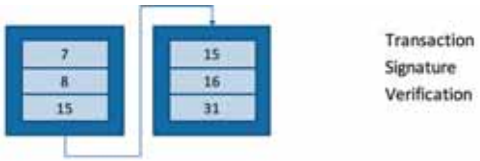
De blockchain en hoe het werkt?

Waarom het de blockchain heet, weet niemand. Het bekt lekker, maar het hadden ook cirkels of rechthoeken kunnen zijn, maar dat terzijde.



De karakteristiek van de blockchain is dat de output van het eerste blok, de input vormt voor het tweede blok enzovoorts. Het eerste blok wordt het zogenaamde Genesis-blok genoemd. Het is de eerste transactie die wordt vastgelegd in de blockchain. Elk blok is volledig versleuteld, gehashed en omdat alle blokken aan elkaar gerelateerd zijn, is het onmogelijk om de ketting te verbreken door één blok te hacken zonder alle andere blokken te herschrijven. Daarvoor heb je onder andere de private-key van anderen nodig. Omdat de blockchain niet op één node draait, maar bijvoorbeeld in het geval van Bitcoin op meer dan 17.000 nodes, moet een aanvaller dus op 17.000 nodes op hetzelfde tijdstip een volledige herschrijving van de blockchain zien te bewerkstelligen om één transactie te manipuleren. Dat is met de huidige computerkracht onmogelijk. Wellicht dat quantum computing roet in het eten kan gooien, maar ook hiertegen zijn inmiddels 'quantumproof' algoritmes op de markt.

Reinier van der Drift is co-founder van Tymlez. Sinds midden jaren '90 heeft Reinier zich toegelegd op sterke authenticatie en identity management. In 2015 verkocht hij zijn softwarebedrijf Authasas aan het Engelse beursgenoteerde Microfocus. Sindsdien houdt Reinier zich bezig met Tymlez, een bedrijf dat een enterprise ready blockchain development platform ontwikkelt en op de markt brengt. Reinier is bereikbaar via reinier.vanderdrift@tymlez.com.



sign("Hello World", User 's private key) = n67n54n6l10xf15
sign("Hello World!", User's private key) = vk34jxl140501025

verify("n67n54n6l10xf15", "Hello World", User 's public key) = valid or invalid

Consensusprotocollen

De integriteit en het onderhoud van blockchains wordt gedaan door consensusprotocollen. Er zijn verschillende consensusprotocollen en naast het eerder aangehaalde 'proof of work'-protocol, zijn de twee belangrijkste 'proof of stake' en 'majority voting'. Het concept van consensusprotocollen in computernetwerken is niet nieuw. De inmiddels bijna vijftig jaar oude Boeing 747 heeft vijf boordcomputers die elk individueel de koersbewegingen van de piloot analyseren en via een 'majority voting' consensusprotocol tot overeenstemming komen alvorens de koersbeweging wordt ingezet. De consensusprotocollen kunnen per use-case verschillen. De protocollen zorgen ervoor dat de transacties worden gevalideerd en bijgeschreven in de blockchain. In het geval van cryptocurrencies wordt dat gedaan door zogenaamde miners. Miners zetten daarvoor hun krachtige computers in, wat geld kost natuurlijk. Via een loterijsysteem, wordt een pool van miners gevraagd om een cryptografische puzzel op te lossen. Voor hun diensten worden zij betaald in de betreffende currency, die ze vervolgens kunnen verhandelen.

Mining

'Mining' is een gedistribueerd consensussysteem dat wordt gebruikt om transacties in de blockchain op te nemen. Het dwingt een chronologische volgorde in de blockchain af, beschermt de neutraliteit van het netwerk, en maakt het mogelijk dat verschillende computers overeenstemming bereiken over de toestand van het systeem. Om te worden bevestigd, moeten de transacties worden verpakt in een blok dat aan zeer strikte cryptografische regels moet voldoen die door het netwerk worden gecontroleerd. Deze regels voorkomen dat voorgaande blokken kunnen worden gewijzigd, omdat daarmee alle volgende blokken ongeldig zouden worden. 'Mining' creëert ook het equivalent van een concurrerende loterij en verhindert daarmee dat een individu zelf nieuwe blokken kan laten opnemen in de blockchain. Op deze manier kan een individu geen controle krijgen over wat wordt opgenomen in de blockchain of delen van de blockchain vervangen om de eigen transactie terug te draaien.

Dus wat is de blockchain?

Een nieuwe vorm van informatietechnologie, een gedecentraliseerd systeem van 'checks and balances', een infrastructuur, een organisatiesysteem dat universeel is en op wereldschaal [3].

Wat kunnen we met blockchain-technologie?

Zoals eerder gezegd, richt blockchain-technologie zich primair op het elimineren van de Trusted Third Party. Het is een peer-to-peer technologie die de TTP uitsluit. Daardoor kunnen (business)processen opnieuw worden ingericht en kan een grote mate van efficiency bereikt worden. Een goed voorbeeld daarvan is de financiële sector.
Jan wil graag €100 overmaken naar Piet. Op dit moment loopt dat via de bank die, als TTP, de feitelijke transactie namens partijen uitvoert en daarvoor betaald krijgt. In geval van blockchain-technologie is de uitkomst nog steeds dat Jan €100 overmaakt aan Piet, maar de hele keten van banken en correspondent banken wordt uitgesloten. Jan maakt rechtstreeks het geld van zijn wallet over naar die van Piet. Voor de bank betekent dit dat zij haar directe invloed op de klant kwijtraakt. Zij weet niet alles meer over haar klant en daarmee wordt zij in het hart geraakt van haar businessmodel.

Als men kijkt naar de basisfunctionaliteit van blockchain-technologie dan zijn dit drie functies:

1. Data logging
2. Smart contract
3. Digitaal eigenaarschap

Met deze drie functionaliteiten kan men in de business processen herdefiniëren en –inrichten.

http://www.amazon.com/Bitcoin-Blueprint-New-World-Currencey/dp/1491920491

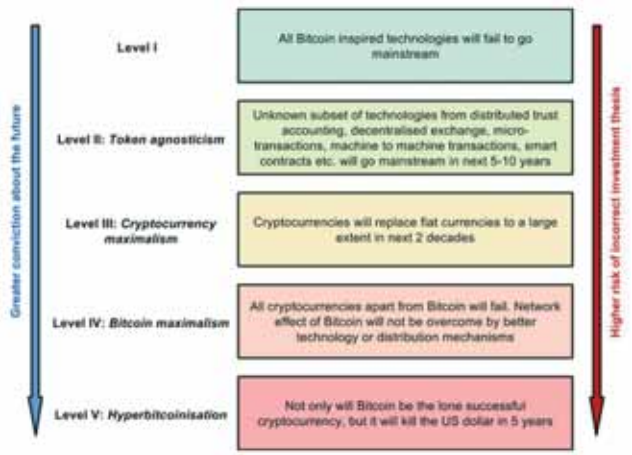
Business processen

Het grootste voordeel komt te liggen bij de gebruiker. Hij krijgt de controle. Hij gaat bepalen aan wie, waarvoor, wanneer en voor hoelang hij data beschikbaar gaat stellen. Dat gaat huidige businessmodellen volledig op zijn kop zetten. De Facebooks en Googles van deze wereld kunnen hun borst nat maken. Maar ook bedrijven als Microsoft en SAP moeten zich achter de oren gaan krabben. Disruptie gaat nu eenmaal

gepaard met snelheid van handelen. Voor je het weet ben je je marktpositie kwijt.

Toekomst

Hoe gaat de toekomst eruitzien en wat kunnen we op korte en langere termijn verwachten?
Meher Roy [4], een ingenieur bij Novartis, heeft een model waarin hij vijf niveaus heeft uitgewerkt waarlangs de crypto-kolonisatie van de maatschappij zich zou kunnen voltrekken.



Niveaus crypto-kolonisatie (Meher Roy)

Op dit moment focust de ontwikkeling zich op niveau 2 & 3. Er wordt behoorlijk geïnvesteerd door overheden, banken en venture capital-maatschappijen om deze niveaus te bereiken. Het andere model van Roy plaatst de vijf niveaus in perspectief van technologie en risico's.

Belief / bet	Platform opportunities	Incremental risk	Advantages
Level I	Not Applicable	Not Applicable	Not Applicable
Token agnosticism	Hyperledger, Eris, Codius, Ripple / Stellar	-Lack of solutions for identity and Private Key management -Regulatory uncertainty resulting from end-users controlling transactions -Platform specific flaws like weak consensus algorithm	-Applicable to all assets including fiat money, shares and cryptocurrencies -Can replicate all applications pioneered by cryptocurrency community -Relative compatibility with existing regulations
Cryptocurrency maximalism	Bitcoin, Ethereum, Tendermint, Pebble, Ripple / Stellar (partially) etc.	-Societal inertia to new forms of value holds massive network effect -System that possesses sound monetary policy and consensus method, fast transaction speed and is scalable appears late -Associated political ideologies prevent mainstream growth	-Market segment dissatisfied with conventional banking system is a ready market -Significant public interest for the time being
Bitcoin maximalism	Sidechains	-New technologies that improve on network maintenance cost, transaction speed and scalability outcompete Bitcoin	-Significant first mover advantage for Bitcoin
Hyperbitcoinisation	Not Applicable	-Opinion proves to be a delusion	-None

Technologiën en risico's (Meher Roy)

Dus het korte termijnperspectief ligt bij de permissioned blockchain, terwijl maximalisatie van cryptocurrencies op langere termijn wordt voorzien.

De blockchain als concept zal disruptief blijken voor veel bestaande business-modellen

Conclusie

De blockchain als concept zal disruptief blijken voor veel bestaande businessmodellen. Trust gaat op een nieuwe manier georganiseerd worden. Voor de ICT-community gaan spannende en interessante tijden aanbreken. Welke reuzen gaan ten onder en welke nieuwe toekomstige giganten gaan opstaan? Het begint bij het ontdekken van de mogelijkheden van deze technologie. En juist daarom worden er nu zoveel pilots en PoC's gedaan met blockchain. Welke keuzes gaat u maken?

Referenties

[1] www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business?language=nl
[2] http://a16z.com/2016/12/16/the-end-of-cloud-computing/
[3] www.melanieswan.com/documents/BlockchainThinking_SWAN.pdf
[4] https://medium.com/@Meher/a-model-to-makes-sense-of-beliefs-and-associated-crypto-finance-platforms-f761a7d782cb#.qdj2kwp4x

Links

Explaining Bitcoin Mining: https://youtu.be/iyq4od8MBoE
De blockchain uitgelegd: https://youtu.be/gKC2oelL878
De blockchain is eating Wall Street (TED Talk Alex Tapscott)_: https://youtu.be/WnEYakUxsHU
Website van Melanie Swan: www.melanieswan.com
State of the blockchain: http://www.coindesk.com/research/state-of-blockchain-q3-2016/
EB84 – Tim Swanson: Permissioned Ledgers And The Case For Blockchains Without Bitcoin : https://youtu.be/k3pM8vB2QYc

ALLES WAT JE MOET WETEN OVER BLOCKCHAIN

Met de opkomst van de Bitcoin hoor je ook vaak het woord 'blockchain' vallen. Maar wat is het nu precies en vooral: wat moet je er als professional op het gebied van informatiebeveiliging mee? Héél kortgezegd is een blockchain een digitaal grootboek, meest bekend door de toepassing in het digitale betalingssysteem Bitcoin om de transacties en saldo's te valideren. Blockchains kun je daarnaast ook gebruiken om zaken te registreren zoals eigendom, licenties en identiteit. Zet je die in een blockchain dan is de registratie automatisch decentraal, geauthentiseerd en publiek verifieerbaar. Een voorbeeld dat goed geregeld kan worden in een blockchain is een audit trail; een controlespoor waarmee ondernemingen hun transacties administratief volgen en controleren. In een blockchain gaat dat automatisch én gevalideerd. Het enige waar ze dan nog voor moeten zorgen, is goede rapportage. Eigenlijk alles dat voor een mens waarde heeft, waarvan kenmerken vastgelegd kunnen worden en van aanbieder naar afnemer 'getransporteerd' kan worden, kan in een blockchain geregistreerd worden.

Op dit moment gebruikt de financiële sector blockchain het meest. In 2016 investeerde deze sector één miljard dollar in de technologie [2]. Financiële dienstverleners experimenteren met blockchain-oplossingen voor het verwerken van transacties waarbij diverse financiële instrumenten zijn betrokken. Het World Economic Forum sprak recentelijk de verwachting uit dat in 2017 tachtig procent van alle banken zich bezig zullen houden met blockchain-projecten [3]. NASDAQ Linq gebruikt bijvoorbeeld blockchain voor het registreren, verwerken en afhandelen van particuliere effectentransacties [4].
Blockchain wordt op dit moment dus gebruikt bij Bitcoin en 'gewone' financiële transacties, maar voor welke sectoren is het nog meer interessant? Er wordt onderzoek gedaan naar het gebruik in de zorg zoals medische dossiers en meetdata versleuteld in de blockchain opslaan, waarbij patiënten zelf de gegevens kunnen ontsluiten. Maar: hoe komt de zorgverlener bij het dossier als de patiënt zelf geen toegang kan verlenen, bijvoorbeeld vanwege zijn medische toestand?
Blockchain is interessant voor sectoren met veel tussenpersonen, specialisten, administratieve handelingen, hoge onzekerheid, complexiteit en hoge transactiekosten. Grote hoeveelheden data verwerken, is nog een probleem: blockchain repliceert de hele boekhouding, waardoor alle data meerdere malen in de keten bewaard worden. Je opslagmogelijkheden moeten dat aankunnen. Daarnaast is een blockchain nu nog niet efficiënt doorzoekbaar. Op dit moment zijn het juist de sectoren met weinig transacties maar wel een uitgebreide keten met veel verschillende bedrijven die blockchain gebruiken. Denk aan de verkoop van onroerend goed, waarbij een makelaar betrokken is, de daaraan gekoppelde leningen bij de bank afgenomen worden, de registratie bij het Kadaster uitgevoerd wordt en De Nederlandsche Bank de controle op financiële zaken doet. Ondertussen zijn overheden bezig met blockchain-proefprojecten bij kadastrale processen en het eigendom van percelen. Dit is vooral een probleem in ontwikkelingslanden, waar vaak sprake is van onvolwassen instellingen en corruptie aan de orde van de dag is. Niet-gouvernementele organisaties gebruiken blockchain om donateurs inzicht te geven in waar en hoe hun geld gebruikt wordt. Passend, want hier is transparantie, hét grote kenmerk van blockchain, erg belangrijk voor donateurs. Tot slot gebruikt het transnationale identiteitssysteem e-Residency in Estland een blockchain-systeem om dossiers te beheren die deelnemers moeten kunnen inzien.
En denk voor andere blockchain-mogelijkheden bijvoorbeeld aan supply chain management in de industriële sector; iedere supply chain kan met blockchain transparant gemaakt worden. Of bijvoorbeeld het eigenaarschap en de afkomst vastleggen van kunst, goud en diamanten. Of een boek kopen of een reis boeken via een online winkel.

Is een blockchain té transparant?

Blockchains werken decentraal en zijn verifieerbaar voor eenieder die de keten kan lezen. Die transparantie is een grote kracht van het systeem. Maar eenmaal opgeslagen informatie, zoals de transactiedata of logdata, is achteraf niet meer aan te passen, omdat de keten dan zou breken. Een eerder gemaakte fout, gecorrigeerd in een later blok, blijft dus altijd zichtbaar in de blokken uit het verleden, waar die fout is vastgelegd. Blockchain gaat dus in principe niet samen met privacy. Informatie kan versleuteld opgeslagen worden in de blockchain. Alle encryptie heeft een houdbaarheidsdatum, wat twee problemen geeft: cryptoanalyse of een brute-force aanval zal de informatie ooit ontsluiten.
Daarom werken Bitcoin-betalingen bijvoorbeeld met een pseudo-anonieme identiteit, het adres van jouw wallet. Anderen zien nog steeds wel welk bedrag er verhandeld is, alleen ze weten niet van wie naar wie het is gegaan. Iedereen kan in de Bitcoin-blockchain zien dat er een transactie is gedaan tussen twee wallets, maar niet van wie die wallets zijn. Je moet de identiteiten achter de adressen kennen om te weten wie de Bitcoins heeft. Helemaal privé is het nog niet, als jij weet naar welke wallet je op zoek bent, zijn alle transacties zo gevonden. Een andere oplossing daarvoor die vooral in de financiële wereld wordt bekeken, is een samenspel tussen off-chain data die on-chain een tijdsstempel krijgt. Hier worden privacygevoelige data in hash-vorm opgeslagen op de blockchain, waardoor de informatie alleen bekend is bij de partijen met een rol in de transactie. R3's Corda loopt hierbij voorop [5]. Ook Digital Assets Holding met haar Global Synchronization Log [6], en het Hyperledger project [7] kijken naar vergelijkbare oplossingen om zowel het privacyprobleem als het schaalbaarheidsprobleem op te lossen.

Chantal Craandijk is via Craandijk Communicatie onder andere werkzaam als interviewer en is bereikbaar via www.craandijk.com. Lex Borger is hoofdredacteur informatiebeveiliging, security consultant bij i-toi en docent scurity aan de Hogeschool Utrecht. Lex is te bereiken via l.borger@i-to-i.nl.

Bitcoin

Mensen die Bitcoins gebruiken, zijn afhankelijk van een decentraal netwerk van blockchainservers die elk een kopie van het grootboek beheren en waarin iedereen elkaars overboekingen kan zien. Om Bitcoins te kunnen gebruiken, installeer je een programma op je computer. 'Bitcoin Core' is het originele programma, er bestaan meerdere clients [1]. Het programma beheert een portemonnee (wallet), wat in feite niets anders is dan een asymmetrisch sleutelpaar. De client is een sleutelbeheerder waarmee transacties vanuit de wallet getekend kunnen worden. De privésleutel geeft toegang tot de wallet en de publieke sleutel is het adres van de wallet. Omdat de Bitcoin-blockchain openbaar is, kan iedereen controleren wat het saldo is van de betalende wallet.
Het wallet-programma stuurt een transactie tussen twee wallets in en valideert die. Daarna wordt de transactie bij het eerstvolgende acceptatiemoment opgenomen in de blockchain. Acceptatiemomenten ontstaan wanneer een validator, ook wel Bitcoin-miner genoemd, als eerste een complexe cryptografische puzzel oplost en daarmee 'proof-of-work' levert. Deze miner bezit hiermee de volgende cryptografische sleutel voor het volgende blok, checkt alle uitstaande transacties (bijvoorbeeld of een Bitcoin niet twee keer uitgegeven wordt), voegt zijn beloning toe (op dit moment 12,5 Bitcoin) en neemt deze op in de administratie door een schakel toe te voegen en dit aan de andere servers te melden. Elke andere blockchainserver controleert het block en accepteert het als de miner zijn werk goed gedaan heeft. In deze fase kunnen verschillen ontstaan, omdat er meerdere miners zijn met een oplossing. Blockchain-servers dienen er ook op te letten dat er geen langere ketens bestaan dan wat zij hebben, anders moeten ze transacties terugdraaien en overgaan en de langere keten volgen. Zo kunnen er 'orphan-blocks' ontstaan, maar collectieve consensus wordt snel gevonden. Als een block is opgenomen in de langste keten is de beloning van de miner een feit en het block een onderdeel van de blockchain. De transacties zijn nu vastgelegd en zijn daarmee een deel van de blockchain-historie van Bitcoin-transacties, die helemaal teruggaat tot het ontstaansmoment in 2009.

Public, private en permissioned blockchains

Publieke blockchains zijn op zijn best pseudo-anoniem; je bent hier nooit honderd procent anoniem. Het is ook mogelijk om de blockchain uit het publieke domein te halen. Naast publieke blockchains zijn er ook private blockchains. Deze draaien op bijvoorbeeld de infrastructuur van een bedrijf, achter de firewall [8]. Toegangsbeveiliging zorgt ervoor dat alleen geautoriseerde gebruikers toegang hebben om te lezen en aan te passen. Dit heeft nog steeds voordelen boven traditionele databases, bijvoorbeeld binnen de context van een decentraal geleid bedrijf of federatie, of om transparant compliance aan te tonen. Deze blockchains zijn geschikter voor privacygevoelige gegevens. Belangrijk, want het nadeel van volledige transparantie is natuurlijk het delen van gegevens met partijen waarmee je die niet zou willen delen.
Er is nog een ander risico met een public blockchain: een onderliggende aanname is dat er een publiek consensusmodel is, waarbij het volgende blok pas geaccepteerd wordt als er consensus bereikt is. Wat als de meerderheid van alle boekhouders onder de invloed van één marktpartij valt? Dit geeft een validatiemonopolie. Onder zo'n monopolie zou deze partij met zijn stemkracht direct kunnen beïnvloeden welke blokken toegevoegd worden aan de blockchain. Eén oplossing hiervoor is de 'permissioned' blockchain, waarbij in de blockchainregels is opgenomen dat een groep aangewezen validators de controlemacht verspreid houdt [9][10].
Of een blockchain public, permissioned of private moet zijn, zal altijd een aandachtspunt zijn. Je wil als overheid bijvoorbeeld niet dat iedereen zich ongelimiteerd aan de DigiD-blockchain aansluit, waardoor de DigiD-blockchain een permissioned blockchain zal moeten zijn.

Hoe veilig is blockchain?

De integriteit van de blockchain blijft in stand met hashing en elektronisch ondertekenen. Die bescherming is afdoende totdat een aanvaller de encryptie kraakt. Dat zal altijd een kat-en-muisspel blijven.
Crypto wordt standaard eens in zoveel tijd gebroken. Dat was voorheen met MD5, en op dit moment met SHA1. Ook sleutellengtes zijn belangrijk. Vroeger zaten we met 512 bits en inmiddels zitten we minimaal op 2.048 bits. Als kwantumcomputers in de toekomst RSA2048 kunnen breken dan kunnen private keys berekend worden uit de public keys en ligt dus de inhoud van elke Bitcoin-wallet voor het grijpen. Als SHA256 breekbaar is, zijn alle hashes van de daarop gebaseerde blockchains volledig herschrijfbaar en valt het hele

Blockchain: 'I see what you see, you see what I see, and I know that you see what I see'

vertrouwen in de blockchain weg. Wat we hieraan kunnen doen, is methodes ontwikkelen die de encryptiealgoritmen in de blockchain op een transparante manier kunnen versterken of vervangen. Zo zal blockchain beter bestand zijn tegen de nieuwe rekenkracht van kwantumcomputers. Dit maakt het mogelijk weer minder schaalbaar.

Ook het publieke karakter maakt beveiligen moeilijk. Zo kan de FBI of de NSA met veel financiële middelen en andere bronnen een identiteit achterhalen, ook op een blockchain. Ga je ervan uit dat je een server in de cloud niet kunt vertrouwen, dan kun je aan encryptie denken. De privacy kun je ook in een blockchain beter borgen met attribute-based concepten zoals Enigma en Sieve dat doen.

Enigma is een project van het Massachusetts Institute of Technology (MIT) [11]. Het is een gedecentraliseerd cloud-platform met gegarandeerde privacy. Met Enigma kunnen ontwikkelaars bijvoorbeeld peer-to-peer applicaties maken die gebaseerd zijn op privacy by design, of blockchain by design. Hierdoor hoeven ze geen trusted third party te gebruiken. Ze kunnen bewerkingen uitvoeren op data, zonder er toegang toe te hebben. Persoonsgegevens worden opgeslagen, gedeeld en geanalyseerd zonder de identiteit van de 'verzender' te hoeven prijsgeven.

Het MIT en Harvard University ontwikkelden het cryptografische

systeem Sieve [12][13] om beter grip te krijgen op encrypted data in de cloud. Applicaties die toegang willen tot je persoonlijke data moeten jou daarvoor expliciete toestemming vragen. Krijgen ze die dan ontvangt de applicatie een sleutel tot een specifiek attribuut of bepaalde data. Weiger je, dan wordt de sleutels opnieuw versleuteld. Dit is echter niet direct toepasbaar in een blockchain, die juist niet veranderd kan worden.
Het overzicht en de transparantie van blockchain en diens onveranderlijke en onuitwisbare karakter zijn belangrijke pluspunten. Maar een organisatie wil misschien niet dat concurrenten of leveranciers al haar transacties kunnen volgen. Dit probleem kan dan worden opgelost door voor elke transactie een nieuwe encryptiesleutel te gebruiken, maar dat gaat dan wel ten koste van de efficiëntie. En, heel belangrijk, heeft iemand ooit toegang gekregen tot versleutelde data dan is dat niet meer in te trekken. Iemand die ooit een sleutel had, blijft toegang houden…

Schaalbaarheid en snelheid

Eén van de grootste zorgen over blockchain is schaalbaarheid. Het vergt veel rekenkracht om een blockchain te verlengen. Ook kost het de nodige opslagcapaciteit, wat alleen maar zal toenemen, hoewel de kosten van opslagmedia met de dag dalen. Omdat het functioneren van een blockchain afhankelijk is van een partij die 'proof of work' levert wanneer uitbreiding nodig is, is het beperkt stuurbaar wanneer een registratie opgenomen kan worden in een blockchain. Kan het dan wel op grote schaal en snel toegepast worden? De techniek is complex. Er is een gebrek aan brede expertise met de ontwikkeling en beheer van blockchain en er is nog helemaal geen regelgeving.
Zoals gezegd is er veel rekenwerk nodig om proof of work te leveren. Voor Bitcoins is dit nu ongeveer zoveel als het elektriciteitsgebruik van Guatamala [14]. Dit is niet efficiënt. Het is echter niet het enige consensusalgoritme dat in gebruik is. Er is een ander, efficiënter, consensusalgoritme; 'proof of stake'. In dit geval leggen de nodes een waarde in om te bewijzen dat ze een aandeelhouder zijn in de blockchain en dus belang hebben bij het goed functioneren ervan. Afhankelijk van de grootte van het aandeel wijst het consensusalgoritme de volgende validator aan. Iemand met een groot aandeel maakt dus meer kans.
En hoe zit het met de transactiesnelheid, een andere grote zorg? Creditcardmaatschappij VISA kan bijvoorbeeld bijna 56 duizend transacties per seconde verwerken [15]. Het Bitcoin-platform kan twee tot drie transacties per seconde aan, Ethereum tienduizend en Tymlez kan in een private blockchain honderdduizend transacties per seconde halen. We staan echter nog in de kinderschoenen. Blokken bevatten meerdere transacties. Bij de ontwikkeling van een consensus-mechanisme moet er een afweging gemaakt worden tussen robuustheid en snelheid. Echt inzichtelijk worden schaalbaarheidsproblemen pas als er grotere blockchain-proefprojecten worden uitgevoerd.
Door de al eerdergenoemde off-chain opslagtechniek te gebruiken, kunnen veel hogere transactiesnelheden gehaald worden. Een voorbeeld hierbij is het Raiden Network van Ethereum [16].
Veel analisten zijn van mening dat blockchain op dit moment hyperscale, real-time transactieplatforms niet zal vervangen. Grote onzekerheid is er nu nog over het veiligheidsgehalte van blockchain en over het gevaar van hackers. Steeds meer ontwikkelaars maken applicaties, waardoor de applicatielaag kwetsbaar wordt, wat weer hackers kan aantrekken – als die niet al zijn komen kijken door de groeiende transactievolumes en de daarbij behorende toenemende economische waarde.
Blockchain biedt in grote lijnen wel een oplossing voor beveiligingsproblemen, toch zullen de nieuwe aanvalsoppervlakken ook weer nieuwe vragen creëren. Netwerkapparatuurmaker Juniper volgt daarom de ontwikkelingen op de voet om de integriteit van data tijdens de overdracht en gegevens binnen de applicatielaag te waarborgen. Andere obstakels voor blockchain liggen in onvoldoende gebruiksgemak, weerstand van partijen wiens businessmodel te lijden heeft onder het succes van blockchain, zoals intermediairs.

De toekomst

Het internet had in zijn begindagen met grotendeels vergelijkbare problemen te kampen. Een van de redenen voor de explosieve groei van het internetgebruik is dat het internet een in hoge mate decentraal fenomeen is waarop nog altijd relatief weinig toezicht wordt gehouden. Blockchain is nog decentraler dan het internet en krijgt in de toekomst dan ook vergelijkbare problemen. Waar de toepassing van e-mail nodig was voor de ontwikkeling van internet en het TCP/IP-protocol, is het gebruik door Bitcoin dat voor blockchain. Er zal daarom een blockchain-protocol komen dat de financiële wereld, overheid, high-tech industrie én gebruikersgroepen breed moeten dragen. Wereldwijde coördinatie en regelgeving zijn moeilijk realiseerbaar, zo niet onmogelijk. Overheden en wetshandhavers zullen de grootste moeite blijven hebben om zicht te houden op cryptovaluta en ander publieke blockchain-technologieën die in sommige gevallen illegale activiteiten mogelijk maken.
De territoriale soevereiniteit van data is een ernstig probleem. Veel rechtsgebieden zoals China en Europa hebben

regelgeving ontwikkeld die voorschrijft waar data moet worden opgeslagen. In de cloud kan de locatie van data diffuus zijn, maar bij blockchains dat nog moeilijker te bepalen. De informatie kan zich in feite overal binnen een verspreid grootboeksysteem bevinden. Er zal een shake-out plaatsvinden, waarna er een aantal varianten over blijven met ieder een eigen specialisatie.

De blockchain-strategie draait fundamenteel om samenwerking en niet om concurrentie. Omdat interoperabiliteit van cruciaal belang is voor blockchains, zullen open source-initiatieven daar een belangrijke rol gaan spelen. Private blockchains vragen om een bepaalde mate van standaardisatie en overeenstemming tussen de deelnemende partijen. Goed gedocumenteerde, gestandaardiseerde koppelingen tussen uiteenlopende systemen zullen bijdragen aan een bredere toepassing van blockchains; een gebrek daaraan zal de groei in de weg zitten.

Aan blockchain zitten te veel voordelen verbonden om er zomaar aan voorbij te gaan. De technologie heeft de potentie om voor ingrijpende maatschappelijke veranderingen te zorgen. Het kan bijdragen aan een toekomst waarin applicaties zelfstandig met elkaar communiceren om aantrekkelijke megaservices te creëren die de kwaliteit van ons leven verbeteren. Veel mensen zien de opkomst van blockchain als een belangrijke nieuwe stap in de ontwikkeling van het internet, waarbij we afstevenen op het 'internet of value'. Om de voordelen van blockchain optimaal te kunnen benutten, moeten bedrijven en brancheorganisaties hun krachten bundelen en zorgen voor de complexe coördinatie voor de aanvankelijke inrichting van de nieuwe operationele modellen. Worden de belanghebbende partijen het niet eens over de details en gaan ze niet samenwerken dan krijgt de technologie geen voet aan de grond.

Blockchain bezit een ongekend potentieel om wrijving binnen toevoerketens tegen te gaan, een einde te maken aan de noodzaak van intermediairs en het overzicht en de beveiliging te verbeteren. De technologie biedt de mogelijkheid om met geautomatiseerde contracten te werken, en zou daarmee weleens de fundamentele aard van bedrijven en de relatie tussen werknemers, klanten en leveranciers op zijn kop kunnen zetten. Blockchain is een van de vele nieuwe technologieën die de groei van de 'gig economy' van zzp'ers en economie van delen kunnen bevorderen door een einde te maken aan de administratieve rompslomp tussen partijen. Het zal wel nog jaren duren voordat blockchain-technologie voor ingrijpende maatschappelijke veranderingen zorgt. En kan pas echt een succes worden als organisaties elkaar vertrouwen en intensief samenwerken: 'I see what you see, you see what I see, and I know that you see what I see'. En dat is oké.

Links

[1] Suraya Zainudin, 14 Best Bitcoin Wallets For Secure Bitcoin Storage: www.hongkiat.com/blog/bitcoin-wallets

[2] Declan Harty, Finance Firms Seen Investing $1 Billion in Blockchain This Year, Bloomberg: http://bloom.bg/2lqfm0h

[3] The future of financial infrastructure, World Economic Forum: http://bit.ly/2aObRdV

[4] Building on the Blockchain, Nasdaq: http://bit.ly/2gvHvUP

[5] Richard Gendal Brown, Introducing R3 Corda: A Distributed Ledger Designed for Financial Services: http://bit.ly/2lLtbcq

[6] The Global Synchronization Log, Digital Asset: http://bit.ly/2m1LTxj

[7] Hyperledger: https://www.hyperledger.org

[8] Alan Morrison, Blockchain and smart contract automation: Private blockchains, public, or both?, PwC: http://pwc.to/2lWP09f

[9] Nick Williamson, Permissionless vs Permissioned Consensus & Tradeoffs, Credits: http://bit.ly/2lq7CeL

[10] Why Blockchain Consensus Mechanisms Matter, The Intrepid Review: http://bit.ly/2lWUBw9

[11] MIT's Bitcoin-Inspired 'Enigma' Lets Computers Mine Encrypted Data, Wired: http://bit.ly/2m1xX6l

[12] James Mickens, Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds, Harvard University: http://bit.ly/2lq9S5v

[13] Secure, user-controlled data, MIT News: http://bit.ly/1q2lFb0

[14] Bitcoin Energy Consumption Index: http://digiconomist.net/beci

[15] Visa Inc. at a Glance: http://vi.sa/2muTgur

[16] Raiden Network, Payment-Channel Network for Ethereum: http://raiden.network

De input van dit artikel is tot stand gekomen via een Delphi-proces. Bij deze onderzoeksmethode, genoemd naar het orakel van Delphi, wordt een groot aantal experts om hun mening over een bepaald onderwerp gevraagd. Door de antwoorden van de andere experts anoniem terug te koppelen, wordt in een aantal rondes geprobeerd tot consensus te komen. Daarna zijn deze antwoorden gebundeld en herschreven tot een artikel. De experts hebben de eindversie uiteraard geaccordeerd. Onze hartelijke dank aan (in alfabetische volgorde) Paul Bessems, Weconet Blockchain Technologies, Reinier van der Drift, Tymlez :reinier.vanderdrift@tymlez.com, Yurry Hendriks, ABN-AMRO Bank (yurry.hendriks@nl.abnamro.com, Jeroen van Hoof, PwC (jeroen.b.van.hoof@nl.pwc.com), Paul Obsitnik, Juniper Networks (Twitter @pobsitnik), Marjan van der Plas, ABN-AMRO Bank (marjan.van.der.plas@nl.abnamro.com), Harld Röling (harld.roling@h.roling.nl) en anderen voor hun medewerking.

0-DAY AANVALLEN OP DE BLOCKCHAIN

Blockchain is niet meer weg te denken bij de huidige innovatieve trajecten binnen onder andere de overheid, zorg en financiële sector. Blockchain is een techniek waar velen hun heil in zien en wordt een basis om een aantal problemen op te lossen. Bijvoorbeeld problemen die we zien bij centrale toepassingen die we decentraal willen inzetten. Deze worden beheerd door één organisatie en gebruikt door meerdere organisaties. Overheid zou bijvoorbeeld een blockchain-omgeving voor identiteiten (soort van DigiD) kunnen outsourcen zonder dat ze de controle verliezen over het beheer van de identiteiten. Meerdere servers bij diverse organisaties die dan de identiteit van de burgers kunnen vaststellen, maar de identiteiten worden door de overheid beheerd. De basis van deze blockchain-omgeving ligt bij de overheid en de overheid houdt de controle.

Met dat laatste heb ik gelijk de basis te pakken van de problemen die kunnen ontstaan als je nu een blockchain-omgeving neerzet die tien tot vijftien jaar gaat draaien. De techniek is nog nieuw en niet volwassen genoeg om in te zetten voor systemen die langer dan vijf jaar mee moeten gaan. Waarom, dat heeft mede te maken met lekken in de hardware, software, gebruikte algoritmes en de mogelijkheid deze op te lossen. De standaard 0-day lekken van deze wereld.
Een voorbeeld uit het verleden zijn de Root CA's en de daarbij gebruikte sleutellengtes, algoritmes en levensduur. De 512 bits sleutels en het MD5 algoritme waren vroeger goed, maar worden tegenwoordig niet meer als veilig gezien, Alle Root CA's die 512 bits sleutels en/of MD5 bevatten, zijn uit de Root CA Trust lijsten gehaald. Terwijl er Root CA's bijzitten die nu nog steeds een geldige einddatum hebben.

Aanvallen op de software

In de software is al sinds jaar en dag bekend dat elk systeem weleens een lek heeft. Lekken in software, data verlies, beschikbaarheid van systemen en andere problemen komen bij alle organisaties voor. Meestal zonder veel problemen maar soms, helaas, met het lekken van grote hoeveelheid zeer gevoelige gegevens. Bijvoorbeeld het lekken van gebruikers en versleutelde wachtwoorden van Yahoo en LinkedIn.
De techniek van de blockchain kun je verdelen in een aantal onderdelen. De belangrijkste zijn: software, hardware, identificatie (gebruikers, IAM) en de gebruikte encryptie algoritmes. Op alle lagen kunnen lekken worden gevonden en moet er een oplossing doorgevoerd worden. Bij de software kun je updates doorvoeren en gebruikers zijn te verwijderen, al dan niet binnen een korte tijd. Bij lekken van gebruikersgegevens, kunnen deze geblokkeerd of gereset worden. Bij een hardwareprobleem is het vaak wat moeizamer maar niet onmogelijk om deze ook op te lossen. De 0-day lekken, en de daarbij gepaarde eventuele aanvallen, zijn dan op een standaard manier te detecteren en tegen te gaan. Voor encryptie algoritmes is dat een ander verhaal en heeft het meer impact voor een blockchain.

Aanvallen op het algoritme

Bij blockchains zijn verschillende algoritmes vereist om authenticatie, versleuteling en signing door te voeren. Voor authenticatie wordt vaak asymmetrische encryptie (bijvoorbeeld RSA of ECC) gebruikt, versleutelen wordt met symmetrische encryptie (bijvoorbeeld AES) gedaan en voor signing is een hashing algoritme (zoals SHA256) nodig.
Sleutellengte is een belangrijk onderdeel bij het gebruik van de encryptiealgoritmes. Langere sleutels worden vaak gezien als veilig en toekomstvast. Op dit moment worden RSA met 2048 bits lengte, AES256 en SHA256 als veilig beschouwd.
Over tien tot vijftien jaar is de wereld heel anders dan nu en moet je rekening houden met compleet nieuwe technieken zoals kwantum computers. Van de kwantum computers weten we nu al dat deze de asymmetrische encryptie algoritmes kunnen breken. Bij foutvrije kwantum computers van vijftig QuBits is het al mogelijk om RSA te kraken. Er bestaan nu al kwantum computers van twintig QuBits. Al zijn deze kwantum computers nog niet foutvrij.
Naast de kwantum computers is het kraken van een algoritme ook op huidige machines een mogelijkheid. In het verleden hebben we dat gezien bij de voorloper van SHA1, het MD5 algoritme. Maar ook RSA met sleutels die kleiner zijn dan 1024 bits zijn met de huidige systemen niet meer veilig.
Bij een 0-day lek op een algoritme is dan niet meer de vraag óf dat gebeurd, maar meer wannéér deze in praktijk ontdekt gaat worden! Dat kan weleens eerder zijn dan we nu denken en ik vermoed dat dit tussen 2020 en 2025 op asymmetrisch algoritmes uitgevoerd wordt. Dat is al met drie tot acht jaar.
Met deze wetenschap is het ontwikkelen van een blockchain voor meer dan tien jaar een risico indien je deze opzet met de algoritmes zoals RSA of ECC. Bij het ontwikkelen van nieuwe

Harld Röling is werkzaam bij de afdeling CISO van een Nederlandse bank en heeft zich sinds 1999 gespecialiseerd in de technische en organisatorische aspecten van asymmetrisch Key Management en PKI. Daarnaast is Harld vrijwilliger bij Bits of Freedom voor de Privacy Cafe's en de Toolbox. Harld is bereikbaar op e-mailadres harld.roling@hroling.nl.

De vraag die we zeker gaan krijgen en ook beantwoord moeten krijgen, is ‘wat zijn de gevolgen van een gekraakte blockchain omgeving?

blockchain-omgevingen moet je dus na gaan denken hoe je met 0-day aanvallen op de algoritmes omgaat.
Het on-the-fly veranderen van algoritme is een eis die je mee moet nemen voor het bouwen van de software van de blockchain. Een eis die nu nogal nieuw is en klinkt, maar met vijf jaar een standaard gaat worden. Lessons-learned uit het verleden is de basis voor een gedegen blockchain-omgeving.

Gevolgen van het kraken van de blockchain

De vraag die we zeker gaan krijgen en ook beantwoord moeten krijgen, is ‘wat zijn de gevolgen van een gekraakte blockchain omgeving?’. Een aantal scenario’s heb ik hierna beschreven.
Bij lekken op het level van de software en identificatie (IAM), is het in het ergste geval mogelijk om veranderingen aan te brengen en deze te laten tekenen door een sleutel van de blockchain. Gevolg is dat er een identificatie of transactie uitgevoerd kan worden waarvoor niemand een goedkeuring heeft gegeven. Een voorbeeld van wat kan gebeuren is de DAO-hack uit 2016. Toen is er een soort lek in het smartcontract misbruikt om miljoenen weg te sluizen naar derden. Dit was blockchain-technisch volkomen legaal en kon daardoor gewoon uitgevoerd worden.
Misbruik van lekken op hardware niveau is een stuk moeizamer. Hackers kunnen de blockchain uit de lucht halen, maar echt nieuwe transacties uitvoeren is een ander verhaal. Vaak worden lekken in hardware gebruikt als opstapje naar software om daar aanvallen uit te voeren. Daarnaast is de support voor hardware vaak maximaal vijf jaar en dan wordt deze niet meer door de leverancier ondersteund. Vervangen moet dus wel mogelijk zijn en wordt nu al veelvuldig uitgevoerd bij systemen die langer dan vijf jaar moeten draaien.
Het kraken van het algoritme is van hele andere aard. Hiermee kun je een al gesigneerde transactie veranderen en mogelijk smartcontract-acties opstarten. Ook dit zal het blockchain zien als legaal gebruik, want het is netjes digitaal ondertekend en voldoet technisch aan alle eisen. Als je een blockchain hebt opgezet waar identificatie en authenticatie (bijvoorbeeld DigiD) wordt bepaald, is het mogelijk om massaal identiteiten te misbruiken. Met DigiD zul je dan aanvragen bij Belastingdienst kunnen uitvoeren. Dit is een algemeen probleem dat op alle IAM-systemen van toepassing is, maar bij blockchain-omgevingen een hogere impact heeft.

Conclusie

Met de huidige technieken in algoritmes is het nog niet mogelijk een blockchain te bouwen die post kwantum compliant is. Een post-kwantum signing algoritme is nog niet beschikbaar, al zijn er wel ontwikkelingen gaande.
Een van de oplossingen om toch van start te gaan, is de omgeving zodanig te ontwikkelen dat de gebruikte algoritmes te vervangen zijn. Indien er dan een post-kwantum compliant algoritme beschikbaar komt, zal deze in een bestaande blockchain gebruikt kunnen gaan worden.
Met dit in het achterhoofd moet je dus goed nadenken over wat je met de blockchain wilt doen en voor hoelang deze in productie blijft draaien. Is dat minder dan vijf jaar, dan is het geen probleem deze neer te zetten en de techniek van blockchains verder te onderzoeken. Wil je iets neerzetten dat na 2025 nog moet draaien, dan is nadenken over het vervangen van de algoritmes een vereiste!
Tevens is het nodig na te denken of alle identiteiten of transacties in de blockchain opnieuw bepaald en ondertekend moeten worden. Wil je dat doen, dan is het een grote verandering in de huidige manier van denken over hoe een blockchain moet worden opgezet.
Al met al, is het opzetten van een goede blockchain niet iets wat je even snel kunt doorvoeren. Een team met gedegen kennis van blockchain en encryptie is een vereiste om een omgeving voor de lange termijn veilig neer te zetten.

TRACEABLY OWNED

Today's big buzzwords are 'blockchain' and Bitcoin, but the concept has been around since the 1990s. The Attributer himself in 1998 was consulting for one of the companies involved in the Bolero consortium, a project to digitise and dematerialise paper bills of lading (BoLs). A BoL is a negotiable financial instrument. Ownership of the bill means ownership of the cargo of a ship on the high seas. The bill is a 'document of title' that can change ownership during its lifecycle. The security issue with digital documents is that multiple copies are indistinguishable, being bit-for-bit replicas, unlike paper for which there is only one physical original. The scheme developed by The Attributer was based on a chain of interlocking digital signatures that secured and publically proved the entire history of the document. It is easy to get carried away with the cryptographic technology, but back 1998 The Attributer was applying SABSA thinking to determine the business requirements for a digitised BoL scheme. Here are the main principles that were the foundation for the 1998 work:

- An authorised, trusted party must be able to create an electronic document of title, such as a bill of lading, which holds real value that can be transferred from party to party.
- Other parties, who trust the creator to have created only valid electronic documents that have real value, must be able to view the document, to verify its contents and to verify its authenticity. They must be able to verify that a trusted originating party created it to be sure that it has the value that it purports to carry.
- The creator must be able to pass ownership to another party, who in turn may pass ownership to another, and so on indefinitely.
- At any stage in the ownership process, any interested party (who is authorised to so do) must be able to view the electronic document, verify its original authenticity, verify its history of ownership transfers and verify its present ownership.
- The security mechanisms used must be linked to the documents only, and must not be dependent in any on the methods used for communicating or storing these documents. The system should work with whatever data communications protocols and networks the various participants use. Security mechanisms embedded in network solutions will not meet the requirements.
- Whilst trust is obviously an important attribute associated with the creation of the original electronic document, the chain of trust from that point onwards should as much as possible rely on provably strong security mechanisms that cannot be easily subverted. In particular these security mechanisms should not rely on the trusted operation of computer systems by third parties where those systems cannot be secured to a 'provably secure' level.
  It is not just origin authentication and contents authentication that counts here. It's a question of current ownership. We need to have a means to establish the following criteria:
- Who created the electronic document? Are they someone we trust? Therefore do we believe that the document they created carries real value? Can we be sure that the document we are looking at is authentic and really came from that trusted party?
- Has the document remained unchanged in its substance since it was created? If there has been a bona fide need to enrich or change the document in any way during its lifetime, do we recognise the party doing the changes as authorised and trusted to do that? Can we verify the authenticity of the changes, both in terms of origin and content?
- Who owns the document NOW? When someone represents him/herself as the rightful owner of the electronic document, and hence as the owner of the value that it carries, can we be sure that they are telling the truth?

This is where the SABSA thinking is important. Getting the business requirements right is what leads to a successful technology model that can truly support the business application.

The Attributer

Interview Aart Jochem

VAN HIT&RUN NAAR AANVALLEN DOOR BEROEPS-CRIMINELEN

"We hebben als security professionals meer en meer te maken met beroepscriminelen." Het is de waarschuwing die Aart Jochem geeft wanneer we hem vragen naar de belangrijkste ontwikkelingen op het gebied van cybersecurity in de afgelopen tien jaar. Tien jaar waarin hij eerst bij GovCERT en sinds 2012 bij het Nationaal Cyber Security Center (NCSC) mede vorm gaf aan de weerbaarheid van de Nederlandse samenleving op het vlak van digitale veiligheid. Zo gaf hij sinds 2012 leiding aan de afdeling Monitoring & Response van het NCSC. Een job die hij begin december verruilde voor die van Corporate Information Security Officer (CISO) bij PGGM. Reden voor ons om met Aart terug te blikken op de afgelopen tien jaar.

De tegenstanders waar we als security professionals de laatste jaren mee te maken hebben, zijn volgens Aart dus buitengewoon professioneel geworden. "We hebben het niet meer over relatief onschuldige hit & run-aanvallers, maar veel meer over professionele criminelen en statelijke actoren die heel geavanceerde en gerichte cyberaanvallen kunnen uitvoeren. Acties waarvoor ze beschikken over vrijwel onbeperkte middelen, in de vorm van tijd en geld. Allemaal gericht op diefstal van veel geld en kostbare informatie", geeft hij aan.

Professionalisering sleutelwoord

Professionalisering is volgens Aart sowieso het sleutelwoord dat de ontwikkelingen in ons vakgebied in het afgelopen decennium het beste weergeeft. Niet alleen als je kijkt naar de aanvallers waarmee we te maken hebben. Maar ook wat betreft de ontwikkeling van onszelf als security professionals. We kúnnen volgens Aart niet alleen op de hoogte zijn van de laatste ontwikkelingen en trends. Nee, we móeten hiervan op de hoogte zijn. Een vorm van volwassenheid die van je wordt verwacht wanneer je doel is een organisatie minder kwetsbaar te maken voor cyberaanvallen.

"Om de professionele tegenstanders waarmee we te maken hebben het hoofd te kunnen bieden, moeten we cyberdreigingen in een steeds eerder stadium weten te detecteren", gaat hij verder. "Zodat we vervolgens snel kunnen handelen om de impact van een aanval te verkleinen. De doelstelling van elke security professional." "Om hierin te slagen moet je continu op de hoogte te zijn van de threat landscape van je organisatie, het cyberdreigingsveld. En juist dat dreigingsveld verandert continu", concludeert hij.

Cybersecuritybeeld Nederland

Dit dreigingsveld voor Nederland in kaart brengen, is volgens Aart een belangrijke rol die eerst GovCERT en later het NCSC op zich heeft genomen. Uitvloeisel hiervan is bijvoorbeeld het jaarlijkse CSBN-rapport, het Cybersecuritybeeld Nederland. Het rapport werd voor het eerst uitgegeven in 2011, toen nog opgesteld door GovCERT. "Met het Cybersecuritybeeld Nederland wil het NCSC inzicht bieden in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity. Om zo de awareness ten aanzien van de gevaren waarmee we te maken hebben te vergroten. In de politiek, maar ook bij andere publieke en private beslissers en beleidsmakers." Awareness als het gaat om cyberdreigingen is de afgelopen jaren volgens Aart zeker toegenomen, in sommige sectoren meer dan in andere. "De financiële sector en grote organisaties hebben eenheden ingericht om dreigingen te monitoren en snel te reageren. Andere sectoren blijven nog achter." Het verhogen van bewustzijn voor cyberdreigingen is een belangrijk doel van eerst GovCERT en later het NCSC. "De ontwikkelingen op ons vakgebied gaan snel. Het NCSC is er om overheid én het bedrijfsleven in vitale sectoren zo goed mogelijk op de hoogte houden en te reageren als dat nodig is. Ontwikkelingen te schetsen, onze vitale infrastructuur te monitoren, beveiligingsadviezen te geven en schade te beperken."

"Zichtbaar zijn door steeds weer die stip op de horizon te bepalen. Op basis waarvan security professionals binnen diverse bedrijven en organisaties vervolgens hun koers kunnen uitzetten", vat Aart samen.

Samenwerken: publiek-privaat

Iets dat volgens hem alleen lukt wanneer verschillende partijen nauw samenwerken. "Niet alleen binnen de overheid", benadrukt hij. "Maar juist publiek-privaat. Een samenwerking waarin het NCSC veel investeert. De begrippen 'need to know' en 'urge to share' staan in de security-wereld van oudsher hoog in het vaandel. En daar plukken we als gezamenlijke professionals continu de vruchten van. De basis is steeds weer weten waar kwetsbaarheden zitten, die informatie delen en vervolgens de boel versterken."

Als voorbeeld van de publiek-private samenwerking, die in de ogen van Aart de afgelopen jaren steeds verder is geprofessionaliseerd, noemt hij de oprichting van verschillende ISAC's, Information Sharing and Analysis Centres, in Nederland. Het NCSC stimuleert en faciliteert deze vorm van informatiedeling binnen sectoren. Het zijn publiek-private samenwerkingsverbanden waarbinnen deelnemers onderling informatie en ervaringen uitwisselen over cybersecurity. Ook worden analyses gedeeld, met name op tactisch niveau. Een vorm van kruisbestuiving die volgens Aart toegevoegde waarde oplevert voor alle deelnemers, zowel publiek als privaat.

"Je ziet, mede door deze verregaande samenwerking in Nederland in combinatie met de toenemende afhankelijkheid van ICT, dat informatiebeveiliging een onderwerp is dat binnen organisaties in steeds meer boardrooms ter tafel komt. Niet meer louter vanuit de technische hoek, maar ook echt vanuit de beleidskant. Informatiebeveiliging begint een strategische factor te worden voor geavanceerde organisaties en bedrijven. Waarschijnlijk hebben afgelopen jaren enkele incidenten die het hart van organisaties troffen hieraan bijgedragen, maar zeker ook de strengere regelgeving op datalekken en beveiligingsincidenten."

Opvallende ontwikkelingen uit het Cybersecuritybeeld Nederland 2016

(het rapport werd begin september 2016 gepresenteerd)

- Beroepscriminelen voeren langdurige, hoogwaardige en geavanceerde operaties uit
- Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk
- Ransomware is gemeengoed en is nog geavanceerder geworden
- Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden

Bevindingen die door staatssecretaris Klaas Dijkhoff van Justitie bij de presentatie van het rapport als 'zorgelijk' werden getypeerd. Reden voor hem extra in te zetten op 'digitale dijkbewaking', het Nationaal Detectie Netwerk waarmee overheid en bedrijven elkaar informeren over actuele dreigingen.

Bron: www.ncsc.nl

Sandra Kagie is freelance tekstschrijver/journalist. Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'. Haar website is www.sanscriptproducties.nl en op Twitter is zij actief als @SanSanscript.

Welke ISAC's zijn er?

In Nederland zijn er ISAC's voor de volgende sectoren:

- Haven
- Airport
- Financial Institutions
- Multinationals
- Telecom
- Nucleair
- Zorg
- Energy
- Water
- Managed Service Provider (MSP)
- Insurance
- Rijks
- Keren en Beheren
- Pensioenen

In een ISAC zijn verschillende vertegenwoordigers van organisaties uit de betreffende sector aangesloten. Ook zijn vaak verschillende publieke organisaties aangesloten. Naast het NCSC zijn dit vertegenwoordigers van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Team High Tech Crime van de Nationale Politie. Met de voorzitters van de verschillende ISAC's worden een aantal keer per jaar sessies belegd om de overkoepelend thema's met de sectoren te bespreken. ISAC's kennen vaak een ontwikkeling in vertrouwen en aanpak naarmate ze langer met elkaar samenwerken.

Bron: www.ncsc.nl

Nederland loopt wat betreft deze publiek-private samenwerking volgens Aart in de wereld voorop. "Dat moet ook wel", geeft hij vervolgens aan. "Want we lopen ook voorop als het gaat om digitalisering. We zijn één van de meest ICT-intensieve economieën van Europa. Dat biedt kansen, maar het levert ook risico's op. In Nederland zorgt de overheid misschien voor de spelregels, maar de infrastructuur en systemen zijn bijna volledig in handen van private organisaties. Daarom moeten we er sámen voor zorgen dat de digitale wereld veilig en vertrouwd blijft."

Gezonde sense-of-urgency

Met die wil om samen op te trekken, zit het volgens Aart bij zijn nieuwe werkgever wel goed. "Niet voor niets is PGGM voorzitter van de ISAC pensioenen", geeft hij aan. "Ik heb hier een gezonde sense-of-urgency aangetroffen. Informatiebeveiliging wordt hier serieus genomen." Waar hij de komende tijd dan ook vooral naar uitkijkt, is het verantwoordelijk zijn voor de beveiliging van een IT-omgeving die een belangrijke maatschappelijke waarde vertegenwoordigt. "We werken bij PGGM als pensioen-uitvoeringsorganisatie aan de zekerheid van miljoenen mensen", geeft hij aan. "Een verantwoordelijkheid die ik absoluut voel en heel serieus neem."

"Of ik ook iets gaat missen? Incident response is een mooi vak. Maar ik hoop het hier natuurlijk niet nodig te gaan hebben", zegt hij met een glimlach. "En verder was mijn werk bij het NCSC natuurlijk ook gericht op internationale samenwerking. Met buitenlandse CERT's, Computer Emergency Response Teams, bijvoorbeeld. Digitale dreigingen laten zich immers niet beperken door landsgrenzen. Die internationale oriëntatie is bij PGGM veel minder. Die open samenwerking met buitenlandse collega's ga ik missen."

Terugkijken: DigiNotar

Wat hij in elk geval níet gaat missen, is de wisselvalligheid van de politiek en de lange doorlooptijden die Den Haag kenmerken. Maar ondanks dat kijkt Aart met plezier terug op tien jaar overheid (GovCERT/NCSC). Ook de DigiNotar-hack (augustus 2011) is wat dat betreft geen gevoelig punt. "Ik had me in 2013 voorgenomen voor het laatst een presentatie te houden over deze casus", zegt hij nu. "Maar een paar maanden geleden heb ik er nog een presentatie over gegeven. Als voorbeeld van een real life scenario. Lessen die we toen hebben geleerd, gelden eigenlijk nog steeds, vandaar." "Naast het voorbeeld hoe een kwetsbaarheid bij een kleine organisatie een grote impact kan hebben op een land, heeft de aanpak van de crisis ook de toon gezet voor de samenwerking tussen incident response, opsporing en inlichtingen."

"Waren we destijds voorbereid op een hack als deze? Ik heb het me diverse keren afgevraagd. Een scenario als dit hadden we niet voorzien. Maar geoefend waren we zeker wel. Wat me verder nog heel helder voor de geest staat, is dat mensen zich destijds meer dan volledig inzetten. En in anderhalve week tijd voor een maand hebben gewerkt. Zonder twijfel een heel markant moment in mijn carrière, maar ook in de geschiedenis van cybersecurity in Nederland."

"DigiNotar heeft als geen ander incident duidelijk gemaakt dat ICT kwetsbaar is. En hoe onze samenleving afhankelijk is van een goed functionerende, veilige ICT-infrastructuur."

SURF SECURITY EN PRIVACY AWARD 2017 VOOR BART JACOBS

Professor Bart Jacobs van de Radboud Universiteit heeft de SURF Security en Privacy Award 2017 ontvangen. Jacobs krijgt de award voor zijn verdiensten op het gebied van security en privacy. "Professor Jacobs heeft veel belangrijk werk verricht op het gebied van internetsecurity en privacy. Voorbeelden hiervan zijn het vernieuwende securityonderzoek naar de OV-chipkaart, zijn inzet om attribuut-gebaseerde privacyvriendelijke authenticatie (IRMA) voor elkaar te krijgen en meer recent het PEP-project (security en privacy in personalised medicine). Het is belangrijk dat zulk onderzoek wordt gestimuleerd", aldus Wim Biemolt, voorzitter van SURFcert.

SURF

SURF is een samenwerkingsverband van het onderwijs en onderzoek waarin de Nederlandse universiteiten, hogescholen, universitair medische centra, onderzoeksinstellingen en mbo-instellingen gezamenlijk investeren in ICT-innovatie. SURF brengt ICT-professionals samen binnen netwerken en samenwerkingsprojecten voor kennisdeling rond ICT-thema's. Door innovaties tegen aantrekkelijke voorwaarden beschikbaar te maken, zorgt SURF dat de mogelijkheden die ICT biedt optimaal kunnen worden benut. SURF bestaat uit drie werkmaatschappijen met een eigen aandachtsterrein: SURFmarket, SURFnet en SURFsara. Meer informatie over SURF: www.surf.nl.

Naast zijn onderzoekswerk prijst de jury Jacobs' bijdrage aan de discussie over security en privacy in het publieke domein. "Zijn artikelen in de pers en optredens op tv zijn noodzakelijk voor de bewustwording over deze onderwerpen."

Professor Bart Jacobs (l.) en Wim Biemolt.

Prijs

De SURF Security en Privacy Award wordt jaarlijks uitgereikt aan een persoon, initiatief of idee met een substantiële bijdrage aan het collectieve beveiligingsniveau van de Nederlandse hogeronderwijs- en onderzoeksinstellingen. De prijs, die 2500 euro bedraagt, is uitgereikt tijdens de SURF Security- en Privacyconferentie van SURFcert, SCIRT en SCIPR, die dit jaar in Wageningen heeft plaatsgevonden. Het geldbedrag kan Bart Jacobs gebruiken voor zijn werk op security- en privacygebied en draagt zo direct bij aan een veiliger internet.

SURF Security en Privacy Award

SURF heeft de ambitie om een vertrouwde, betrouwbare en veilige omgeving te realiseren en duurzaam te borgen, waarin eindgebruikers en instellingen (inter)nationaal eenvoudig, veilig en vertrouwd toegang hebben tot diensten, data en instrumenten. De Security en Privacy Award is een initiatief van SURFcert, de SURF Community voor Informatiebeveiliging en Privacy (SCIPR), en de SURFnet Community van Incident Response Teams (SCIRT). Met de SURF Security en Privacy Award wil SURF personen of initiatieven uit zijn doelgroep speciale aandacht geven en belonen voor hun waardevolle bijdrage hieraan.

Links

Beveiliging bij SURF: www.surf.nl/themas/beveiliging
SCIPR: http://bit.ly/2nViYsX
SCIRT: http://bit.ly/2nrJn3x
SURFcert: www.surf.nl/diensten-en-producten/surfcert/index.html
Winnaar SURF Security Award 2016: http://bit.ly/2nGTL8n
Meer informatie over Professor Bart Jacobs: http://www.cs.kun.nl/~bart/PRESS/index.html

UNIEK PARTNERSHIP OP HET ALLERHOOGSTE NIVEAU VAN INFORMATIEBEVEILIGING

Dertig jaar samenwerking; in welke branche zou dit nu niet bijzonder zijn? Sinds de jaren tachtig hebben Avensus en Thales e-Security UK elkaar op het gebied van High Grade Security versterkt. Destijds besloot Avensus haar diensten voor hoogwaardige informatiebeveiliging uit te breiden met Thales Hardware Security Modules (HSM). Thales kreeg daarmee een betrouwbare partner die met expertise crypto-oplossingen inzet en onderhoudt. Kwaliteit van dergelijke oplossingen eindigt immers niet alleen bij de oplossing zelf. Voor Avensus heeft de samenwerking geresulteerd in het feit dat zij de enige gecertifieerde Thales Gold Partner in de Benelux is en marktleider op het gebied van Crypto Services. Wat zijn volgens deze specialisten de uitdagingen van vandaag op het gebied van data security?

Compliancy en zogenoemde best-practices vragen erom om informatie te versleutelen en toegang tot gevoelige data strikt te controleren. Wekelijkse krantenkoppen tonen het aantal inbreuken met gestolen of gecompromitteerde identiteiten waarmee toegang tot alle soorten van persoonlijke, medische of financiële gegevens verkregen wordt. Naast en ook dóór de complexere bedreigingen, wordt strenge wet- en regelgeving opgelegd, zoals GDPR (General Data Protection Regulation) en eIDAS (EU regelgeving digitale handtekeningen). Nederland kent sinds 2016 de Meldplicht Datalekken waarbij hoge boetes worden opgelegd wanneer organisaties hun privacygevoelige data niet goed hadden beschermd. Daarbij moeten deze organisaties hun klanten op de hoogte stellen en ligt imagoschade op de loer.

Het 2017 Thales Data Threat Report toont dat investering in preventie van datalekken topprioriteit voor organisaties heeft. Compliancy biedt een goede basis voor een sterke securitystrategie.

Data-encryptie en key management cruciaal

Het besef dat traditionele securitytools niet meer voldoen in het voorkomen van multi-layer attacks groeit. Het explosieve gebruik van cloud-oplossingen al dan niet gecombineerd met legacy problematiek resulteert in een IT-omgeving waarin organisaties de controle over de infrastructuur verliezen en de perimeter vervaagd. Door dit besef en doordat datalekken tegenwoordig tot bedrijfsrisico worden ingeschaald, zal data-encryptie en key management een cruciaal onderdeel van een sterke beveiligingsstrategie worden. Encryptie is van grotere importantie dan enkel als inzet voor versleuteling van laptops en USB-sticks als bescherming tegen verlies of diefstal. De wetgever legt niet voor niets de nadruk op encryptie als best mogelijke optie voor informatiebeveiliging.

Een stijgende vraag naar encryptie zal leiden tot diverse single-function oplossingen die verschillende vraagstukken aanpakken. Dit vergroot echter ook de complexiteit van IT-security. Slimmer is het om voor totaaloplossingen te kiezen die zich op een scala van beveiliging richten. Dit scheelt in complexiteit, vermindert druk op implementaties en performance, en scheelt zeker ook in kosten.

Ervaring inzetten in andere branches

Gökmen Kiremit, director security bij Avensus, vertelt: "Avensus is gepokt en gemazeld als het om digitale beveiliging gaat en heeft een leidende positie in de markt van encryptie, data-protectie en key-management. Het overgrote deel van onze banken en centrale overheid bedient Avensus met Thales-oplossingen. Als enige Nederlandse Thales Gold Partner heeft Avensus de ambitie haar activiteiten uit te breiden naar meerdere markten. De ervaring die we uit de streng gereguleerde financiële en overheidssector hebben, gebruiken we om andere branches te helpen. Denk aan gezondheidszorg, transport en industrie, waar bescherming van privacygevoelige data en intellectueel eigendom met encryptie en data-protectie technologie steeds meer gemeengoed is."

"Cybercrime, strenge wet- en regelgeving, explosieve groei aan mobiele transacties en technologische innovaties komen op ons af. Europese beveiligingseisen, eisen van de Payment Card Industry en van de Nederlandsche Bank. Avensus volgt klantuitdagingen rondom compliancy en reputatiebescherming. Het gaat ons niet alleen om het leveren van de beste oplossing voor informatiebeveiliging; het is ook onze taak mensen en organisaties bewust te maken van de risico's. Zo is Thales e-Security onze vaste partner op het jaarlijks Avensus Security Event waar relaties inspiratie & informatie opdoen over trends en ontwikkelingen van informatiebeveilging. Dit jaar gaat het natuurlijk over GDPR, IoT, PEP & eID, PCI-DSS/HSM en eIDAS. Noteer 15 juni in uw agenda als dergelijke thema's u bezighouden."

Meer informatie over Thales, Avensus, het Security Event op 15 juni of het 2017 Thales Data Threat Report kunt u opvragen bij Avensus Marketing & Communicatie. Contactpersoon: Shirley Stoetzer -sstoetzer@avensus.nl.

Mr. Rachel Marbus
@rachelmarbus op Twitter

DE CRIMINALISERING VAN HET BEVEILIGINGSMIDDEL

Toen Netflix naar Nederland kwam, heb ik meteen een abonnement genomen. Al jaren was ik op zoek naar een goed alternatief voor de tv, die had ik namelijk uit ergernis uitgezet in 2009 en nooit meer aangezet. De kijkhonger bleef, maar buiten het downloaden om was er toen niet echt een goed alternatief. Met Netflix kwam dat er eindelijk.

Ik ben natuurlijk heel erg privacyminded. Dus gebruik ik een VPN als ik verbinding maak met de digitale wereld. Netflix vindt dat niet cool, want wie een VPN gebruikte kreeg automatisch het USA aanbod (en dat was ook heel fijn, ik geef het eerlijk toe, want het aanbod was vele malen groter). Daarop volgde een VPN-verbod, keihard afgedwongen, want als er ook maar iets draait wat ruikt naar VPN dan wordt de toegang tot Netflix geblokkeerd. En dat terwijl ik een betalende klant ben. En graag veilig het internet opga. VPN wordt daarmee gecriminaliseerd en zij die het gebruikten zijn alleen maar slecht van zins. Dat is de omgedraaide wereld.
Nu hoor ik u denken: 'Ja maar, je kunt dan toch anoniem allemaal illegale dingen doen met een VPN?'. Dan zal ik u zeggen: Je kunt op allerlei manieren allemaal heel illegale dingen doen. Daar heeft die VPN niets mee te maken. Het is een middel om jezelf beter te beschermen online. Dat is alles. Vergelijk het eens met het mes. Daarmee kun je iemand vermoorden. Keihard doodsteken, wel honderd keer achter elkaar je mes laten neerdalen in een lijf. Dat is een brute misdaad. Maar is daarmee het mes dan fout? Nee, de mens die de handeling verricht. Heel logisch, zo wordt in de offline wereld al jaar en dag geredeneerd in het strafrecht. De mens is schuldig, niet het middel. En toch wordt in de digitale wereld telkens het beveiligingsmiddel verketterd.

Er is al heel veel jaren iets vreemds aan de hand in de digitale wereld met beveiligingsmiddelen. Want het is niet de eerste keer dat een middel als 'het kwaad' wordt gezien. Cryptografie is daar een mooi en treffend voorbeeld van dat nog steeds aan allerhande exportbeperkingen is onderworpen, het wordt gelijkgesteld aan wapens en munitie. En zo wordt ook op een negatieve manier gekeken naar TOR, wat gelukkig nog steeds op een redelijk normale manier gebruikt kan worden – niet overal ter wereld helaas, maar het biedt nog steeds de mogelijkheid voor personen om ongecensureerd van de digitale wereld te genieten.
Trouwens, zomaar een gedachte hè, stel nu eens dat er iets mis gaat terwijl ik Netflix aan het kijken ben en dat dit aantoonbaar voorkomen had kunnen worden als de VPN aangestaan had. Kan ik dan Netflix aanklagen voor geleden schade omdat zij mij – willens en wetens – dwingen mijn beveiliging uit te schakelen? Lijkt me een hele leuke case. Want volgens mij is het bijzonder crimineel om mensen te dwingen hun beveiliging uit te zetten. Een beveiligingsmiddel is net zoiets als je gordel dragen terwijl je autorijdt of die helm die je draagt als je op de scooter zit, de condoom die je omdoet bij het vrijen. Het is noodzakelijk voor je eigen veiligheid.

CRISISOEFENINGEN: EEN KORTE ACHTERGROND

In IB-Magazine nummer 1, 2017 schetsten Sandy Janssen en Alf Moens een beeld van cybercrisisoefening OZON. Nu gaan zij in op crisisoefeningen in het algemeen. Als een security incident lang onzichtbaar blijft en de impact van een incident onderschat wordt, kan dit zich ontwikkelen tot een cybercrisis met veel grotere impact. Bijvoorbeeld verlies van vertrouwen, reputatieschade en grote financiële schade. Een crisis kan zich dan als een olievlek uitbreiden en ook andere partijen treffen. Ook richten kwaadwillende actoren zich zelden op één organisatie, maar meestal op tientallen -zowel publieke als private organisaties- tegelijkertijd. Cyberrisico's kunnen daarom vaak niet meer door één organisatie alleen worden opgepakt en samenwerken tussen organisaties is noodzakelijk.

"een goede voorbereiding is het halve werk' is het gezegde. Dat geldt ook voor het reageren op een cybercrisis. Veel organisaties hebben nog geen vastomlijnde cybercrisisaanpak. Naast operationele en strategische maatregelen, zoals cybersecurity onderdeel maken van de algemene crisisaanpak, is oefenen met cybercrisisscenario's een relatief nieuw hulpmiddel. Bij sociale en fysieke veiligheidsrisico's is het al gebruikelijk om te oefenen. Bij cyberdreigingen is dit in opkomst. Oefenen kan helpen om de crisisstructuren vorm te geven.

De aandacht voor cybercrisisoefeningen groeit. In 2009 [1] roept de Europese Commissie lidstaten al op "om regelmatig cybercrisisoefeningen te organiseren voor grootschalig netwerksecurity incident response en herstel bij grote incidenten." Dit wordt in 2011 [2] nog eens onderstreept in het Europees Parlement. Er zijn weliswaar enkele grote voorbeelden van cybercrisisoefeningen, zoals Cyber Europe [3] georganiseerd door ENISA, (internationaal), ISIDOOR georganiseerd door het NCSC (nationaal) [4] of Cyberdawn [5] in de Nederlandse telecomsector (nationaal) maar in de praktijk wordt nog weinig geoefend [6]. Het (sectorbreed) oefenen verbetert zowel de interne als de externe samenwerking.

Door te oefenen met cybercrisisscenario's leren medewerkers en organisaties hoe ze op een cybercrisis moeten reageren. Medewerkers moeten vaak beslissingen nemen onder druk, dit kun je alleen goed

Terminologie

Security incident – Een security incident is een 'IT-verstoring die de verwachte beschikbaarheid van diensten en/of de ongeoorloofde openbaarmaking, aankoop en/of de wijziging van informatie' verstoord.

Cybercrisis – Een cybercrisis is 'een abnormale en onstabiele situatie waarbij strategische doelen, reputatie en betrouwbaarheid in het geding komen doordat verstoring van de IT, bewust of onbewust, het hart van de organisatie raakt'.

doen als je deze vaardigheid getraind hebt: 'oefening baart kunst.' Ook vergroot oefenen het bewustzijn voor de mogelijke cyberrisico's.

Cybercrisisoefeningen helpen om bruggen te slaan tussen het tactisch/operationeel niveau en het strategisch niveau en tussen het technische en niet technische niveau; zowel intern als extern. Belanghebbenden die bij een crisis betrokken zijn, werken in de praktijk vaak nog niet samen of communiceren zelfs niet met elkaar. Leden van het crisismanagementteam leren elkaar beter kennen in crisisomstandigheden. Ook medewerkers leren elkaar beter kennen, weten elkaar beter te vinden en kunnen van elkaar leren.

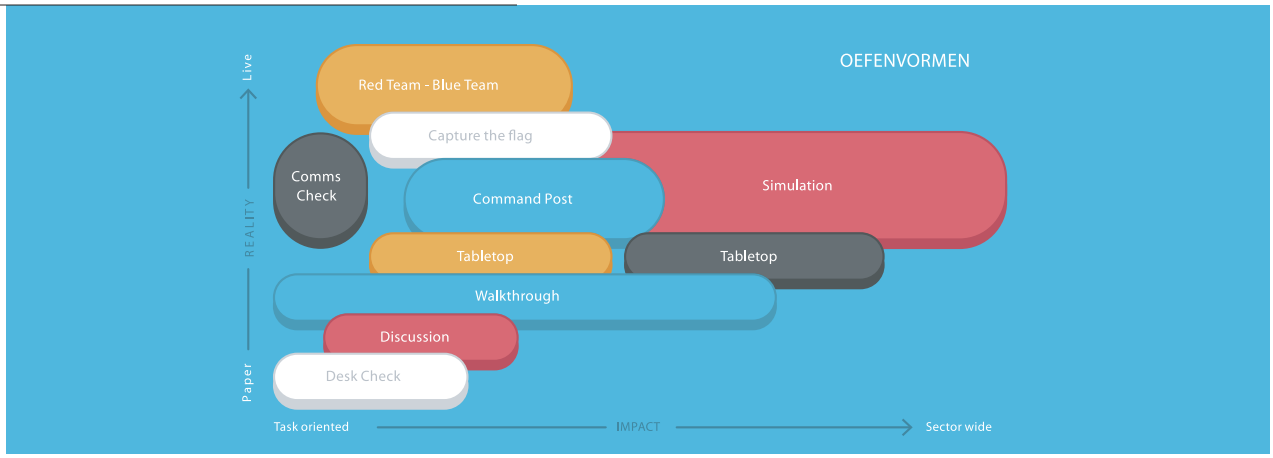
Ook zorgt oefenen voor meer draagvlak voor cybersecurity op bestuurlijk en directieniveau. De tijdens de oefening geleerde lessen kunnen bijdragen aan het verbeteren van de crisisorganisatie en aan de operationele processen voor incidentafhandeling en communicatie. Oefenen vergroot hiermee de algehele weerbaarheid tegen cyberdreigingen.

Oefenvormen

Afhankelijk van de oefendoelen kun je verschillende vormen voor oefeningen gebruiken, zowel groot- als kleinschalige oefeningen. Dat kunnen papieren/discussie oefeningen of praktijkoefeningen zijn, in verschillende vormen, zie tabel 1. Hierdoor kan het opzetten van een oefening al laagdrempelig zijn.

Oefenvorm: Discussie (Papier)	**Methode:**
Desk Check	Discussie met systeemeigenaren om (wijzigingen van) plannen en/of procedures te valideren.
Walkthrough	Met betrokkenen een specifiek dreigingsscenario uitdiepen door een crisissituatie stap voor stap te doorlopen zoals; detectie, opschaling, respons, nabehandeling en afsluiting.
Workshop	Een walkthrough van een crisisplan of een crisisscenario inclusief het bespreken van de reacties van betrokkenen. Acties en reacties van spelers kunnen zonder tijdsdruk worden gerepeteerd.
Table Top-oefening	Alle aspecten van het crisismanagement worden met betrokkenen doorlopen. Er wordt gebruik gemaakt van gesimuleerde berichten. Zo kan de crisisstructuur en de onderlinge samenwerking geoefend worden en/of specifieke vaardigheden getraind worden, met de mogelijkheid om de oefening te pauzeren en acties en reacties tussentijds bespreken.
Oefenvorm: Praktijk	**Methode:**
Comms Check	Deze oefening voer je uit om communicatiemethoden en kennisgevingssystemen te checken en valideren.
Oproepoefening	Hierbij test je of je binnen de afgesproken tijd een crisisteam bij elkaar krijgt.
Distributed Table Top-oefening	Is qua opzet gelijk aan een Table Top-oefening, maar zonder de mogelijkheid tot discussie. Deelnemers moeten handelen alsof er sprake is van een crisis. De mogelijke acties en reacties kunnen achteraf in een evaluatie besproken worden.
Command Post Exercise (CPX)	Een crisis wordt zonder inzet van externe betrokkenen, externe omgevingsfactoren en spelers gesimuleerd. Crisisteams krijgen vragen en opdrachten in een realistisch en evoluerend scenario. Zo kunnen de teams in hun eigen werkomgeving met gebruik van eigen faciliteiten de mogelijkheid om acties en reacties te oefenen.
Simulatieoefening	Men speelt in de eigen werkomgeving onder zo normaal mogelijke werkomstandigheden een realistisch scenario na. Het scenario ontwikkelt zich aan de hand van besluiten en acties van de betrokkenen. Er kan zowel met interne als met externe betrokkenen geoefend worden.
Capture the flag	Het doel is om een vlag of belangrijk 'element' te veroveren. Dit kan in teams of individueel al dan niet in competitieverband.
Red Team/Blue Team	Een team (rood) valt een netwerk, informatiesysteem of ander belangrijk bedrijfsonderdeel aan. Het andere team (blauw) moet de aanval proberen te verijdelen.

Tabel 1 – Oefenvormen voor crisisoefeningen



Voor het opzetten van dergelijke oefeningen kan gebruik gemaakt worden van ISO 22398:2013. Deze ISO is geschreven voor het organiseren van crisisoefeningen in het algemeen en geeft de rolverdeling en structuur van oefeningen goed weer. Hele laagdrempelige voorbeelden voor oefeningen zijn bijvoorbeeld te vinden op Linux journal [7].

Conclusie en aanbevelingen

Als onderdeel voor ons whitepaper over de crisisoefening hebben we uitgebreid literatuur bestudeerd. In dit onderzoek hebben we gezien dat er al wel met cyber geoefend wordt op nationaal niveau en internationaal niveau, vooral in NATO en ENISA verband. Sectorspecifieke oefeningen vinden wel plaats bijvoorbeeld in de zorg, telecom- en energiesector, maar nog niet vaak. De focus bij onderwijs- en onderzoeksinstellingen, maar ook in veel andere sectoren, ligt vooral nog op het oefenen van sociale en fysieke risico's (bijvoorbeeld BHV en evacuatieoefeningen). Oefeningen kunnen laagdrempelig zijn, oefenscenario's zijn prima herbruikbaar en deelbaar. Zeker de kleinschaligere oefeningen, zoals Table Top, capture the flag of Red Team/Blue Team kunnen met weinig inspanning in teamverband uitgevoerd worden en zouden onderdeel kunnen zijn van een vast bewustzijns- en trainingsprogramma.

Links

[1] Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience – EC (2009) – 149: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0149:FIN

[2] Achievements and next steps: towards global cyber-security – EC (2011) – 163 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52011DC0163

[3] Cyber Europe 2016: the pan-European exercise to protect EU Infrastructures against coordinated cyber-attack: www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 (geraadpleegd op 21 december 2016)

[4] ISIDOOR: operationele cyberoefening met publieke en private partners: www.ncsc.nl/actueel/nieuwsberichten/isidoor-operationele-cyberoefening-met-publieke-en-private-partners.html (geraadpleegd op 21 december 2016)

[5] Telecomsector bouwt met grootschalige oefening CyberDawn aan sterke samenwerking op cybersecurity: www.nederlandict.nl/news/telecomsector-bouwt-met-grootschalige-oefening-cyberdawn-aan-sterke-samenwerking-op-cyber-security/ (geraadpleegd op 20-10-2016)

[6] The 2015 Report on National and International Cyber Security Exercises, ENISA, dec. 2015: www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

[7] Example Security Exercises: www.linuxjournal.com/content/example-security-exercises (geraadpleegd op 21 december 2016)

Alf Moens en Sandy Janssen werken voor SURFnet. SURFnet is onderdeel van de coöperatie SURF, de ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland. Binnen SURF werken universiteiten, hogescholen, mbo-scholen, onderzoeksinstellingen en de universitaire medische centra (UMC's) samen aan ICT-voorzieningen én -vernieuwingen. Alf Moens is naast Security Officer voor SURFnet ook Corporate Security Officer bij SURFnet en nauw betrokken bij het onder controle brengen van informatiebeveiliging bij de aangesloten instellingen. Sandy Janssen is deelnemer aan het Jong Talenten-programma van SURFnet en heeft het opzetten van de oefening en de uitwerking van de scenario's voor OZON begeleid.

HET JAAR VAN HET LOSGELD

Op 7 februari is het 2017 Annual Threat Report uitgekomen van SonicWall. Voor mij was dit een nieuw rapport, maar als je even zoekt dan zie je dat er ook in 2016 al een rapport was en dat in de tijd dat Dell eigenaar was van SonicWall er ook al securityrapporten uitkwamen waar SonicWall flink in bijdroeg. Anders dan die oudere rapporten zijn de versies uit 2016 en 2017 een goede mix van tekst en grafisch werk. En ruim twintig pagina's is goed verteerbaar. Het doet ze kennelijk goed weer een zelfstandig merk te zijn.

Genoeg redenen om ook naar de inhoud te kijken. Het rapport lijkt gericht op de technische CxO. SonicWall heeft de informatie voor het rapport verkregen uit hun GRID Threat Network, met meer dan een miljoen sensors. Het is big data uit hun producten, wat geaggregeerd een schat aan informatie kan opleveren. En dat doet het ook. Een aantal onderwerpen waar ik zelf ook over geschreven heb passeren de revue:

- De invoering van chip en PIN in de Verenigde Staten. In het eerste jaar na invoering zijn aanvallen op point-of-sale apparaten met 88% afgenomen. De Target hack staat nog diep in ons geheugen gegrift. Dat wordt nu dus verleden tijd.
- De groei van ransomware. Individuele verhalen gaven al die indruk, maar de cijfers van het GRID van SonicWall liegen er niet om: een meer dan honderdvoudige groei! De toename van TLS-versleuteld verkeer wordt aangewezen als enabler hierin. Dat verkeer moet natuurlijk aan de grens van de enterprise geïnspecteerd worden. Het is één van de reclames voor eigen producten die er ingeschreven zijn. Al met al helemaal niet storend.
- IoT-apparaten worden grootscheeps gebruikt in DDoS-aanvallen. Dat is niet het enige. Het verdwijnen van de drie grote exploit kits, Angler, Neutrino en Nuclear wordt opgemerkt en de opkomst van Rig.
- Het aantal unieke virussamples is in 2016 afgenomen. Een geluid dat ik uit meerdere hoeken gehoord heb. Is het een trend? De tijd zal het leren.

Het rapport sluit af met geloofwaardige voorspellingen voor 2017 en wat nabeschouwingen. Eén scenario daaruit klinkt behoorlijk dreigend: een aanval met malware op IoT op productielijnen en energievoorziening, met een vraag om losgeld.

Al met al een waardig rapport om elk jaar naar uit te kijken. Het SonicWall 2017 Annual Threat report is te downloaden vanaf de website van SonicWall [1].

Links

[1] https://blog.sonicwall.com/2017/02/sonicwall-threat-report-reveals-cybersecurity-arms-race/

Lex Borger is hoofdredacteur IB-Magazine, security consultant bij i-toi en docent scurity aan de Hogeschool Utrecht. Lex is te bereiken via l.borger@i-to-i.nl.

GEZOCHT: SECURITY PROFESSIONAL

Al een aantal jaren lezen we dat er een groot tekort dreigt aan professionals in de informatiebeveiliging. Aan de andere kant zijn er ook berichten vanuit het UWV dat er best veel hoger opgeleide ICT'ers in de WW zitten. Kwestie van omscholen en inzetten, toch? Of is het niet zo eenvoudig? Dit artikel schetst de ontwikkelingen op dit vlak en de eerste ervaringen met het gebruik van de QIS-beroepsprofielen. QIS is een publiek-privaat project over het onderwerp Qualification of Information Security professionals en wordt gesteund door het PvIB.

"Wereldwijd zijn er twee miljoen professionals te weinig in 2020", aldus het ISC2 Workforce report uit 2015 [1]. Het PLATO rapport [2] uit 2014 heeft een soortgelijke boodschap: "op korte termijn te weinig goed opgeleide professionals met op langere termijn in het algemeen te weinig professionals". Het gevolg hiervan gaat zijn dat er een strijd ontstaat om de échte security professionals binnen te halen, dat er een wildgroei ontstaat aan 'gelukszoekers' die zich security professional noemen en dat het voor organisaties moeilijk blijkt om de juiste mensen aan te nemen. Organisaties zijn simpelweg niet goed voorbereid op de ontwikkelingen op het terrein van informatiebeveiliging. Zo wordt het ook genoemd in de ISF Threat Horizon 2018 [3].

De bomen en het bos

Op dit moment is het lastig voor een werkgever om te zien of een kandidaat een goede security professional is. Er zijn geen standaard opleidingen voor, maar wel heel veel verschillende certificeringen die onderling nauwelijks met elkaar te vergelijken zijn. Zie bijvoorbeeld het artikel 'Aanleg en praktijkervaring maken de cyber security professional' uit IB-Magazine nummer 7, 2016 of tabel 'Overzicht certificeringen' in het aparte kader bij dit artikel. Je ziet haast door de bomen het bos niet meer! Het vinden van een goede aansluiting tussen vraag en aanbod vergt begrip over en weer: het zijn twee kanten van dezelfde medaille. Ten eerste; hoe zorg je ervoor dat je als informatiebeveiliger ook herkenbaar bent als de juiste professional? Ten tweede; hoe weet je als werkgever dat je de juiste persoon aanneemt? Heb je als ethical hacker genoeg aan een CISSP- of CEH-certificering of zijn die juist niet zo relevant?

Als bevlogen professional zijn we dan geneigd om er nog meer certificeringen en opleidingen tegenaan te gooien, de één nog 'relevanter' dan de andere. Het lost de verwarring alleen niet op. Eerst moet duidelijk zijn wat we van de professional verwachten in een specifieke functie, daarna kan worden vastgesteld welke kennis en kunde hier voor nodig zijn.

Body of Knowledge

In verschillende landen is men al jaren bezig met dit vraagstuk. Zo ook in de Verenigde Staten van Amerika. De CISSP-opleiding is midden jaren 80 ontstaan vanuit de behoefte aan een standaard, leveranciers onafhankelijk, certificeringsprogramma. De ISC2-certificering is in 1994 gelanceerd.
Daarnaast lopen er ook andere trajecten om dit aan te vullen. Bijvoorbeeld vanuit ISACA met het CSX programma gericht op Cyber Security, naast de al bestaande certificeringen als CISA, CISM en CRISC. Deze certificeringen zijn gebaseerd op een basale kennistoets, waarbij andere gecertificeerden onderbouwen (attesteren) dat deze kennis en kunde ook in de praktijk wordt toegepast, net zoals de eis dat men al een tijd in het vakgebied werkzaam moet zijn. Het is voor een jonge discipline acceptabel, maar niet bij de groei naar volwassenheid van het vakgebied; we gaan van 'trust me' naar 'prove me'.

	Veiligheid van de I-functie (Information risk management)	Veiligheid van de ICT-functie (ICT-beveiliging)
Strategisch en/of tactisch	CISO	ICT-beveiligingsmanager
Tactisch en/of operationeel	Information Security Officer	ICT-beveiligingsspecialist*

** Het beroep ICT-beveiligingsspecialist kent drie niveaus, genummerd van 1 (mbo-niveau) tot 3 (universitair-niveau).*

Tabel 1 - Positionering functies.

In het Verenigd Koninkrijk wordt gewerkt met een certificering vanuit de CESG, de Engelse overheid. Je laat je hierbij certificeren op kennis en kunde niveau en tegen een rol (niet alleen 'tell me', maar ook 'prove me'). Er zijn drie niveaus te onderkennen: practitioner, Senior Practitioner en Lead Practitioner. In totaal zijn er zeven rollen onderkend [7]:

- Accreditor
- Security & Information Risk Adviser
- IA architect
- IA auditor
- IT security officer
- Communications Security Officer
- Penetration tester

De certificering op niveau gebeurt tegen een gemeenschappelijk Body of Knowledge. Er is kennis nodig van een veelheid aan gebieden met ook een zekere diepgang en heel belangrijk, deze kennis moet je ook kunnen toepassen. Deze beoordeling gebeurt in een interview door vakgenoten.

QIS

In Nederland is sinds 2013 een projectgroep bezig onder de naam Qualification of Information Security professionals (QIS). Gesponsord door het bedrijfsleven en de Rijksoverheid, wordt gewerkt aan een Nederlands certificeringsstelsel. In 2014 is een whitepaper [4] gepubliceerd, waarbij er vier beroepen in de informatiebeveiliging worden uitgewerkt met daarbij ook de vereiste kennis en kundeniveaus. Dit whitepaper bouwt voort op de eerdere publicatie Functies in de Informatiebeveiliging [5].

De vier beroepen die onderscheiden worden, zijn: CISO, Information Security Officer, ICT-beveiligingsmanager en ICT-beveiligingsspecialist. Zie tabel 1 voor een positionering van deze functies.

Gemeenschappelijk aan deze functies zijn de verwachte kennis en kunde, die zijn opgebouwd met behulp van het e-competence framework (e-CF) [6]. Bij elkaar levert dat een gemeenschappelijke Body of Knowledge op. In die zin zijn de Nederlandse en de Engelse benaderingen gelijk (certificering tegen een Body of Knowledge), alleen de benaderingswijze is anders.

Na de ALV van de PvIB op 29 juni 2016 is besloten dat PvIB eigenaar wordt van de beroepsprofielen. Het certificeringsstelsel voor Nederland wordt separaat opgezet en waarschijnlijk kun je je vanaf januari 2018 als professional laten certificeren als bijvoorbeeld Information Security Officer of ICT beveiligingsspecialist.

Opleiding

Als de eisen aan de functie bekend zijn, dan is de volgende vraag hoe mensen de vereiste kennis en kunde kunnen verwerven. Hoe passen de vele bestaande certificeringen in dit beeld en hoe kun je je verder ontwikkelen / scholen tot een functie in het vakgebied?
Tot op heden wordt de eis aan kennis en kunde ingevuld door te vragen naar relevante certificeringen. De bekendste certificeringen op dit vlak zijn dan CISSP en CISM, maar er zijn er

Jan Wessels is security officer voor de business line Wholesale bij het Global Information Security Office van Rabobank en lid van de werkgroep QIS. Hij is bereikbaar via Jan.Wessels@rabobank.com.
Olaf Streutker is Strategic Advisor bij het Corporate Information Security Office van ABN AMRO Bank en lid van de stuurgroep QIS. Hij is bereikbaar via olaf.streutker@nl.abnamro.com.

Gebruik van de beroepsprofielen binnen Rabobank

Als één van de sponsoren van QIS, werkt Rabobank aan standaardisering van de beroepsprofielen en wel op basis van de PvIB-beroepsprofielen. Op dit moment is het profiel van ISO gestandaardiseerd en wordt er gewerkt aan profielen binnen de SOC-omgeving op basis van het profiel ICT-beveiligingsspecialist. Vanwege de omvang en complexiteit van de omgeving, bestaat het ISO profiel op drie niveaus: junior, medior en senior. Het PvIB ISO-profiel is genomen als basis voor het medior niveau. Voor de andere niveaus zijn de verwachte competentieniveaus aangepast. Opvallend is dat het PvIB ISO-profiel uitgaat van een bachelor niveau, waarbij in de Rabobank vertaling een sterkere nadruk op een master niveau ligt. Ter onderbouwing van de informatiebeveiligingskennis en kunde is gekozen voor een aantal certificeringen zoals CISSP en CISM. Tevens geldt ook de EDP-opleiding als onderbouwing van kennis en kunde.

Voor de SOC-specialisten zijn nu profielen opgesteld voor cryptospecialist, security tester en security analist. In samenwerking met de specialisten is vastgesteld welke certificeringen we gebruiken ter onderbouwing van de kennis en kunde.

Wie werkt er binnen security?

In de huidige situatie zijn er al mensen werkzaam binnen security. Grote vraag daarbij: is er een gemeenschappelijk profiel op te stellen voor de verschillende functies. Eind 2015 is er enquête gehouden onder medewerkers werkzaam binnen information security bij ABN AMRO, ING en Rabobank. De enquête is door 186 medewerkers ingevuld. Door verschillen in de opzet van enquête is het niet altijd gemakkelijk om te komen tot een eenduidig totaal beeld. Er is dan ook geen diepgaande statistische analyse op uitgevoerd. Bijgaand een overzicht van de hoofdconclusies.

Leeftijdsopbouw

De leeftijdsopbouw per bedrijf is hierin niet meegenomen (resultaten voor ABN AMRO en Rabobank). Het is nu nog een werkgebied voor de oudere medewerker, slechts 26% van de 186 respondenten is jonger dan 35 jaar. Wel is onze verwachting dat dit beeld snel gaat veranderen.

Opleidingsniveau

Er is een behoorlijk hoog opleidingsniveau; ruim 90% van de 186 respondenten hebben een opleiding op bachelor niveau of hoger. In het huidige werk en denkniveau (niet formeel getoetst) is de verschuiving nog beter te zien.

EQF niveau	Opleiding (%)	Huidig niveau (%)	Toelichting
3	1%	0%	Mbo-3
4	2%	0%	HAVO / MBO-4
5	7%	4%	VWO
6	37%	31%	Bachelor
7	52%	64%	Master
8	1%	1%	Doctor

Overzicht Certificeringen

Certificeringen van het personeel

Niet alle medewerkers zijn gecertificeerd (resultaten voor ABN AMRO, ING en Rabobank). Een groot aantal medewerkers heeft meerdere certificatiescertificeringen. CISSP en CISM zijn en blijven populair. Naast deze zijn er ook nog andere certificeringen binnen de organisatie zoals CRISC, CCSK en SABSA; deze zijn niet opgenomen in de grafiek omdat hier te weinig informatie over was.

Er is een tekort aan cyber security professionals of gewoon informatiebeveiligers in het algemeen

nog veel meer. In de basis betreft het vaak een toets op basiskennis, waarbij een competentietoets (niet alleen weet je het, maar kun je het ook toepassen) wordt uitgevoerd door een ervaringseis en bevestiging door een andere certificaathouder.

Er zijn in de markt veel opleidingen op verschillende niveaus (mbo, hbo, wo) die pretenderen op te leiden tot een niveau in de informatiebeveiliging, zonder dat meteen duidelijk is wat je er mee kunt. Een rondgang op de in 2015 gehouden IB Opleidingenmarkt bevestigde dat beeld. Dat kan het voor studenten (en zij-instromers) lastig maken om de juiste keuze te maken. Op 12 april 2017 wordt opnieuw een IB Opleidingenmarkt gehouden – we zijn benieuwd welke ontwikkeling zich de afgelopen twee jaar heeft doorgezet.

Op basis van het profiel ICT Beveiligings Specialist zijn nu twee mbo-4 keuzedelen door het Ministerie van OCW goedgekeurd (Security in systemen en netwerken 1 & 2). Mbo-studenten die deze extra keuzedelen als verdieping van hun mbo-opleiding ICT-beheerder en Netwerk- en mediabeheerder [8] met succes afronden, zijn daarmee direct gekwalificeerd voor het vakgebied.
Op hbo en universitair niveau (bachelor en master) is nog afstemming nodig om te komen tot een goede afspiegeling tegen de beroepsprofielen. De gesprekken met de diverse hogescholen en universiteiten zijn veelbelovend.

Conclusie

Er is een tekort aan cyber security professionals of gewoon informatiebeveiligers in het algemeen. Waar de financiële sector behoefte aan heeft, is duidelijkheid over wat een dergelijke persoon moet kunnen, zowel wat betreft de technische als de meer 'softe' skills. Dit is te belangrijk om over te laten aan de markt, waar ook andere belangen een rol kunnen spelen: de professie moet dit zelf op een onafhankelijke manier definiëren. Het QIS-framework en certificering biedt hiervoor een hele goede basis.

Referenties

[1] The 2015 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, 2015, URL: http://bit.ly/1GMoD5x
[2] Arbeidsmarkt voor Cyber Security Professionals, PLATO, 2014, URL: http://bit.ly/2lztRRT
[3] ISF Threat Horizon 2018, ISF, 2016, URL: http://bit.ly/2lzxJIY
[4] Beroepsprofielen Informatiebeveiliging 2.0, 2017, URL: http://bit.ly/2mkkxzy
[5] Functies in de Informatiebeveiliging, 2006, URL: http://bit.ly/2mf8Cq7
[6] CEN Workshop Agreement CWA 16234:2014 Part 1, European e-Competence Framework 3.0 - Part 1: A common European Framework for ICT Professionals in all industry sectors; http://bit.ly/1UopNgR
[7] CESG Certified Professional Scheme - the standard for UK Cyber Security professionals, http://bit.ly/2lgTbJH
[8] Keuzedelen Security in systemen en netwerken 1 & 2, www.kwalificatiesmbo.nl

VERSLAG CISO 15

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING

De eerste CISO-bijeenkomst zonder de betrokkenheid van Cees Coumou vond plaats op 8 februari in het BOVAG-huis in Bunnik en werd begeleid door privacy-jurist Rion Rijker van Ilionx Information Security bv.

Bart van Staveren opent de bijeenkomst met een toelichting op de gewijzigde aanpak: nu Cees Coumou niet meer direct betrokken is, zijn Gerard de Weert en Pim van den Hoff bereid gevonden het gat op te vullen. Dit is ook de eerste keer dat het begin van de bijeenkomst niet 15.00 uur is maar 16.30 uur. Dit is voor de aanwezigen een tijdstip dat sterk de voorkeur heeft en beter te combineren met zakelijke activiteiten. Er zijn nu ook ruim meer dan de gebruikelijke dertig leden aanwezig. Dit heeft de inbreng uit de zaal niet beperkt.

Aandachtspunten

Vanaf 25 mei 2018 vervangt de Europese Algemene Verordening Gegevensbescherming (AVG) onze Nederlandse Wet bescherming persoonsgegevens (WBP). Over de verordening doen veel indianenverhalen de ronde: van torenhoge boetes tot hoofdelijke bestuurdersaansprakelijkheid; en van verbod op outbound marketing tot onwerkbare situaties vanwege eindeloos toestemming vragen aan individuen. Maar wat betekent deze verordening nu echt voor uw organisatie? En hoe gaan we als CISO om met deze ontwikkelingen? Hoe kunnen we anticiperen op het moment dat de verordening van kracht wordt?

Rion Rijker heeft zich als privacy-jurist verdiept in de AGV en de verschillen met de WBP. Tijdens CISO 15 bespreekt hij de belangrijkste aandachtspunten uit deze omvangrijke verordening. Aan de hand van casussen trekt hij de discussie over de diverse aandachtspunten open. Rion gaat eerst in op het verschil tussen een Europese Richtlijn en Europese verordening. De WBP is gebaseerd op een Europese richtlijn, waaraan alle staten zelf invulling geven. Vandaar ook grote verschillen tussen de lidstaten van de EU. De Europese verordening gaat verder en geeft heel dirigerend aan wat en deels ook hoe de lidstaten de privacybeveiliging en wetgeving moeten inrichten. Er geldt vanaf mei 2018 nog maar één privacywet in de hele EU, in plaats van 28 verschillende eigen nationale wetten, gebaseerd op de Europese privacyrichtlijn uit 1995. De nieuwe wet zorgt onder meer voor versterking en uitbreiding van privacyrechten van burgers, meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken en steviger bevoegdheden voor alle Europese privacytoezichthouders.
De privacytoezichthouders hebben richtlijnen en FAQ's opgesteld. De autoriteit persoonsgegevens (AP) heeft deze richtlijnen laten vertalen in het Nederlands en heeft Nederlandstalige vragen en antwoorden opgesteld [1].

Rion behandelde de volgende aandachtspunten:

- *Toestemming artikel 7*
  Organisaties moeten kunnen bewijzen dat zij geldige toestemming hebben gekregen. En het moet voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven.
- *Recht op verwijderen artikel 17*
  Cliënten hebben het recht om een organisatie te vragen hun persoonsgegevens te verwijderen. Straks kunnen zij daarnaast eisen dat de organisatie de verwijdering doorgeeft aan alle andere organisaties die deze gegevens van deze organisatie hebben gekregen.
- *Dataportabiliteit artikel 20*
  Cliënten hebben straks (onder bepaalde voorwaarden) het

recht om van de organisatie hun persoonsgegevens in een standaardformaat te ontvangen. Zo kunnen zij hun gegevens makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst. Bijvoorbeeld als zij zich willen uitschrijven bij de ene sociale netwerksite en zich inschrijven bij een andere. Zij kunnen zelfs eisen dat de organisatie hun persoonsgegevens direct doorstuurt aan de nieuwe dienstverlener, als dat (technisch) mogelijk is.

- *Profiling artikel 22*
  Profiling houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie.
- *Verantwoordelijkheden en verantwoordelijken artikel 24*
  Verplichting om aan te kunnen tonen dat de verwerking in overeenstemming met de verordening wordt uitgevoerd. Artikel 40 en 42 stellen hierover dat dit ook kan middels gedragscodes of certificering.
- *Beveiliging van de verwerking artikel 32*
  Adequate technische maatregelen rekening houdend met de stand van de techniek en procedures.
- *Privacy by design artikel 25*
  De verwerkingsverantwoordelijke dient, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen te treffen.
- *Registreren van verwerkingsactiviteiten artikel 30*
  Organisaties hebben een documentatieplicht. Dit houdt in dat zij met documenten moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen. Een van de maatregelen is een register waarin de verwerkings-activiteiten bijgehouden worden (wie heeft wat wanneer, waarom, en hoe bewerkt).
- *Risicoanalyse artikel 35 en 36*
  Bent u van plan persoonsgegevens te verwerken en levert dit een groot privacyrisico op voor de betrokkenen (de mensen van wie u gegevens verwerkt)? Zodra de algemene verordening gegevensbescherming (AVG) van toepassing is, bent u verplicht om dan eerst een Privacy Impact Assessment (PIA) uit te voeren. Hierdoor krijgt u inzicht in wat de risico's zijn en kunt u passende maatregelen nemen om deze te verkleinen. Een PIA wordt ook wel data protection impact assessment (DPIA) of een gegevensbeschermingseffectbeoordeling genoemd. U bent in ieder geval verplicht om een PIA uit te voeren als u:
  - systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profilering;
  - op grote schaal bijzondere persoonsgegevens verwerkt;
  - op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Braafste jongetje van de klas

Nederland heeft met zijn WBP al vergaande wetgeving in de richting van de verordening. Als je al alles netjes volgens de WPB had ingericht, hoef je waarschijnlijk geen grote aanpassingen te plegen. Was je privacybeveiliging nog niet geheel op orde dan is het nu zaak om die op orde te brengen met allereerst het houden van een goede risicoanalyse, die met name ook voor de business de risico's van het niet voldoen aan het licht brengt.

Verdere verdieping

Op http://bit.ly/2j5OR1P staan al de volgende richtlijnen (Guidelines) uitgewerkt:

- Richtlijnen voor functionarissen voor de gegevensbescherming(FG)
- Richtlijnen voor het recht op dataportabiliteit
- Richtlijnen voor het bepalen van de leidende toezichthouder van een verantwoordelijke of verwerker

De meldplicht datalekken, die geldt sinds 1 januari 2016, verplicht organisaties om een ernstig datalek te melden bij de AP. De AP houdt toezicht op de naleving van de meldplicht en heeft deze taak ook in 2017 hoog op de agenda staan. Daarnaast blijft de AP zich richten op situaties waarin de beveiliging overduidelijk niet op orde is. De AP houdt onder meer klantportalen in de gaten. Het is van belang dat organisaties dit soort portalen goed beveiligen, om ervoor te zorgen dat de gegevens van hun klanten niet in verkeerde handen terechtkomen. De gepresenteerde sheets en casussen van CISO 15 zijn te bekijken op het besloten ledengedeelte op de PvIB website (agenda-archief): https://www.pvib.nl/actueel/evenementen/ciso-15.

Referentie

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-publiceren-richtlijnen-europese-privacywet

Geert Martens is sinds 1 februari gepensioneerd als senior ICT/OA- auditor en senior controller bij UWV. Zijn werk bestond de laatste jaren in het inrichten van de control, AO/IB en risicomanagement op de grote geldstroom. Tijdens zijn tijd bij de accountantsdienst van UWV heeft hij het ISO-traject getrokken. Hij is bereikbaar via gjm.martens@hccnet.nl.

TSTC

ICT en Security Trainingen

TSTC is een gerenommeerd IT opleidings-instituut en erkend specialist in informatie-beveiliging- en cybersecurity trainingen.

Security professionals kunnen bij TSTC terecht voor bijna vijftig security trainingen op zowel technisch als tactisch- strategisch gebied. Naast alle bekende internationaal erkende titels is het ook mogelijk diepgang te zoeken in actuele security thema's.

Top 10 Security trainingen

CEH • OSCP • CCSP • CCFP • CISSP • CJCISO • CRISC
Privacy CIPP/E-CIPM • CISM • ISO 27001/27005/3100

Recognition for Best ATC's and CEI's

TSTC Accredited Training Center of the Year 2016

Circle of Excellence Instructor 2016

www.tstc.nl

Want security start bij mensen!!

BOEKREVIEW

HET EERSTE LEERBOEK OP BASIS VAN HET QIS

Ik ben de afgelopen jaren een paar keer betrokken geweest bij het maken van een security-curriculum voor een hbo IT-opleiding. Een leerboek kiezen hoort daar bij. En dan wordt het moeilijk. In het Nederlands is er 'Informatiebeveiliging onder controle', maar dat is vrij theoretisch en specialistisch. Er zijn veel Engelstalige boeken, het nadeel daarvan is de taal, maar ook de zware nadruk op gedetailleerde technische kennis. Veel daarvan is door de dynamiek in het vakgebied alweer verouderd wanneer het boek gebruikt wordt. Deze veroudering is ook het probleem waar het kwalificatiestelsel [1] mee te maken heeft gehad. Er is gezocht naar het zetten van een standaard die de juiste balans tussen toekomstvastheid en specificiteit neerzet.

Dus een boek dat hierop aansluit, is een welkome verschijning in de markt. Dit boek is gericht op het mbo-niveau, en specifiek op profiel ICT Security Specialist 1. Er kan er maar één de eerste zijn, dus dat is op zich een prestatie. Dit boek is echter ook een genot om door te nemen. Het heeft een handzaam formaat, gebruikt kwaliteitspapier en kleurendruk die ook functioneel goed bijdraagt aan het begrip. Een boek dat ik best op het bureau van een menig manager zou willen leggen in de hoop dat ze er iets uit opdoen. Maar daar is het niet voor geschreven. Het is echt een leerboek en daar zit de belangrijkste toepassing ook.

De stof is ingedeeld in negen hoofdstukken, kort gezegd:

1. Principes
2. Wetgeving
3. Dreigingen en kwetsbaarheden
4. Risico-analyse
5. Controls
6. Systeembeveiliging
7. Netwerkbeveiliging
8. Cryptografie
9. Inventarisatie en configuratie

Het hele boek bevat realistische casussen en praktische opgaven die de student aan het denken zetten, ook voordat de antwoorden gegeven worden. Elk hoofdstuk heeft een praktisch onderwerp dat als rode draad fungeert. Ik vind het een hele goede keuze om de vingerafdruk te behandelen (hoofdstuk 5). Het is onmogelijk om alle mogelijke maatregelen te behandelen. Door juist één pittig, actueel onderwerp te kiezen, wordt de theorie ook duidelijk en is het aan de student om dit op andere gebieden te projecteren, met de geleerde handvatten.

Titel: Security in systemen en netwerken
Subtitel: Keuzedeel MBO
Auteur: Jan Dolphijn
Taal: Nederlands
Pagina's: 216
Uitgever: Brinkman Uitgeverij, Amsterdam
Datum: 2016
ISBN: 978-90-5752-348-9

Hoofdstuk 8 en 9 zijn pittige hoofdstukken voor mbo-studenten, ze vragen beiden een uitstapje uit de comfortzone van IT-techniek, naar respectievelijk getaltheorie en procesdenken. En Jan Dolphijn brengt dat goed, in kleine stappen met hapklare brokken.

Ik heb nog gekeken wat er niet in het boek staat, door de focus te houden op het gekozen QIS-profiel. Dat zijn een aantal geavanceerde onderwerpen, die dan ook niet op het beoogde profiel passen:

- De organisatie van informatiebeveiliging
- De menselijke factor
- Structuur in en overzicht over maatregelen
- Diepteonderwerpen zoals IAM, SIEM, BCM
- IB-audit

Als ik één aanmerking moet maken, is het dat er in het boek geen index opgenomen is. Elk hoofdstuk begint wel met een lijst termen, maar het zou beter geschikt zijn als referentieboek als er ook een totaaloverzicht was, met directe verwijzing naar paginanummers in de stof. Verder is het boek nog niet te vinden op de website die wordt genoemd op de achterflap [2], maar dit zal een kwestie van timing zijn. Er staat wél extra materiaal op de website van de uitgever [3].

Alles bij elkaar genomen lijkt het me een goed boek voor mbo-studenten en eventuele anderen die kiezen dit tot zich te nemen. Mijn complimenten aan Jan Dolphijn en de experts om hem heen die hem hierbij geholpen hebben.

Links

[1] QIS: http://bit.ly/2mBQDGA
[2] http://www.mbopraktijk.nl
[3] Brinkman Uitgeverij: http://bit.ly/2I2EZZ7

Door Lex Borger, hoofdredacteur IB-Magazine, security consultant bij i-to-i en docent security aan de Hogeschool Utrecht. Lex is te bereiken via l.borger@i-to-i.nl.

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de 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 kunt u sturen naar ibmagazine@pvib.nl.

TWEEDE KAMERVERKIEZINGEN: KUNNEN WE AL DIGITAAL STEMMEN?

Als u dit leest, zijn de Tweede Kamerverkiezingen inmiddels achter de rug. Vooraf was er veel te doen over mogelijke verstoring van het stemproces, de procedure rondom het tellen van de stemmen, de invloed van 'nation states' op de uitslag, en natuurlijk het gooien met digitale modder door de diverse lijsttrekkers. Wat vinden de redacteuren van uw lijfblad van de gang van zaken, welke bedreigingen en mogelijkheden zien ze, en zou het ook anders kunnen?

Maarten Hartsuijker

Eerlijke verkiezingen zijn onontbeerlijk voor de democratie. Zeker in een tijd waarin het door polarisatie al moeilijk genoeg is om je door de politiek vertegenwoordigd te voelen. Het is daarom essentieel om in het stemproces elke schijn van oneerlijkheid weg te nemen. Met een onveilige stemcomputer kan dus niet gestemd worden. Maar het papieren stemproces is ook niet immuun voor fraude. Stemmen in ontvangst nemen en tellen is mensenwerk. En waar mensen werken, worden fouten gemaakt en is beïnvloeding mogelijk. Zowel het stemmen met een computer als met de hand heeft dus nadelen. Volgens mij zijn deze te reduceren door de mens en de computer elkaar aan te laten vullen. Als in een ICT-proces de juistheid van gegevens belangrijk is, worden over het algemeen aanvullende maatregelen op het gebied van traceerbaarheid/controleerbaarheid getroffen. In het stemproces zou je de controleerbaarheid kunnen vergroten door een uitgebrachte elektronische stem te printen. De stemmer kan zijn keuze vervolgens controleren en in een stembus achterlaten. Het stembureau telt na en controleert de handmatige telling met de totalen van de computer. Zowel de computer als het stembureau geven hun gegevens door. Hierdoor kan er bij de consolidatie nogmaals op fouten en fraude gecontroleerd worden. Als ergens in het proces de computer en de handtelling van elkaar verschillen, kunnen er vervolgens aanvullende controles plaatsvinden. Je zou het een 'drie ogen principe' kunnen noemen: twee van de mens, een van de computer.

Bart van Staveren

Terugkijkend op de verkiezingsperiode, zowel in Amerika als in Europa, zijn mij vanuit de optiek van informatiebeveiliger twee nieuwsfeiten opgevallen die mij aan het denken hebben gezet. In de eerste plaats de pogingen om vanuit het buitenland de websites van politieke partijen en regeringen te hacken en het met de daarmee verkregen informatie beïnvloeden van het democratisch proces in de betreffende landen. Dat regeringen voldoende aandacht moeten besteden aan informatiebeveiliging is geen nieuws en zij hebben hun beveiliging in het algemeen op orde. Iets anders is het gesteld met politieke partijen en individuele politici. Een awareness-programma gericht op deze doelgroep lijkt me zeker noodzakelijk. Professionele ondersteuning van partijen en politici door informatiebeveiligers op rekening van de staat lijkt me een noodzaak. Ook het nieuws over 'trollen' en het via sociale media verspreiden van nepnieuws om zo campagne te voeren vind ik een angstig gegeven. Hoe kunnen we echt nieuws onderscheiden van nepnieuws? Wat is hierbij de rol van sociale

Maarten Hartsuijker | Lex Borger | Bart van Staveren | Tom Bakker | Lex Dunn

De verkiezingen zijn geweest, maar daarmee hebben we nog geen regering en zeker niet één die potentieel de rit uit kan zitten

media? En als het beschermen van de juistheid van gegevens een van de doelstellingen van informatiebeveiliging is, is hier dan een rol weggelegd voor ons vakgebied? Als we deze laatste vraag positief beantwoorden ligt er mogelijk een nieuwe uitdaging voor PvIB.

Tom Bakker

De discussie gaat eigenlijk al minder om het hacken van stemcomputers of risico's bij het tellen van de stemmen, maar meer over het beïnvloeden van het stemgedrag van burgers. Dat is natuurlijk van alle tijden, denk maar gewoon aan de verkiezingscampagnes. Waar het om gaat, is dat via social media burgers beïnvloed worden door het moddergooien van politici en het verspreiden van nepnieuws om de tegenstander zwart te maken. Alles wordt uit de kast gehaald. Als je dan bedenkt dat er ook nog 'datagraaiers' bestaan die vrijwel alles van je weten (profiling) kun je er op wachten dat iemand op een gegeven moment deze informatie gaat kopen en daarmee burgers of bepaalde groepen gericht gaat beïnvloeden. Onwaarschijnlijk? Het kan en als het kan zal het ook gebeuren.

Lex Borger

Directe beïnvloeding van de verkiezingen is wel zo goed als uitgesloten, denk ik. Het proces is landelijk bepaald, we stemmen met het potlood en ook het verwerken van de resultaten is helemaal onder de loep genomen. We moeten ons wel realiseren dat er 'nation states' zijn die er belang bij hebben als de Westerse landen politiek verdeeld zijn en een onstabiele basis hebben, dat verkleint de gecombineerde politieke macht. We hebben ze verschillende sociale platforms gegeven waarop ze die verdeeldheid kunnen zaaien. We hebben dit al gezien bij de Amerikaanse verkiezingen.

Aan de andere kant moeten we zelf ook beseffen dat we voor onszelf met sociale media een wereld hebben gemaakt van snelle likes en dislikes, waarbij de inhoudelijke discussie met diepgaande analyse van feiten met wederzijds respect niet meer mee lijkt te doen. Dit is hoe een sterke samenleving gemaakt wordt. Het tactisch bespelen van sentiment is belangrijker geworden en leidt makkelijker tot een gewenst verkiezingsresultaat. Dat er dan voor de verkozen politici een onmogelijke formeer- en regeertaak wacht, vergeten we even. Ik zie graag de ouderwetse discussie weer terugkomen.

Als jullie dit blad krijgen, zijn de verkiezingen geweest. Maar daarmee hebben we nog geen regering, zeker niet één die potentieel de rit uit kan zitten. Ik ben benieuwd of de informatieronde al gedaan is ...

Lex Dunn

Al jaren zien we van alles en nog wat verschuiven van analoog naar digitaal. Ook onze samenleving wordt steeds digitaler. Waarom zouden we dan ook niet digitaal stemmen? Op zich kan dat heel simpel zijn, en in de praktijk gebeurt dit ook al (recentelijk kreeg ik nog een uitnodiging om via een daarin gespecialiseerde website te stemmen voor een nieuw bestuur van het pensioenfonds). Het gaat daarbij dan om enerzijds vertrouwen in de derde partij, die de stemming organiseert, en anderzijds het onmogelijk maken dat men vaker dan één keer kan stemmen. Ook wil je als kiezer zekerheid dat jouw stem wordt uitgebracht op de door jou gekozen kandidaat. Collega Maarten geeft hierboven al een mogelijk scenario, en collega Bart geeft aan dat hier wellicht een rol voor ons als PvIB is weggelegd.

Een meer zorgwekkende ontwikkeling is de manier waarop social media worden ingezet om niet alleen het eigen standpunt van een partij tot in den treure duidelijk te maken, maar vooral om de politieke tegenstanders tot op het bot af te breken, bij voorkeur met behulp van nepnieuws. Gaan we hier straks ook een kabinet van twitterende nitwits krijgen, waardoor elk nieuw wetsvoorstel tot 140 tekens beperkt zal zijn? Overigens: als u denkt dat de manier waarop de kandidaten hier in Nederland naar elkaar uithalen al erg is, dan had u de recente uitzending van 'Wider den tierischen Ernst' van de Akense carnavalsvereniging moeten zien. De manier waarop de verschillende redenaars politiek gehakt maakten van diverse prominenten (waaronder ook een bekende, blonde Nederlandse politicus) was zeker uitermate leerzaam!

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn
Maarten Hartsuijker (Classity)
Rachel Marbus (KPN)
Bart van Staveren

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
e-mail: secretariaat@pvib.nl
website: www.pvib.nl

ABONNEMENTEN 2017
De abonnementsprijs in 2017 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

SLIMME INVESTERING

Laatst zat ik op een verjaardag en spraken we over de slimme meter. Jullie zullen wel denken 'Dat was een spannende verjaardag' en dat was het inderdaad... Terug naar het gesprek. Een meter die het gas- en elektriciteitsgebruik doorgeeft aan de energieleverancier. Vorig jaar kwam bij mij de vraag binnen of ik zo'n meter wilde. Ik heb daar in mijn enthousiasme "ja" op geroepen. Het monteren was een fluitje van een cent en daarna heb ik nooit meer naar de meter omgekeken.

Eind vorig jaar besloot ik dat het tijd was om mijn dak vol te hangen met zonnepanelen. Het dak heeft de goede hellingshoek, de goede richting voor de zon en is schaduwvrij. Misschien nog wel het belangrijkste: de investering levert op mijn dak meer op dan op de bank. Op een dag was het zover, de panelen werden geplaatst en werden aangesloten op de omvormer. Die is nodig om de stroom die geleverd wordt door de panelen terug te leveren aan de energieleverancier. De omvormer wordt aangesloten op de extra groep in mijn meterkast en nu maar wachten op het moment dat de panelen meer leveren dan dat ik zelf gebruik en er teruggeleverd wordt. Ik zat heerlijk met mijn hoofd in de meterkast mezelf rijk te rekenen. De website die hoort bij de omvormer geeft aan hoe hard de installatie overdag werkt en hoe diep hij 's nachts slaapt.

Ik dacht weer aan de slimme meter en zocht of er een appje was waarmee je kunt zien hoeveel er teruggeleverd wordt. En ja hoor, 'there's an app for that' en dat kun je dus zien. Per dag is standaard en als je het per uur wilt zien, hoef je dat alleen maar even aan te geven. Mijn enthousiasme wordt groter en groter en ik geef aan graag het verbruik per uur te willen zien. Na een aantal dagen is dat geregeld en het is geweldig: in een eenvoudige grafiek wordt duidelijk wanneer ik energie vraag uit het net en wanneer ik energie teruglever. Helemaal gelukkig vertel ik het aan wie het ook maar wil horen.

Totdat ik iemand het verhaal vertel en die mij droog zegt: "dus ze weten precies wat jouw dagritme is en ze weten ook of het huis leeg is". Ik begin te twijfelen en sputter terug dat dat klopt, maar dat mijn kinderen dat ook weten via mijn telefoon. "Dus jij hebt evenveel vertrouwen in de beveiliging van de slimme meter en de energieleverancier als je vertrouwen hebt in de beveiliging van Apple."

Ik slaap die nacht onrustig, wetend dat als de data van elf miljoen belastingbetalers wellicht gekopieerd zijn in het kader van 'makkelijker kunnen we het niet maken, wel veiliger', dat het kopiëren van mijn gegevens bij mijn energieleverancier ook mogelijk zou kunnen zijn. Dat weten ze wanneer ik op het strand lig. Ik kan natuurlijk mijn wasdroger op een schakelklok hangen om hem iedere dag een uurtje energie te laten gebruiken, of de elektrische radiatorkachel op een timer aansluiten om dezelfde reden.

Ik vertel het mijn vrouw, die mij aankijkt en de meest dodelijk reactie geeft die ik me kan bedenken, namelijk het stilzwijgen. Ze heeft gelijk, ik draaf door, denk ik.

Berry

SECURITY ACADEMY

OPLEIDINGENOVERZICHT

INFORMATION SECURITY *CERTIFICATION TRACK*

- S-ISF®: Information Security Foundation opleiding
- S-ISP®: Information Security Practitioner opleiding
- S-ISME®: Information Security Management Expert opleiding

IT-SECURITY *CERTIFICATION TRACK*

- S-ITSF®: IT-Security Foundation opleiding
- S-ITSP®: IT-Security Practitioner opleiding
- S-ITSE®: IT-Security Expert opleiding

PRIVACY & DATA PROTECTION *CERTIFICATION TRACK*

- S-DPF®: Privacy & Data Protection Foundation opleiding
- S-DPP®: Privacy & Data Protection Practitioner opleiding

ETHICAL HACKING *CERTIFICATION TRACK*

- S-EHF®: Ethical Hacking Foundation opleiding
- S-EHP®: Ethical Hacking Practitioner opleiding
- S-EHE®: Ethical Hacking Expert opleiding

BUSINESS CONTINUITY *CERTIFICATION TRACK*

- S-BCF®: Business Continuity Foundation opleiding
- S-BCP®: Business Continuity Practitioner opleiding
- S-BCME®: Business Continuity Management Expert opleiding

Preparation courses

- CISSP® Preparation Course
- CCSP® Preparation Course
- CISM® Preparation Course
- CRISC® Preparation Course
- CISA® Preparation Course

Hierboven ziet u een greep uit ons portfolio. Bij de Security Academy kunt u terecht voor het behalen van verschillende internationale titels van SECO-Institute®, ISC²® en ISACA®. Daarnaast biedt de Security Academy een aantal opleidingen aan op specialistische onderwerpen binnen Security. Denk hierbij aan opleidingen als Internet of Things Security, Encryptie of Social Engineering.
Voor het complete overzicht, meer informatie en cursusdata kunt u terecht op onze website.

www.securityacademy.nl info@securityacademy.nl +31(0)348-40 80 61