iB
INFORMATIEBEVEILIGING
jaargang 15 - 2015
#2

DREIGINGEN EN KWETSBAARHEDEN

Logging - Niet Dat, maar Wat en Hoe

Near Field Communication rukt op...

KeePass: een einde aan wachtwoord-ergernissen

SECURITY Academy

NIEUWE OPLEIDINGEN

Privacy Officer

De privacy wet- & regelgeving (Wbp) is voor ieder bedrijf van belang en krijgt steeds meer aandacht van o.a. het College Bescherming Persoonsgegevens.
U leert in deze 3-daagse opleiding de prangende privacy vraagstukken binnen uw organisatie te vertalen naar risico's in uw eigen omgeving en daarop adequaat advies te vervaardigen.

De opleiding bestaat uit 6 modules:

- Module 1: Ontstaan van de Wbp
- Module 2: Richtlijnen
- Module 3: Privacy in uw organisatie
- Module 4: Rechten en plichten
- Module 5: PIA & Privacy audit
- Module 6: Privacy & calamiteiten

De opleiding tot Privacy Officer is uniek omdat er een begrijpbare vertaling wordt gegeven vanuit wet- en regelgeving (met praktijkvoorbeelden) waardoor u voldoende kennis verkrijgt om adviezen te geven inzake de privacy vraagstukken binnen uw organisatie en u als gesprekspartner kunt fungeren met de diverse (management)lagen binnen uw organisatie en externe partijen.

De cursusprijs bedraagt € 1.950,- euro exclusief BTW. Dit is inclusief cursusmateriaal, catering.

CISSP® Fast Track Prep. Course

Tijdens deze 6-daagse CISSP Fast Track opleiding wordt u opgeleid tot een breed onderlegde specialist op het gebied van informatiebeveiliging. Na afronding van de opleiding heeft u een gedegen kennis van de 10 CISSP-domeinen om deze in de praktijk te kunnen toepassen en bent u geheel voorbereid op het internationale CISSP-examen.

Deze CISSP Fast Track opleiding is bedoeld voor cursisten die al veel ervaring hebben in het vakgebied informatiebeveiliging (minimaal 5 jaar). Omdat er 2 domeinen per dag worden behandeld in de CISSP Fast Track zal het tempo hoog liggen.

De cursusprijs bedraagt € 3.900,- euro exclusief BTW. Dit is inclusief cursusmateriaal, catering maar exclusief het (ISC)2 CISSP examen.

BEL ONS +31(0)348-408061

WWW.SECURITYACADEMY.NL
INFO@SECURITYACADEMY.NL

INNOVEREN IS AANVALLEN

Ik vertel regelmatig over de security-paradox: als beveiliger moet je jezelf tegen alle scenarios verdedigen, als aanvaller heb je aan één succesvol scenario genoeg voor een doorbraak. Om die verdediging op te zetten heb je al snel een hele organisatie nodig, met beleid, standaarden en richtlijnen.

Dit geeft de aanvaller een voordeel: hij heeft geen logge organisatie nodig en kan zich heel innovatief opstellen. Innovatie is in de basis niets anders dan iets nieuws proberen, met de verwachting dat je meestal zult falen, maar af en toe een succes zult hebben.

En als je dat een stap verder neemt, ga je leren van je successen en daarop voortbouwen. En dat is precies wat je hackers ziet doen, of ze nou voor overheden of criminele organisaties werken, of onafhankelijk werkzaam zijn. Je zou dit agile werken kunnen noemen.

Verdedigen leidt dus kennelijk tot organiseren en documenteren, en het resultaat is niet veranderingsgezind. Aanvallen leidt daarentegen tot innovatief, agile gedrag, met een minimum aan organisatie en documentatie. Het is als een voetbalcoach die tijdens de wedstrijd de opstelling verandert. Agile werken, dat ken ik, het werkt. Om succesvol zaken te doen moet je snel kunnen handelen, met continue innovatie. Agile dus. Maar dan komen we wel ergens dezelfde paradox weer tegen: de organisatie is ingericht met afdelingen en functies, een verdeling van taken, bevoegdheden, verantwoordelijkheden, met beleid, standaarden en richtlijnen. Statisch dus. Log. En hier komt de organisatie zichzelf weer tegen. Hoe kan agile samengaan met de traditionele organisatie?
Als beveiliger in deze tijd leren we al om met deze paradox om te gaan: wees geen nee-zegger, maar denk mee met de business. Denk als een aanvaller, wees bereid om soms buiten het boekje te werken, wanneer de beloning opweegt tegen het risico. Wees daar transparant over. Risk-based-werken noemen we dat.

Kun je zonder beleid, standaarden, richtlijnen? Nee, het horen je hygiëne-regels te zijn. Kunnen ze lean worden? Ja. Hoe moet dat? Om daar achter te komen moet je vooral je business goed kennen, zodat je de discussie kunt voeren. Traditioneel verdedigend ga je onderuit.

Lex Borger, hoofdredacteur

In dit nummer

ISO 27001 IN HET MKB: EEN FLINKE UITDAGING

'Het midden- en kleinbedrijf is de motor van onze economie en aanjager van innovatie.' aldus onze Minister van Economische zaken. MKB-bedrijven zijn informeel, ondernemend, flexibel en kennen weinig bureaucratie. Met een krap budget weten ze toch een hoop te bereiken. Deze eigenschappen zorgen er wel voor dat het een uitdaging is om de ISO 27001 certificering voor informatiebeveiliging te behalen.

De meeste normenkaders voor informatiebeveiliging zijn universeel van scope en houden geen rekening met de verschillen tussen organisaties [1]. Zo is ISO 27001 niet ontworpen met kleinere bedrijven in het achterhoofd [2]. De norm schrijft een proces en methode voor om risico's te onderkennen en maatregelen te implementeren, maar veel MKB-bedrijven hebben nou eenmaal weinig formele processen. Daarbovenop komt vaak een gebrek aan geld, tijd, prioriteit en benodigde expertise. In dit artikel vind je een verkenning van de uitdagingen en een lijst met aanbevelingen. Deze aanbevelingen zijn het resultaat van academisch literatuuronderzoek in combinatie met een rondgang langs verschillende Nederlandse MKB-bedrijven.

Managementaandacht

Ondernemers zijn goed in het bewust nemen van risico's. Deze risicobereidheid zorgt ervoor dat ondernemende MKB-bestuurders vaak liever investeren in nieuwe kansen dan in security. Ook zijn ze vaak zo druk met de dagelijkse operatie, dat security niet hoog op de agenda staat. Zeker als er nog nooit een heftig security-incident is geweest, is de motivatie laag om tijd en geld te investeren in het schrijven van een informatiebeveiligingsbeleid [3]. De wens om toch aan ISO 27001 te beginnen komt daarom vaak uit de commerciële hoek: het is een eis van een klant of bij een aanbesteding.

Een MKB-bedrijf heeft per definitie een relatief klein aantal medewerkers en een vaak platte, informele organisatiestructuur met korte communicatielijnen. Juist omdat de directie dagelijks in nauw contact staat met hun personeel is het vertrouwensniveau hoog [3] en kan het zijn dat de kans op een incident wordt gebagatelliseerd.

Gebrek aan middelen

Bestuurders weten vaak wel dat een beveiligingsincident flinke reputatie- en imagoschade kan opleveren. Maar dat dit zelfs het einde van het bedrijf kan betekenen is niet altijd bekend. De gevolgen kunnen escaleren door een juridische nasleep, boetes, hoge reparatiekosten en hogere verzekeringskosten na het incident [4]. MKB-bedrijven hebben niet altijd voldoende buffers en inkomsten om een dergelijke klap op te vangen.

Maar juist die krappe budgetten zorgen ervoor dat security maatregelen worden uitgesteld. Security goed doen is namelijk duur. ISO 27001-certificering behalen en behouden is nog duurder. Het vereist een continue inspanning die vaak wordt onderschat. Er is ook sprake van een negatieve spiraal: als er weinig geld wordt besteed aan beveiliging, zal het bewustzijn

van de risico's ('awareness') laag zijn, waardoor er nóg minder in beveiliging zal worden geïnvesteerd [2].

Een complicerende factor is dat ISO 27001 functiescheidingen voorschrijft. Bij interne audits mag men niet zichzelf controleren bijvoorbeeld. Als er weinig mensen zijn kan het lastig zijn deze verantwoordelijkheid te beleggen. Extra mensen aannemen of externe consultants inhuren is dan de enige (dure) oplossing.

Gebrek aan benodigde kennis

Het kan zijn dat het behalen van het ISO 27001 certificaat wordt gezien als een "IT-project", terwijl het in werkelijkheid om bedrijfsrisico's gaat die veel breder zijn dan alleen IT. Als dit niet wordt onderkend door het management kan het lastig zijn om de security activiteiten op alle benodigde afdelingen in de organisatie te laten landen. Het krijgt dan simpelweg geen prioriteit.

Soms is technische IT-expertise wel aanwezig, maar is er geen kennis aanwezig van het uitvoeren van risicoanalyses, het ontwikkelen van een beveiligingsbeleid en het continu verbeteren van het proces volgens ISO 27001 [5].

Weinig formele processen

Veel MKB-bedrijven hebben weinig tot geen formele processen. Dat is prettig want daardoor kunnen ze flexibel zijn en snel inspelen op veranderingen en klantvragen. Collega's hebben de ruimte om zelf te bepalen hoe ze hun werk doen en worden aangemoedigd van het gebaande pad af te wijken.

Als de beveiligingsmaatregelen te strikt zijn, komt de effectiviteit in het geding [6]. Bovendien is deze vloeibare structuur lastig te verenigen met ISO 27001, omdat deze norm een aantal formele processen voorschrijft. Bepaalde veranderingen mogen niet zomaar worden doorgevoerd en moeten goed worden gedocumenteerd zodat dit later kan worden gecontroleerd. Er is een precieze beschrijving van beleid, procedures, beslissingen en reviews nodig. Deze documenten kunnen natuurlijk eenmalig worden opgesteld om het certificaat te behalen, maar als de documentatie in de praktijk niet gebruikt wordt, zal deze snel verouderen. Bij de eerstvolgende audit blijkt de beschreven situatie niet meer te lijken op de werkelijkheid die wordt aangetroffen [5].

Bij bedrijven die aan agile systeemontwikkeling doen, wordt er soms voor gekozen om zo min mogelijk documentatie bij te houden. Het agile manifesto zegt immers: "working software over comprehensive documentation". Als er vervolgens tijdens een audit moet worden aangetoond welke wijzigingen er zijn geweest aan welke componenten kan dat ingewikkeld zijn.

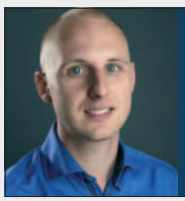
Om compliance aan ISO 27001 aan te kunnen tonen is een bepaalde mate van 'procesvolwassenheid' benodigd. Het Capability Maturity Model (CMM) beschrijft niveaus van procesvolwassenheid van een organisatie. Uit onderzoek blijkt dat een CMM-niveau van lager dan 4 ervoor zorgt dat de zekerheid die het ISMS biedt beperkt is [7]. Omdat veel MKB-bedrijven niet verder komen dan het eerste of tweede niveau kan dit een probleem opleveren.

Aanbevelingen

De volgende aanbevelingen kunnen helpen om toch met succes informatiebeveiliging te bedrijven in het MKB:

- Onderschat de impact en benodigde middelen voor het behalen en behouden van een ISO 27001 certificering niet. Bekijk daarom goed of certificering echt gewenst is door een grondige kosten-baten analyse te maken. Het kan wellicht beter zijn om eerst klein te beginnen door een basis te leggen en de awareness te verhogen. Het kan helpen om te werken vanuit de 'principes' van ISO 27001, zonder precies de processen te willen volgen.

- Zorg voor voldoende kennis van het management van de mogelijke gevolgen van een beveiligingslek, zodat er urgentie en commitment ontstaat om maatregelen te nemen. Hou hierbij vooral de bedrijfsrisico's in de gaten om te voorkomen dat het geheel als een 'IT project' wordt gezien. Zorg ervoor dat de rol van security officer expliciet wordt belegd, en dat deze persoon het juiste mandaat en middelen heeft om effectief te kunnen zijn.



Jurriaan Kamer is interim CIO gespecialiseerd in agile transformaties. Hij was verantwoordelijk voor IT-security in verschillende MKB-bedrijven en in 2012 leidde hij de nieuwbouw van de software van DigiD.
Twitter: @kajurria. Blog: www.kajurria.nl.

Streef certificering niet alleen na voor het papiertje

- Schakel professionele hulp in en zorg voor voldoende training voor de mensen die betrokken zijn bij de implementatie.
- Verhoog de succeskans door de implementatie 'lean en mean' te doen: voorkom bureaucratisering zoveel mogelijk door pragmatisch om te gaan met de ISO 27001 eisen. Bepaalde zaken kunnen gecombineerd worden, zonder dat dit de certificering in de weg staat.
- Het is niet aan te raden de ISO 27001 werkzaamheden los te zien van de dag-tot-dag operatie. Probeer het werk zoveel mogelijk te in te bouwen in bestaande processen. Als er geen formele processen zijn kan dit erg lastig zijn, dus overweeg om de procesvolwassenheid van bepaalde activiteiten eerst te verhogen, alvorens met de implementatie te beginnen.
- Streef certificering niet na alleen voor het papiertje maar blijf gefocust op resultaten en de uiteindelijke business value die het oplevert.

Over het onderzoek

Dit onderzoek werd uitgevoerd in het kader van de Executive MBA in Business & IT (Nyenrode Business Universiteit). Om oorzaken en aanbevelingen te vinden werd er een academisch literatuuronderzoek gedaan. De zoektocht leverde 12 relevante artikelen van voldoende kwaliteit op. De bevindingen werden vervolgens getoetst in interviews met eindverantwoordelijke IT (security) managers van drie verschillende Nederlandse MKB-bedrijven. Het onderzoek heeft een aantal pragmatische inzichten opgeleverd. Om de academische waarde verder te vergroten zou het onderzoek kunnen worden uitgebreid naar een grotere groep bedrijven.

De in dit artikel genoemde aspecten zijn niet uniek voor ISO 27001. Uit de literatuur [8][9] blijkt dat MKB-bedrijven die ISO 9000 of Total Quality Management (TQM) implementeren, met vergelijkbare uitdagingen te maken krijgen. Deze frameworks zijn ook gebaseerd op de PDCA-cyclus van continue verbetering en kennen een hoge mate van formele documentatie.

Links

[1] Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270. http://bit.ly/1CwliW9 (betaalmuur)

[2] Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: a holistic approach. In ISSE/SECURE 2007 Securing Electronic Business Processes (pp. 331-339). http://bit.ly/17zlA5S

[3] Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: an empirical examination. Information Management & Computer Security, 13(4), 297-310. http://bit.ly/1DUGqK5 (betaalmuur)

[4] Henson, R., & Hallas, B. (2009). SMEs, Information Risk Management, and ROI. http://bit.ly/1AXLIUh

[5] Coles-Kemp, E., & Overill, R. (2007, July). The Design of Information Security Management Systems for Small-to-Medium Size Enterprises. In Proceedings of the 6th European Conference on Information Warfare & Security (p. 47). Academic Conferences Limited. http://bit.ly/1vNHPeJ

[6] Anderson, J. (2013). Information Security for SME's. IT Practices for SME Success Series, The Role of IS Assurance & Security Management, 11-14. http://bit.ly/1vME66P

[7] Spears, J. L., Barki, H., & Barton, R. R. (2013). Theorizing the concept and role of assurance in information systems security. Information & Management,50(7), 598- 605 http://bit.ly/1zgwsNN (betaalmuur)

[8] Lafuente, E., Bayo-Moriones, A., & Garci?a-Cestona, M. (2010). ISO-9000 Certification and Ownership Structure: Effects upon Firm Performance. British Journal of Management, 21(3), 649-665. http://bit.ly/1F2fuWQ

[9] Price, M. J., & Chen, E. E. (1993). Total quality management in a small, high- technology company. California Management Review, 35(3), 96-117. http://bit.ly/1F2fA0M (betaalmuur)

OME IVO

Ik had ooit een oom, laten we hem om redenen van privacy Ivo noemen. De man had een bulderende lach hetgeen vriend en vijand reden gaf tot imitatiedrang. De beste "Ivo" kreeg op feestjes altijd het grootste stuk taart. Nu zult u denken, dat was vast een geliefd man. Dat was hij ook wel, onder zijns gezinden. U weet wel, het eigen soort mensen. Want bij ome Ivo was het altijd veilig, dat vond hij namelijk het allerbelangrijkste. Althans, hij hield er altijd zo van om mensen het gevoel te geven dat ze veilig waren. En warempel waren er dus mensen die dachten dat dat hielp al die dingen die ome Ivo deed om het veiliger te maken.

Ome Ivo hield heel erg veel van ome Fred (laten we hem Fred noemen om redenen van privacy). Ome Fred geloofde ook al zo in veiligheid. Ze waren een goed stel. Samen konden ze de wereld aan. Ze waren wel wat selectief in gehoor, maar goed, dat heb je natuurlijk al snel bij oude heren. Die horen graag alleen wat ze zelf willen horen en als iets ze niet bevalt dan doen ze gewoon wat ze zelf willen. Zo had ik ooit een tante die stelde dat je taart in één keer moet opeten en dat je die zeker niet tot in de eeuwigheid moet bewaren. Ome Fred pakte dan pardoes de taart en dumpte het ding in de vriezer. Bulderlachend riep ome Ivo dan: wie wat bewaart die heeft wat!

Ome Ivo hield erg van verzamelen en bewaren. Zijn hele huis stond vol met spullen die hij van anderen had onderschept om zo maar zijn verzamelingen compleet te maken. Hij was een nauwkeurig man, die nauwgezet hele boekwerken bijhield van alles wat hij samen met ome Fred deed. Dat hoorde zo. Hij was ook erg zuinig op die boekwerken, want als je vroeg of je ze mocht inkijken dan kreeg je bijna altijd nul op het rekest. En als je ze dan toch een keer onder ogen kreeg, zaten ome Ivo en ome Fred er altijd bij om bepaalde pagina's zo snel mogelijk om te slaan zodat je die niet kon lezen. Want ze hielden wel erg van hun eigen privacy en geheimen. De eigen geheimen moeten goed bewaard worden, bulderde ome Ivo dan altijd. Ja, die ome Ivo had toch echt een bewaarfetish.

Hoewel ome Ivo en ome Fred hun hele leven samen zijn gebleven, liep het toch niet goed met hen af. Hun huis bezweek onder de verzamelde troep. Het was op goede dag zelfs zo erg dat ze verplicht bezoek kregen van een schoonmaakploeg. Toen kwamen al die boekwerken natuurlijk ook tevoorschijn. U begrijpt, we hebben gesmuld van de verhalen daarin. Die gekke ome Ivo en ome Fred deden gewoon maar wat om de schijn op te houden. Dat al hun plannetjes eigenlijk helemaal niet werkten, maakte hen niet zoveel uit. Niet lang na die schoonmaakploeg moesten ze het huis verlaten. Daarna heb ik eigenlijk niet meer zoveel van ze gehoord.

Mr. Rachel Marbus,
@rachelmarbus op Twitter

Dit is de eerste van twee artikelen van Jean Coenen over logging management. In het eerste artikel gaat Jean in op het waarom en het wat van logging. In het volgende deel gaat hij in op de inrichting van logging; het Hoe.

De redactie

LOGGING

Niet Dat, maar Wat en Hoe

Dat

Bij veel organisaties groeit het besef dat er logs bijgehouden moeten worden over het gebruik van informatiesystemen; variërend van bedrijfsapplicaties tot ICT-apparatuur. Het alsmaar toenemende aantal incidenten plus veranderde wet- en regelgeving maakt het noodzakelijk dat logging plaatsvindt. Het nemen van de juiste verantwoordelijkheid door directie en bestuur en de verantwoording daarover naar toezichthouders vereisen dat er logs beschikbaar zijn. Als er serieuze incidenten zijn of misbruik van gegevens plaats heeft gevonden, wordt ervan uitgegaan dat er loggegevens zijn die helpen bij het opsporen van oorzaken en het oplossen van problemen. Logs bieden tevens de mogelijkheid dat medewerkers hun verantwoordelijk kunnen nemen voor uitgevoerde taken en werkzaamheden en dit kunnen aantonen. Bij deze situaties komen organisaties er veelal achter dat de noodzakelijke informatie uit logging niet voorhanden is.

Nadat is vastgesteld dat logging noodzakelijk, handig en nuttig is, is de volgende stap de daadwerkelijke implementatie van passende logging inclusief het gebruik ervan. Op een gestructureerde manier moet worden gekomen tot een set van logs die antwoord geeft op de vragen die we hebben, op de momenten dat verantwoording nodig is. Problemen moeten geanalyseerd, verklaard en eventueel opgelost kunnen worden. Hoe kunnen we komen tot een gestructureerde inrichting en effectief en efficiënt gebruik van logging? Wat is er nodig om aan de informatiebehoefte te voldoen en daarmee op momenten van verantwoording en analyse over de juiste en relevante informatie te kunnen beschikken?

Vaak worden door de implementatie van logging veel loggegevens opgeslagen, maar leveren deze weinig of zelfs geen toegevoegde waarde voor een organisatie. Er bestaan geen afspraken of standaardwerkwijzen hoe logs omgezet worden tot informatie die gebruikt kan worden om problemen, afwijkingen en misstanden te ontdekken, analyseren en corrigerende maatregelen te treffen.

Het opslaan van loggegevens zorgt, als er sprake is van een ongestructureerde aanpak, voor extra en onvoorziene kosten. De grote hoeveelheid aan loggegevens kost extra opslagcapaciteit en het aanmaken, opslaan en verwerken ervan kost extra verwerkingscapaciteit. Het bewerken en verwerken van loggegevens zorgt voor extra werk dat niet voorzien is. Deze aspecten zijn voor de ICT-afdeling meestal de belangrijkste criteria om (extra) logging al dan niet te activeren, terwijl voor het maken van deze keuze niet wordt gekeken naar het nut en de noodzaak voor de organisatie.

De 'wat'-vraag kan worden beantwoord als aan de hand van de LogCycle duidelijk wordt in welke stadia loggegevens zich kunnen bevinden. Hieruit valt af te leiden welke activiteiten noodzakelijk zijn om optimaal gebruik te kunnen maken van logging. De LogCycle kent de volgende 6 stadia:

1. **Datacollectie**
2. **Opslag loggegevens**
3. **Normalisatie**
4. **Onderzoek en signalering**
5. **Presentatie**
6. **Vernietiging loggegevens**

De 'hoe'-vraag kan worden ingevuld door een proces voor logmanagement in te richten en te implementeren. Logmanagement kan er in 4 fasen voor zorgdragen dat logging effectief en efficiënt wordt gebruikt als regulier onderdeel van de bedrijfsvoering. Het logmanagement proces ziet er als volgt uit:

1. **Bepaal de doelstellingen**
2. **Implementeer een logsysteem**
3. **Meet de werking**
4. **Stel de doelstelling en de eisen bij**

De combinatie van uw antwoorden op de 'wat'- en de 'hoe'-vraag zullen leiden tot een succesvolle, effectieve en efficiënte inrichting van logging. We hoeven niet langer te blijven hangen bij de constatering dat we moeten loggen, maar kunnen overgaan tot het smeden van een aanvalsplan.

Wat

Om te bepalen welke logs kunnen bijdragen aan de bedrijfsvoering, is het goed om onderscheid te maken tussen het loggen van technische gebeurtenissen in ICT-apparatuur en het loggen van gebeurtenissen in (bedrijfs-) applicaties. De eerste categorie van logging wordt veelal gebruikt om de exploitatie van de ICT omgeving te ondersteunen en om snel op afwijkingen en incidenten in te kunnen spelen. Logging in applicaties is van belang om het gebruik van bedrijfsinformatie door gebruikers vast te kunnen stellen. Dit is relevant als een organisatie zich moet verantwoorden over het gebruik van bepaalde informatie (denk bijvoorbeeld aan persoonsgegevens) of als een gebruiker de

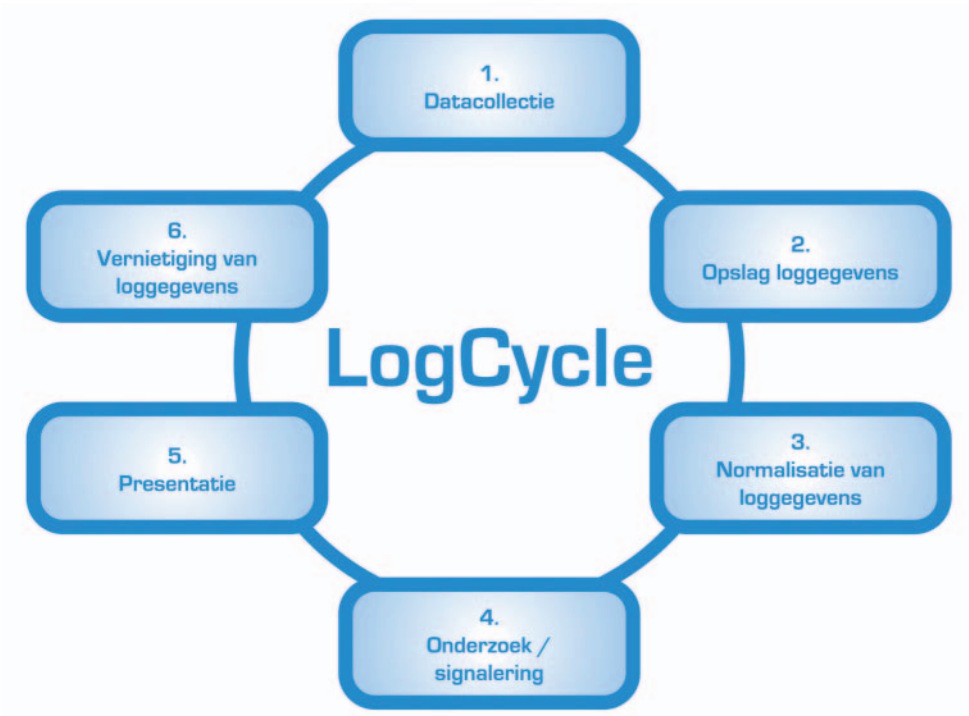
Jean Coenen is security consultant bij Saganto. Hij is per de e-mail bereikbaar via Jean.Coenen@saganto.nl

verantwoordelijkheid wil nemen voor de uitgevoerde taken en werkzaamheden.

Een ander onderscheid bestaat er tussen logging die (bijna) real-time de operatie in de gaten kan houden en logging die opgeslagen wordt voor analyse op een later tijdstip. Hiermee komen we tevens op het onderscheid tussen logging en monitoring, waarbij met monitoring een omgeving continu in de gaten wordt gehouden. Zolang de werking conform de gestelde verwachting is, zal het logsysteem geen actie ondernemen. Op basis van gedefinieerde afwijkingen en grenswaarden voor processen kunnen afwijkingen (excepties) worden herkend en zal direct een (re)actie volgen.

Als logging wordt ingericht op basis van behoeften van de organisatie, dan is de daarvoor benodigde capaciteit alleen nog maar een eis voor het systeemontwerp en daarmee een noodzakelijk onderdeel van een informatiesysteem. De kosten voor logging zijn verantwoord en de logbestanden leveren, op de juiste momenten, bruikbare en noodzakelijke informatie aan de organisatie. Bedreigingen, risico's en verplichtingen voor de bedrijfsprocessen leiden tot een zinvolle definitie van logging, een optimale set van loggingsgegevens (niet te veel en niet te weinig) en nuttige informatie. De diepgang van de informatie is bepalend voor het detailniveau waarop gegevens gelogd dienen te worden en bepalend voor de hoeveelheid loggegevens.

Om een logsysteem structureel vorm te geven is het noodzakelijk om inzicht te hebben in de mogelijkheden en de te hanteren uitgangspunten van logging. Belangrijke uitgangspunten en randvoorwaarden zijn het gevolg van het stadium waarin loggegevens zich kunnen bevinden. In de LogCycle worden deze verschillende stadia beschreven.



LogCycle

Er bestaat een aantal stadia waarin loggegevens zich kunnen bevinden, variërend van het ontstaan van loggegevens tot het verwijderen van loggegevens. De LogCycle beschrijft deze stadia en daarmee de handelingen die uitgevoerd moeten worden om loggegevens optimaal te kunnen gebruiken. Tevens zijn er voor elk stadium voorwaarden waaraan voldaan moet worden om de betrouwbaarheid en de vertrouwelijkheid van loggegevens te waarborgen.

Stadium 1. Datacollectie

Is het verzamelen van gegevens die als nuttige en bruikbare loggegevens kunnen worden aangemerkt; dit kan zowel systeeminformatie als ook applicatie-informatie betreffen. Loggegevens sluiten aan bij het doel dat de organisatie voor ogen heeft. Daartoe bevat een te loggen gebeurtenis minimaal een aantal gegevens zoals: (gebruikers)ID, startdatum, starttijd, eindtijd en een transactiecode. Als loggegevens in een informatiesysteem worden opgeslagen, dan wordt deze collectie vaak geactiveerd via een (standaard)functionaliteit in de applicatie. Bij gebruik van een centraal SIEM-tool wordt voor

het verzamelen van loggegevens een collector gebruikt; deze wordt soms ook wel parser genoemd. Bij de implementatie van een SIEM-tool wordt bepaald welke gegevens uit welke informatiesystemen en bijbehorende tabellen verzameld worden.

> In de collector / parser is vastgelegd uit welke bron welke gegevens opgehaald moeten worden en deze zal deze ongewijzigd centraal in de SIEM-omgeving als authentieke data opslaan. Hiermee kunnen bijvoorbeeld alle transacties van klanten uit diverse applicaties verzameld en aan elkaar gecorreleerd

Stadium 2. Opslag loggegevens
Opslag van loggegevens betreft originele en authentieke data. Indien logging gebeurt in een informatiesysteem, dan zijn hiervoor bij voorkeur separate tabellen beschikbaar, gescheiden van operationele data. Een SIEM-tool slaat de authentieke loggegevens op in een eigen database. De opslag van de originele loggegevens moet ervoor zorgdragen dat de authenticiteit gewaarborgd is. Loggegevens dienen hiertoe beschermd en beveiligd te worden. De loggegevens worden slechts eenmalig opgeslagen, zodat ze te allen tijde uniek zijn. Tevens worden deze loggegevens voorzien van read-only maatregelen, zodat ze nooit gewijzigd kunnen worden. Loggegevens worden idealiter versleuteld en voorzien van specifieke toegangsbeveiliging.

Stadium 3. Normalisatie van loggegevens
Deze fase is niet van toepassing wanneer loggegevens in een informatiesysteem zijn opgeslagen, omdat bedrijfsapplicaties meestal niet over deze functionaliteit beschikken. Bij een SIEM-tool worden voor optimaal gebruik van de logging de authentieke loggegevens genormaliseerd. Dit betekent dat er op de oorspronkelijke loggegevens filters worden toegepast om gegevens in geaggregeerde vorm op te slaan in aparte tabellen. Het doel hiervan is om de toegang en het gebruik van loggegevens te versnellen en te vereenvoudigen. Leveranciers van SIEM-tools hebben vaak een eigen methode voor het filteren en het opslaan van deze geaggregeerde loggegevens. Het normaliseren zal nooit de authentieke loggegevens wijzigen.

Stadium 4. Onderzoek en signalering
Betreft het definiëren van selecties en filters die moeten leiden tot het presenteren van de gewenste inzichten; denk hierbij bijvoorbeeld aan drempelwaarden, trends en ongewenste afwijkingen. Beheerders en gebruikers van het logsysteem bedenken en implementeren standaardoverzichten of op verzoek maatwerkinzichten. Gebruikers zijn specifiek geautoriseerd om toegang te krijgen tot het logsysteem en kunnen rapportages, dashboards en alerts maken en opslaan voor regulier of incidenteel gebruik. Alleen geautoriseerde gebruikers mogen gebruik maken van de mogelijkheden van het logsysteem.

Stadium 5. Presentatie
Dit betreft het daadwerkelijk gebruik van de loggegevens door de (vertegenwoordigers in de) gebruikersorganisatie. Dit kan variëren van het presenteren van overzichten en rapportages, tonen van resultaten en statistieken in dashboards tot het realtime genereren en/of versturen van alerts en meldingen in diverse vormen. Dit stadium zal, samen met stadium 4., de langste periode van de LogCycle bestrijken.
Van groot belang is de vertrouwelijk behandeling van de resultaten. Veelal zijn de loggegevens te herleiden naar een persoon en dienen ze navenant vertrouwelijk toegankelijk te zijn en gebruikt te worden. Ondanks de gerealiseerde toegangsbeveiliging in het logsysteem is het van groot belang dat resultaten, die in papieren vorm of digitaal buiten het logsysteem beschikbaar zijn, denk aan back-ups, net zo vertrouwelijk worden behandeld.

Stadium 6. Vernietiging van loggegevens
Zowel de authentieke als ook de geaggregeerde loggegevens dienen, als de rententieperiode afloopt, vernietigd te worden. Zoek altijd naar de, voor de toepassing, vigerende bewaartermijn en respecteer deze. Bedenk hierbij ook dat loggegevens in een backup-systeem wellicht langer beschikbaar blijven, ook al worden de gegevens in het logsysteem vernietigd. Het verwijderen van de residu-kopiegegevens behoeft dan specifieke aandacht, maatregelen of gebruiksprocedures.

Financiële informatie	minimaal 7 jaar
Medische patiëntendossiers	minimaal 15 jaar
Loggegevens computersystemen	maximaal 6 maanden
Identificatiebewijs	minimaal 5 jaar

Enkele algemeen bekende voorbeelden van vastgestelde bewaartermijnen (deels op basis van de termijnen zoals in wet- en regelgeving zijn voorgeschreven).

VEILIGER MET VOORKENNIS

Deel 2

"People think focus means saying 'Yes' to the thing you've got to focus on. But that's not what it means at all. It means saying 'No' to the hundred other good ideas that there are. You have to pick carefully. I'm actually as proud of the things we haven't done as the things I have done." – Steve Jobs

Voor organisaties is het belangrijker dan ooit om te weten hoe ze de steeds sneller ontwikkelende IT veilig kunnen benutten. In deel 1 heb ik aangegeven waarom een systematische analyse nuttig is om de effecten van veranderingen te bepalen en welke kennis organisaties meestal missen bij de invulling van risicomanagement. Onder de druk van prestatieverbetering en efficiency voeren organisaties nieuwe technologieën in, ook als de risico's voor de bedrijfsprocessen nog niet bekend zijn. In dit tweede deel van dit artikel belicht ik de risico's en kansen van enkele nieuwe ontwikkelingen, zoals de toenemende complexiteit, het voortdurend opschalen van organisaties en systemen en de invloed van quantum-computers.

Grotere complexiteit, toenemende onvoorspelbaarheid

Hoewel er steeds meer data beschikbaar is, leidt dat niet altijd tot goede informatie. Als de verwerking van data onvoldoende rekening houdt met ruis, vermindert dat de kwaliteit van beslissingen. Zo bleek uit een Ernst & Young ICT Barometer over 2009 dat ca. 38% van alle organisaties malware infecties rapporteerden. Het rapport over 2010 signaleerde voorzichtig een lichte verbetering ten opzichte van vorig jaar, omdat dit percentage was gezakt naar 33% [10]. Het is echter weinig aannemelijk dat in 2010 meer organisaties erin slaagden alle besmettingen te ontlopen. Beide E&Y rapporten geven namelijk ook aan dat cybercrime juist aan het toenemen is. Verder is bekend dat veel organisaties steeds huiveriger zijn om publiekelijk toe te geven dat hun systemen waren besmet met malware. Klopt het in eerste instantie ogenschijnlijk positieve signaal dus eigenlijk wel?

Beide rapporten bevatten de percentages van organisaties waarvan de systemen dat jaar niet, eenmalig of vaker zijn besmet, zodat een statistische analyse mogelijk is. Voor de analyse is het uitgangspunt dat opgetreden besmettingen onafhankelijk zijn van elkaar [11]. Uit de analyse volgt dat in 2009 ca. 49% van de organisaties in het rapport gemiddeld 1,50 besmettingen per jaar hadden [12]. Dezelfde analyse op de cijfers van 2010 laat echter zien dat voor ca. 42% van de organisaties het aantal jaarlijkse besmettingen groeide naar 1,54. Doordat meer organisaties "nul" besmettingen rapporteerden, ontstaat op basis van deze ruis een vertekend beeld: van 51% in 2009 tot 58% in 2010. Met de toenemende cyberdreiging is die stijging te verklaren door de toenemende achterstand van standaardmaatregelen zoals Antivirus en een groeiende weerstand van organisaties om toe te geven dat hun systemen zijn geïnfecteerd.

Uit het bovenstaande blijkt dat een oppervlakkige analyse een vals gevoel van veiligheid kan oproepen. Daarnaast levert een analyse met ongeschikte modellen vrijwel zeker verkeerde informatie op. Zo gaan berekeningen met de schade-indicatoren SLE en MTTR ervan uit dat je die waarden nauwkeurig kunt bepalen en dat de kansverdeling van deze factoren statistisch normaal is verdeeld. Dat wil zeggen dat de werkelijke waarde dicht bij het gemiddelde ligt en dat sterk afwijkende waarden zeer onwaarschijnlijk zijn. Het gebruik van de normale verdeling is aantrekkelijk, omdat er lineair gerekend kan worden met gemiddelde waarden. En met een interval van 2x de standaardafwijking rond het gemiddelde, zal 95% van de waarden in de praktijk in dat interval vallen.

Maar in de praktijk komen er naast de normale verdeling ook vaak andere kansverdelingen voor. De schaal van Richter voor aardbevingen en de verdelingen van inkomen en vermogen conform de 20-80 wet van Pareto zijn voorbeelden van kansverdelingen met een machtswet. Als de connectiviteit van knooppunten in een netwerk een machtswet volgt, dan bestaat er geen drempelwaarde voor infecties [13]. Dat betekent dat in dergelijke netwerken de verspreiding van infecties enorm wordt versterkt. Verschijnselen zoals hyperinflatie, vertragingen van projecten en verkeer, en verliezen op de beurs hebben mogelijk andere kansverdelingen, maar gedragen zich eveneens sterk niet-lineair [14,15]. Correlatie aantonen en onzekerheid verminderen zijn veel moeilijker met dergelijke kansverdelingen. De schade per beveiligingsincident kan voor een organisatie bijvoorbeeld

fluctueren tussen nul en een faillissement, zoals bij Diginotar. De kans op een faillissement door incidenten met een machtswet als kansverdeling is veel groter dan bij een normale verdeling. Dergelijke risico's zijn meestal niet betrouwbaar te schatten, omdat de schade van het risico ofwel geen gemiddelde waarde heeft, ofwel geen maximale waarde – en soms allebei [16].

Niet-lineaire effecten verschijnen ook regelmatig in de economie. In de periode 2004 tot 2008 verdrievoudigde de prijs van rijst, terwijl wereldwijd de toename van de vraag met 1% precies even groot was als de groei van de productie [17]. Niemand had die prijstoename voorspeld en zelfs met de kennis achteraf is onduidelijk of die überhaupt te voorspellen was.

"To know what you know and what you do not know, that is true knowledge" – Confucius

De individuele competenties van de betrokken medewerkers hebben grote invloed op de effectiviteit van informatiebeveiliging. Maar mensen gedragen zich soms anders dan verwacht en minder rationeel dan ze zelf denken [18]. Onze hersenen zijn evolutionair afgestemd op patroonherkenning, maar individueel missen we grotendeels het zicht op aanvallen die via het internet lopen. Bovendien heeft de betrouwbaarheid van de beschikbare informatie soms ernstig te lijden als de belangen groot zijn. Dat tweedracht zaaien effectief is, blijkt onder andere uit het langdurige gebrek aan consensus over het verband tussen roken en longkanker [19]. Door de schijn te wekken dat het "Intelligent Design" scheppingsverhaal een wetenschappelijk basis heeft, wist de Protestantse lobby in 2004 af te dwingen dat Amerikaanse schoolboeken moesten vermelden dat de evolutietheorie slechts één van de theorieën is [20]. Evolutiebiologen zoals Richard Dawkins die daartegen ageren worden soms persoonlijk aangevallen. Niet alle wetenschappers zullen daarom zin hebben om zich in zo'n discussie te mengen, waardoor pseudowetenschap langer blijft bestaan.

Omdat de mens kuddegedrag vertoont, blijft een dominante mening vaak (te) lang hangen. Kuddegedrag heeft zich evolutionair bewezen als methode waarbij de meerderheid kan overleven als de roofdieren aan een paar zwakke prooidieren voldoende hebben. Als het aantal roofdieren toeneemt, dan komen ook de sterkere leden van de kudde in gevaar. Daarom is een risicoschatting gebaseerd op de stelregel "als ik hetzelfde doe als de meerderheid, ben ik relatief veilig" in het internettijdperk achterhaald. Op het internet zijn we namelijk geen kudde die samenwerkt om aanvallers effectief te confronteren. Het breed delen van kennis compenseert dit gemis niet helemaal, omdat het ontwikkelen van kennis over cyberaanvallen en de (in)effectiviteit van beveiligingsmaatregelen wordt geremd door de eerder genoemde weerstand van organisaties om incidenten te melden.

Door miniaturisatie en de integratie van sensoren, dataopslag, processorcapaciteit en communicatie neemt het aantal slimme online apparaten steeds meer toe. Het gedrag van dergelijke Complexe Adaptieve Systemen (zoals The Internet of Things) is slecht te voorspellen, omdat oorzaak- en gevolgrelaties vaak onduidelijk zijn. Dat komt omdat het gezamenlijke gedrag van individuele systemen afhangt van hun (lokale) logica en de steeds geactualiseerde informatie die via het netwerk wordt uitgewisseld.

In de nabije toekomst zal de samenleving steeds afhankelijker worden van in aantal en omvang groeiende netwerken. In het verleden is gebleken dat met netwerkstructuren communicatie mogelijk blijft, zelfs al vallen veel verbindingen en knooppunten uit. Netwerkprotocollen zoals TCP/IP zijn daarvoor ontworpen. Die robuustheid vervalt echter als het netwerk zelf de oorzaken van uitval doorgeeft aan kwetsbare andere onderdelen, zoals bij malware of overbelasting het geval is. Naarmate zo'n netwerk groeit in omvang en connectiviteit, neemt de kwetsbaarheid voor uitval toe.

Het is nuttig als een model kan aangeven waar een netwerk kwetsbaar is en hoe de robuustheid ervan kan worden vergroot. Omdat technologie steeds complexer wordt, moeten modellen qua complexiteit meegroeien. Veel organisaties maken die stap niet en blijven eenvoudige modellen gebruiken. Maar ook met complexe modellen wordt het betrouwbaar anticiperen op incidenten moeilijker. De consequentie is dat er meer aandacht nodig is voor de voorbereiding van het signaleren en afhandelen van incidenten [21].

"The problem is that at a lot of big companies, process becomes a substitute for thinking. You're encouraged to behave like a little gear in a complex machine" – Elon Musk

Efficiency en kwetsbaarheid bij schaalvergroting

Outsourcing en schaalvergroting zijn meestal gericht op efficiencyverbetering. De basisgedachte is dat kleine organisaties schaalvoordelen missen en daardoor duurder zijn. Vanwege de toenemende bureaucratie worden de grootste organisaties ook duurder ingeschat. Conform deze vuistregel zijn middelgrote organisaties dus het meest efficiënt. Maar uit de twee onderstaande voorbeelden blijkt dat de grens tussen "middelgroot" en "groot" moeilijk te trekken is.

De TU Delft heeft na onderzoek vastgesteld dat het aantal Nederlandse ziekenhuizen zodanig afneemt door fusies, dat een gemiddeld Nederlands ziekenhuis nu al twee keer zo groot is als een gemiddeld ziekenhuis in New York. Bij verder fuseren ervaren Nederlandse ziekenhuizen daardoor schaalnadelen: als de productie met 1% stijgt, dan nemen de kosten met 1,23 % toe. Door schaalvergrotingen in de periode 2003 tot 2009 verloren de

Henk-Jan van der Molen is freelance docent bij de Security Academy.
De auteur wil iedereen bedanken die een positieve inbreng heeft geleverd aan dit artikel, in het bijzonder Jurgen van der Vlugt en Charlotte Rugers.

ziekenhuizen in Nederland bijna 5% aan productiviteit [22].
Hetzelfde resultaat volgt uit een onderzoek van het Centrum voor Onderzoek van de Economie van de Lagere Overheden naar de fusies van Nederlandse gemeenten [23]. Het onderzoek laat zien dat de kwaliteit van publieke voorzieningen na een gemeentelijke fusie niet verbetert. Ook is er geen efficiencywinst, in de nieuwe fusiegemeente blijven de bedrijfsvoeringkosten per hoofd van de bevolking gemiddeld even hoog.
Bij fusies van organisaties blijkt regelmatig dat het resultaat complexer is dan de som der delen, omdat bij schaalvergroting problemen abstracter worden [24]. Managers blijken minder effectief als de afstand tot de werkvloer te groot wordt [25].

Bij technische vooruitgang hoort dat er meer en complexere systemen worden ingezet. Als een systeem meer complexiteit bevat dan direct zichtbaar is, wordt de kwetsbaarheid van het totale systeem meestal te laag ingeschat. Voor het verhelpen van kwetsbaarheden is de standaardactie het uitrollen van een software-update. Vanwege de vele kwetsbaarheden die overblijven, geeft een snelle updateprocedure weinig garantie voor de toekomst. Naarmate een systeem meer componenten bevat, neemt het aantal defecte componenten en de instabiliteit toe [26]. Daardoor is een complex systeem makkelijker te hacken, omdat een aanvaller uit de vele kwetsbaarheden de eenvoudigste kan kiezen. In een technocratische samenleving waarin de capaciteit van elk systeem is geoptimaliseerd, zijn de gevolgen van uitval onvoorstelbaar groot en het moment waarop de uitval plaatsvindt grotendeels onvoorspelbaar.

"If something is fragile, anything you do to increase performance is inconsequential" – Nicolas Taleb

Zelfs met alleen maar veilige componenten kan een systeem als geheel nog steeds instabiel zijn. In de 19e eeuw is bij stoommachines al aangetoond dat maatregelen om de snelheid constant te houden soms grote oscillaties kunnen veroorzaken [27]. Uit een analyse van de black-out in de VS in 2001 bleek dat het elektriciteitsnetwerk afhankelijk is van een aantal kritieke componenten. Uit later onderzoek blijkt dat naast de geografie ook de fysische eigenschappen van het netwerk belangrijk zijn, zoals componenten die de meeste energie doorgeven in het netwerk [28]. Als die falen, leidt dat tot een onvoorspelbare en abrupte uitval van het hele netwerk [29]. Ook het Europese elektriciteitsnet is kwetsbaar, omdat de nationale netwerken zijn gekoppeld met synchrone wisselstroomkoppelingen die capaciteitsproblemen kunnen doorgeven. Op 28 september 2003 viel bijvoorbeeld in heel Italië de stroom uit, omdat een Zwitserse boom een hoogspanningsleiding uitschakelde. Gelijkstroomkoppelingen kunnen problemen in één netwerk afschermen van de andere netwerken, maar vervanging van alle synchrone wisselstroomkoppelingen is duur.

Als een organisatie te complex wordt, is deze niet meer effectief te managen. Vaak reduceren grote organisaties de complexiteit door processen en systemen te uniformeren. Na elke fusie informatiesystemen uniform maken en houden is echter duur en tijdrovend. Daarnaast is schaalvergroting meestal ongunstig voor de beveiliging, omdat in een grote organisatie de vele systemen de single-points-of-failure van dezelfde infrastructuur delen. In een ICT-monocultuur raakt een cascade uitval van systemen veel gebruikers, maar veel organisaties negeren het toegenomen continuïteitsrisico en staren zich blind op de verwachte efficiencywinst van schaalvergroting. Een eenvoudige analogie: om zoveel mogelijk winst te maken met het kweken van bomen, wil de eigenaar zijn perceel zo dicht mogelijk beplanten. De optimale dichtheid van bomen op het perceel is echter afhankelijk van de frequentie van bosbranden. Als de bomen te dicht op elkaar staan, dan zal met één bosbrand het hele perceel afbranden, zie afbeelding 4. In combinatie met meer online gekoppelde uniforme voorzieningen, meer complexiteit en de noodzaak sneller beslissingen te nemen, vergroot globalisatie het risico van een wereldwijde crisis. Het is verkeerd om je alleen te richten op de schaalvoordelen en tegelijkertijd de grotere kans op uitval te negeren.

Als de bezettingsgraad (p) van een perceel groter is dan 0,592.. dan vormen de ingevulde cellen met elkaar een "giant component" (hier: p=0,6) 12

Inmiddels hebben ook Fortune 500 organisaties ervaren dat ze kwetsbaar zijn voor cybercrime [30]. Om de robuustheid van grotere organisaties op acceptabel niveau te houden, zijn meer maatregelen nodig. Daarbij valt te denken aan de capaciteit om uitval snel te kunnen herstellen, redundantie van onderdelen en back-up systemen, maar belangrijker is alternatieve middelen achter de hand te hebben die geen kwetsbaarheden delen met de primaire productiesystemen. Deze alternatieve middelen vormen de "zekeringen" die belemmeren dat een enkel incident kan uitgroeien tot een grootschalige crisis. Als gekoppelde systemen onderling verschillend zijn, kan malware zich moeilijker verspreiden tussen systemen. Voor kritische voorzieningen kan het risico van malware worden gespreid door diversiteit in software. Om die diversiteit te bevorderen moeten organisaties software kiezen die Open Standaarden gebruiken [31].

Sommige architecturen zijn robuust omdat ze zijn gebaseerd op collectieve verantwoordelijkheid en decentrale sturing, zoals immuunsystemen en sommige sociale systemen [32]. In de biologie is de diversiteit aan soorten de beste verzekering tegen massale uitsterving. Ook innovatie gedijt het best

met diversiteit en flexibiliteit, niet als alles hetzelfde is en blijft. Economische diversiteit is de beste voorspeller van economische groei, beter zelfs dan de grootte van de investering in kennis [33].

Toch bieden outsourcing en schaalvergroting ook kansen. Omdat individuele organisaties cyberaanvallen steeds moeilijker kunnen detecteren, bieden security-diensten vanuit de Cloud voordelen. Als een Cloud oplossing incidenten bij een organisatie in real time kan signaleren, kunnen dezelfde incidenten worden voorkomen bij de andere aangesloten organisaties.

"It is often stated that of all the theories proposed, the silliest is quantum theory. In fact, some say that the only thing that quantum theory has going for it is that it is unquestionably correct" – Michio Kaku

De opkomst van quantum-computing

Op basis van de wet van Moore was het al nodig om voldoende lange encryptiesleutels te gebruiken voor het langdurig vertrouwelijk houden van geheime informatie [34]. Zodra een quantum-computer met voldoende rekenkracht ontwikkeld wordt, ontstaat een trendbreuk die direct grote invloed heeft op de sleutellengte en de methoden van encryptie.

De quantum-computer is voorspeld door de beroemde natuurkundige Richard Feynman en is gebaseerd op de quantum-mechanica, die onder andere stelt dat een elementair deeltje zich in superpositie of meerdere toestanden tegelijk kan bevinden. Ik belicht hier alleen het superpositie beginsel, niet de quantum-verstrengeling van twee elementaire deeltjes. Met twee mogelijke toestanden tegelijk neemt met elk toegevoegd deeltje het aantal toestanden van de deeltjesverzameling met een factor 2 toe. Met zijn briljante inzicht draaide Feynman dit om en speculeerde dat een "quantum-computer" op basis van dit concept een exponentiële rekenkracht zou hebben. In een quantum-computer kan een zogenaamd qubit gelijktijdig 0 en 1 zijn.

Met voldoende qubits kan een quantum-computer sommige rekenproblemen veel efficiënter oplossen dan klassieke computers. Met een inputvariabele in superpositie wordt namelijk de functiewaarde van ALLE mogelijke invoerwaarden in één operatie berekend. Daarmee is bijvoorbeeld de RSA-encryptie te kraken, die gebruikt wordt om encryptiesleutels over het internet uit te wisselen. RSA is gebaseerd op de moeilijkheid om uit een product van 2 grote priemgetallen (P x Q) de factoren P en Q te halen.

Het opstellen van een rekenmethode voor een quantum-computer is overigens niet eenvoudig. Omdat in superpositie elke functiewaarde statistisch evenveel kans heeft "getrokken" te worden, moet de rekenmethode borgen dat de correcte oplossing eruit springt en de foute oplossingen elkaar uitdoven. Bij algoritmes waarbij veelvouden van de kleinste oplossingen ook correct zijn, ontstaat er een piek in het frequentiespectrum van de berekende oplossingen. Het meerdere keren "trekken" van het resultaat van de berekening uit het frequentiespectrum vergroot de kans op een correcte oplossing. Voordat deze überhaupt bestond, heeft de wiskundige Peter Shor al in 1994 een methode gevonden waarmee een quantum-computer efficiënt die P en Q kan berekenen uit hun product [35]. Voor het kraken van encryptie bestaan er naast Grovers algoritme voor het efficiënt doorzoeken van databases enkele varianten op Shor's algoritme voor andere encryptiemethoden [36].

De vooruitgang in de nanotechnologie maakte experimenten met een quantum-computer mogelijk. Het bleek echter bijzonder moeilijk om qubits voldoende lang stabiel te houden om berekeningen mogelijk te maken. In 2011 is met een 4 qubit quantum-computer vastgesteld dat het product 143 bestaat uit de priemgetallen 11 en 13 [37]. De weg vooruit is nog lang, maar in de laatste jaren zijn veel doorbraken gerealiseerd om qubits te stabiliseren. Fysicus Leo Kouwenhoven heeft bijvoorbeeld in 2012 na een experiment met nanodraden sterke aanwijzingen gevonden voor de in 1937 theoretisch voorspelde Majorana deeltjes [38]. Die deeltjes zijn groter en stabieler dan elementaire deeltjes, maar vertonen nog steeds quantum-gedrag. Daardoor lijken Majorana deeltjes veelbelovende bouwstenen voor qubits. Op basis van de technologische vooruitgang worden rond 2030 de eerste quantum-computers verwacht die de huidige asymmetrisch encryptiesleutels kunnen kraken [39]. Dat betekent dat actie nodig is als asymmetrisch vercijferde informatie na 2030 geheim moet blijven!

In het post-quantum-computing-tijdperk zijn een aantal asymmetrische encryptiemethoden niet langer veilig [40]. Met Grovers algoritme halveert een quantum-computer ook de sleutellengte van symmetrische encryptiemethoden. De quantum-computer betekent echter niet het einde van alle systemen die gebaseerd zijn op (a)symmetrische encryptie. Wel zullen cryptosystemen in een soort Y2K-programma moeten overschakelen naar veilige encryptiemethoden waarvoor (nog) geen quantum-rekenmethode bestaat. Die encryptiemethoden vergen echter meer rekenkracht en langere sleutels om dezelfde toepassingen mogelijk te maken [41]. Met voldoende lange sleutels zijn encryptiemethoden zoals AES en SHA voorlopig nog veilig. De quantum-mechanica maakt daarnaast zelf ook een nieuwe encryptiemethode mogelijk. Maar om die methode in te zetten voor Quantum Key Distribution vergt op dit moment een directe optische verbinding tussen Alice en Bob, met alle bijbehorende nadelen. Het alternatief om terug te keren naar handmatige sleuteldistributie is echter nog minder aantrekkelijk. Mogelijk dat de ontwikkeling van quantum-netwerken hiervoor een oplossing kan bieden, samen met quantum-computing in the Cloud.

"If you do not change direction, you may end up where you are heading" – Lao Tzu

Conclusie

In de westerse wereld nemen de loonkosten steeds meer toe ten opzichte van de rest van de wereld. Onder deze druk neigen sommige organisaties ernaar op efficiency te concurreren. Helaas zijn gefuseerde organisaties en grote systemen vaak zo complex dat deze moeilijk veilig kunnen worden ingezet. Bovendien zit er aan efficiencywinst door opschaling een grens. Als een organisatie door fusies boven een bepaalde omvang komt, zal de efficiency afnemen. Bovendien kan je in veranderlijke tijden beter klein en wendbaar zijn.

Om met de rest van de wereld te kunnen blijven concurreren, heeft Nederland continu innovatie nodig. Een organisatie die binnen de snel veranderende context de kansen en bedreigingen van nieuwe technologie wil bepalen, heeft voorspellende modellen nodig. Een model verhoogt de transparantie, waardoor het effect van veranderingen op bedrijfsprocessen beter te voorspellen is. Kennis van techniek en statistiek is nodig om modellen te ontwikkelen die kunnen omgaan met ruis in de invoer en om deze te kunnen toetsen. Zelfs een goed model is niet in alle situaties een "silver bullet" en moet aan de context worden aangepast en regelmatig worden herijkt om missers te voorkomen. Dat komt ook doordat theoretische kennis ontbreekt om betrouwbare modellen te construeren en de interactie tussen individuele systemen en het netwerk te beschrijven. Bovendien moet kennis worden ontwikkeld om met een formele taal de consistentie en volledigheid van een model in de praktijk te verifiëren.

Informatiebeveiliging wordt steeds meer een enabler om nieuwe technologie veilig in te kunnen zetten. Er is echter inzicht in de werking nodig om de kansen en risico's van nieuwe technologie te kunnen bepalen. Bovendien moet de opgedane kennis van de (in)effectiviteit van beveiligings-maatregelen en de voorspellende waarde van modellen worden gedeeld, bijvoorbeeld met een meldplicht voor datalekken. Onvoldoende kennis bij het ontwikkelen en managen van beveiliging resulteert in meer onzekerheid en in meer kosten of grotere risico's.

Beveiliging is geen onderdeel dat aan het einde van een project op de geleverde producten kan worden geschroefd. Om de beveiligingsrisico's van projecten en de inzet van eindproducten te beheersen, moeten beveiligings-experts zo vroeg mogelijk worden betrokken bij de ontwikkeling. Daar waar deze experts onverantwoorde risico's signaleren, moeten processen worden aangepast of losser aan elkaar worden gekoppeld.

Het verminderen van complexiteit van systemen maakt risico's beter beheersbaar. Maar als standaardisatie van systemen binnen één sector te ver doorschiet, vergroot dat het risico op een cascade uitval. Organisaties kunnen bijvoorbeeld wel standaardsoftware kiezen, maar om risico's te spreiden mogen organisaties binnen kritische sectoren niet allemaal dezelfde software gebruiken. Meerdere bewegende doelen zijn namelijk moeilijker te raken dan één doel. Het toepassen van Open Standaarden bevordert diversiteit in gekoppelde systemen, en is daardoor een voorwaarde om single-points-of-failure te voorkomen. Een extra argument is dat innovatie naast flexibiliteit ook diversiteit vergt.

Na een aarzelende start vanuit een theoretisch model, ontwikkelt quantum-computing zich momenteel snel. De impact daarvan op de huidige encryptiemethodes moet worden bewaakt. Deze ontwikkeling illustreert dat de kennis van mensen èn opleidingen voor beveiliging met hun tijd moeten meegaan. Maar naast actuele en relevante kennis heeft de moderne informatiebeveiliger tegelijkertijd een "management interface" nodig – om binnen de organisatie realistische verwachtingen te scheppen en draagvlak te krijgen voor inhoudelijk goede plannen.

Referenties

[10] Zie "ICT Barometer over cybercrime", Jaargang 11, 25 maart 2011 op www.beveiligingswereld.nl

[11] Deze aanname is gebaseerd op "On Software Diversification, Correlated failures and Risk Management", blz 8, P. Chen e.a., 2006. Soms zijn malware besmettingen aan elkaar gerelateerd. Bijvoorbeeld de Citadel malware plaatste het Dorifel virus op computers die al onderdeel waren van het Citadel botnet. Dat geval wordt geteld als één besmetting, omdat Dorifel een manifestatie was van de Citadel malware.

[12] Aangenomen wordt dat het aantal jaarlijkse malware infecties Poisson verdeeld is en de populatie uit twee groepen bestaat. Groep 1 rapporteerde over 2009 (Ï1 = 0) malware infecties. Met de verhouding p(x > 1) / p(x = 1) kan Ï2 van groep 2 worden berekend. Daaruit volgt dat groep 1 uit 51% van de populatie bestaat, groep 2 omvat 49% en heeft (Ï2 = 1,5) infecties per jaar.

[13] "Epidemic outbreaks in complex hetergeneous networks", Y. Moreno e.a., 2002

[14] Zie Duitsland in 1922 (1$ = 1000.000.000.000 Mark) en Zimbabwe met (officieel) 100.000% inflatie in 2008.

[15] "Antifragility, Things that gain from Disorder", chapter 18, N. Taleb

[16] "Power Laws, Pareto distributions and Zipf's law", M.E.J. Newman, 2006

[17] Rapport over "Regional food prices", Juli 2010, Wordbank.org

[18] Zie Daniel Kahnemans Systeem I en II in "Thinking Fast and Slow".

[19] "Merchants of Doubt", N.Oreskes, E. Conway, 2010

[20] Zie de zaak Kitzmiller vs. Dover Area School District

[21] Zie het Computable.nl artikel "Incident Response broodnodig" deel 1 en deel 2, 2006.

[22] "Ziekenhuismiddelen in verband. Een empirisch onderzoek naar productiviteit en doelmatigheid in de Nederlandse ziekenhuizen 2003-2009", Jos Blank e.a., TU Delft, 2011

[23] "Gemeentelijke schaalvergroting levert geen geld op", Maarten Allers, Coelo.nl 2010.

[24] Andere fusies die als mislukt zijn gelabeld: Nuon en Essent (2007), UvA en HvA (2012), de provincies Noord-Holland, Utrecht en Flevoland (2014); zie ook "9 Mergers That Epically Failed"op huffingtonpost.com

[25] "Antifragile: things that gain from disorder", chapter 5, Nicolas Taleb, 2012

[26] "How Complex Systems Fail", R.I. Cook, 2005

[27] "On Governors", Maxwell, Proceedings of the Royal Society, No.100, 1868.

[28] "Vulnerability of Power Grids to Cascading Failures", T. Verma, 2012; "Damage Reduction of Cascade Tripping in High Voltage Power Grids by means of Intentional Islanding", B. Kamphorst, 2013

[29] "The extreme vulnerability of interdependent spatialy embedded networks", Nature Physics ,25 aug 2013

[30] "Massive hack hit 760 companies", http://money.cnn.com, 28 oktober 2011

[31] "Tackling Cybercrime: Divide and Conquer", H.J. van der molen, isaca.org, 2010

[32] "Globally networked risks and how to respond", D. Helbing, 2013.

[33] "The Atlas of Economic Complexity", Harvard, 2013

[34] "Selecting Cryptographic Key Sizes", A.K. Lenstra & E. Verheul, 2001

[35] "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", P.W. Shor, 1996

[36] "The Future of Cryptography Under Quantum Computers" M.A. Barreno, 2002

[37] "Quantum Factorization of 143 on a Dipolar-Coupling NMR system", N. Xu e.a., 2011

[38 "Signatures of Majorana Fermions in Hybrid Superconductor-Semiconductor Nanowire Devices", 2012, L. Kouwenhoven e.a..

[39] "Samen bouwen aan een quantumcomputer, interview met Leo Kouwenhoven", 2014, QuTech.nl

[40] Het gaat hier bijvoorbeeld om RSA, DSA, Diffie-Hellman, El Gamal, ECDSA en ECC.

[41] "Introduction to post-Quantum cryptography", 2008, Daniel J. Bernstein

PROCESS CONTROLLED

The Attributer was recently at a client meeting where the conversation turned to the meaning of the term 'information assurance' and the scope of its application. Doubt was expressed as to whether the term includes the security and assurance of industrial control systems (ICS), supervisory control and data acquisition (SCADA) and industrial programmable logic controllers (PLCs).

There is a historical problem inasmuch that the development of ICS, SCADA and PLCs, and development of conventional business IT, has progressed along completely separate technological lines. Back in the 1960's when business computing was emerging there was no similarity between these two technologies. ICS consisted of electromagnetic transducers and relays to control industrial production systems in factories, oil refineries and the like. Then, as information technology developed, ICS became electronic and embraced microprocessor based systems, then moved to utilise standard platforms (first UNIX, then Windows) and during the 80's and 90's adopted networking and eventually connected to the Internet itself. ICS developers and engineers did not consider security, whereas the mainstream IT industry has been moving along a path of securing business systems against a variety of emerging threats.

As an example, in the late 1990's The Attributer visited a small island where there is one power station. It's a tightly knit community in which everyone knows everyone. We met the Deputy Power Station Manager through some long-time friends from university, and he proudly demonstrated how he could control the power station from his laptop at home. I asked about the security of the system and was met with a blank look on his face. He didn't even understand the question. It was just a friendly casual chat so we did not pursue it, but it was typical of how that type of ICS was being implemented at that time. Even in the mainstream IT industry, the early remote network control systems, using SNMP v1, had no effective security embedded. Later developments of SNMP have fixed this deficiency.

Today there is a growing awareness in the production engineering industry of the need to secure remote control protocols, particularly following the Stuxnet computer worm, discovered in 2010, which targeted Siemens 'Step 7' PLC software, and which reputedly was used to destroy certain Iranian nuclear production facilities. As recently as December 2014 the BBC reported that a blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network [1].

What is not apparent is that these lessons are being learned and implemented in the emergence of IoT (the Internet of Things). There is a growing market for domestic control systems such as HIVE, which can be used to control domestic heating systems remotely from a smart phone, tablet or laptop. What assurance do we have that security has been given sufficient consideration? Stedin announced in January 2015 [2] that they have had a live intervention of their IoT network for managing the Dutch Electricity grid, but no reference has been given as to how this control system is secured. It has recently been published that Samsung smart TVs that have voice activation will capture conversations in the room and transmit them to a central location for language processing. There are many similar developments now being launched, such as Apple's Homekit, Google's Nest Labs solution, and the open standard HyperCat. What assurance do we have that these technologies have been adequately secured against the emerging range of threats that the IoT might imply?

The more we see incidents occur, the more the industry will consider the issue, but as always, security is an emergent property that can only be developed with a view of what potential threats actually exist. SABSA thinking can help by ensuring that threat scenarios are considered during the specification of these new technology applications. The inclusion of the attribute 'process controlled' would at least mean that the threats are analysed alongside the business opportunities being pursued.

The Attributer

Links

[1] BBC News – Hack attack causes 'massive damage' at steel works: http://www.bbc.co.uk/news/technology-30575104

[2] Zelfherstellend net in de Rotterdamse regio: http://www.stedin.net/over-stedin/projecten/zelfherstellend-net

VAN KUNST NAAR KUNDE

Cyber Security 2.0

De economische vooruitgang van veel landen is onlosmakelijk verbonden aan de betrouwbaarheid en het weerstandsvermogen tegen verstoring van hun informatie- en communicatietechnologie (ICT). In andere woorden: manage het cyber-securityrisico. Op papier lijkt dat eenvoudig. Je voert een risicoanalyse uit. Je neemt vervolgens een aantal maatregelen die het ingeschatte risico tot een acceptabel niveau terugbrengen. Helaas is de buitenwereld heel dynamisch. Voordat de maatregelen getroffen zijn, zijn er nieuwe kwetsbaarheden en dreigingen en blijken de risico-inschattingen achterhaald. Ook zijn de getroffen maatregelen vaak niet in staat om Advanced Persistent Threats (APT) tegen te houden.

De internationale NAVO werkgroep "Future Cyber Defence Concepts and Tools" analyseerde in de periode 2012-2013 onder leiding van TNO waar het, populair gezegd, aan schort met de cyber-security, zowel in de militaire als de civiele systemen. Een langetermijnoplossingsrichting kwam naar voren. Dat vormde het thema van discussie tijdens het NAVO-Information-System-Technology-panel-symposium dat op 13 en 14 oktober jongstleden in Tallinn, Estland plaatsvond. De auteur van dit artikel was tevens de voorzitter van dit symposium.

Analyse

Naast de menselijke factor komt een belangrijk deel van de cyber-security-incidenten voort uit het onvermogen van de fabrikanten en leveranciers van apparatuur, programmatuur en de geïntegreerde systemen (vitale infrastructuur, militaire platformen) om nu eens echt te leren van eerdere ICT-beveiligingsincidenten in de afgelopen veertig tot vijftig jaar.
Fundamenteler en onderliggend hieraan is dat we nog steeds accepteren dat de individuele ICT-componenten lekken en programmafouten bevatten. Zo is er bijvoorbeeld nog steeds geen productaansprakelijkheid voor programmatuur. Met dergelijke zwakke ICT-componenten gaan we vervolgens een totaalsysteem bouwen.

Belangrijk deel van security-incidenten komt voort uit onvermogen om te leren

Satéstok

Om de veelal onbekende kwetsbaarheden en onderkende risico's af te dekken voegt een cyber-security-architect een aantal maatregelen toe die het risico moeten verkleinen. Hij of zij kiest daarvoor uit een grote verzameling aan technieken en methoden. Denk aan netwerkbeveiliging (bijv. firewalls), IDS, IPS, dreigingsmodellering, anti-malware/ antivirus, honeypots, kwetsbaarheidsanalyse, pen testing, hardening, cryptografie, PKI, forensische hulpmiddelen, bewustwording van gebruikers, PET, fault tolerant systems, uitwijk en back-up. Veel van de technische maatregelen bevatten echter programmatuur die op haar beurt ook weer zwakheden kent. Het uiteindelijke samenstel van maatregelen is feitelijk een verzameling van lagen met vele gaten die een inherent zwak en onveilig systeem veilig moeten maken. De hoop is dat de gaten niet over elkaar heen vallen, ook niet als er een gat door hackers of cyber-criminelen uitgebuit wordt.

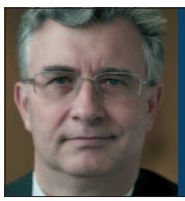
Sommige cyber-security-architecten zijn zeer bedreven in het aaneenrijgen en samenstellen van een evenwichtig pakket ('satéstok') aan maatregelen; andere minder. Soms worden voornamelijk oplossingen gekozen die dichtbij de achtergrond van de architect liggen, bijvoorbeeld cryptografie. Het daardoor geïntroduceerde gat zit dan bijvoorbeeld in het gebrek aan aandacht voor de factor mens die slordig omgaat met de cryptografische sleutels.

Zwakker of sterker?

Een groot probleem is dat cyber security architecten nauwelijks kunnen inschatten of het toevoegen van een maatregel extra veiligheid brengt of deze juist vermindert en wat de meest effectieve en efficiënte mix aan maatregelen is. Een extra detectie- of monitoringsysteem toevoegen kan tijd en aandacht weghalen van de logging van inbraakpogingen waardoor pas later dan wenselijk is gereageerd wordt. Wat dat betreft is cyber-security-architectuur nu eerder een kunst - deels gebaseerd op een onderbuik gevoel dat de juiste maatregelenmix gekozen is - dan op onderzochte principes die aan de basis liggen van (ingenieurs)kunde.

Gebrek aan cyber-security-professionals

Daarnaast constateerde de NAVO werkgroep een steeds groter gat tussen het aantal benodigde cyber security specialisten en de hoeveelheid afgestudeerde cyber security professionals. Op dit moment is er alleen al in de Verenigde Staten en het Verenigd Koninkrijk een tekort van meer dan 20.000 professionals. Maar ook in ons land en andere landen vechten defensie, politie, universiteiten en bedrijven om getalenteerde professionals. De beperkte hoeveelheid opleidingen is daarnaast niet gericht op het opleiden en trainen van cyber-security-architecten en technisch ontwerpers. Cyber-security-architectuur is qua aanpak sterk proces-georiënteerd en minder onderzoekend en analyserend van eerder falen.



Eric Luijf is principal consultant bescherming vitale infrastructuur bij TNO. Eric is bereikbaar via eric.luijf@tno.nl.

De visie: Cyber Security 2.0

Het symposium in Tallinn "Cyber Security and Engineering" bracht een zeventigtal experts bijeen die aan de hand van een introductie, een drietal keynote sprekers en een dertiental presentaties over ingediende papers de door de werkgroep aangedragen visie bediscussieerden. Deze visie bestaat uit een aanpak die op termijn moet leiden tot Cyber Security 2.0 waarbij er sprake is van een integraal researchgebied "Cyber Security Science", een vakgebied "Cyber Security Engineering" en daaraan onderliggend gedegen "Cyber Security Education".

Cyber Security Science

In de discussies over Cyber Security Science kwam naar voren dat in de jaren 70 van de vorige eeuw op deelgebieden van cyber-security fundamentele wetenschap werd bedreven. Op dit moment vindt het meeste wetenschappelijk onderzoek slechts plaats op specifieke deelgebieden ("puntoplossingen"). De aanpak van het hierboven geschetste satéstok-probleem en gebrek aan het leren van geïdentificeerde zwakheden in het verleden vereist betere, wetenschappelijk onderbouwde, methodieken en een integrale aanpak van het gehele cyber-security-domein.

Cyber Security Engineering

Cyber Security Engineering vergt naast nieuwe kennis uit het Cyber Security Science-domein het zetten van een aantal stappen om uit de analyse van eerder falen te achterhalen waar de inherente cyber-security-zwakheden in de cyber-security-architectuur door veroorzaakt worden. Hoe kan het totale ICT- of op ICT-gebaseerde systeem meer weerbaar gemaakt worden tegen cyberverstoringen?
Studenten aan de technische universiteit leren hoe ze een brug moeten ontwerpen, hoe ze rekening moeten houden met materiaaleigenschappen en hoe ze een veiligheidsfactor moeten inbouwen. Op basis van die kunde strijden ze ook in competitie om het bouwen van de beste brug van macaroni. Het resultaat van die kennis en kunde is wel dat vijftig jaar oude bruggen zonder veel aanpassingen dagelijks een veelvoud van de oorspronkelijk bedachte verkeersbelasting verwerken.

Wellicht kunnen we ook leren van de luchtvaartsector waar in dezelfde periode analyses van eerder falen van ontwerpen en menselijke fouten heeft geleid tot lessen die opgepakt zijn door fabrikanten en pilotentrainingen. De veiligheid van de luchtvaartindustrie is daardoor spectaculair verbeterd daar waar ICT dagelijks nieuwe gaten vertoont.

In de discussie tijdens het symposium kwam naar voren dat er nog (te) weinig root-cause-analyse is en dat de kennis over de oorzaken van eerder falen onvoldoende toegevoegd wordt aan de basiskennisbasis van het vakgebied. We patchen of pluggen liever een gat dan dat we vergelijkbare gaten structureel gaan zoeken en daarvoor een structurele oplossing bedenken, ook voor nieuw te ontwikkelen programmatuur.

Cyber Security Education

Wil je op beide bovengenoemde gebieden voortgang boeken, dan is een stevige aanpak van de cyber security opleiding nodig, zowel in de breedte als de diepte. De Nederlandse inbreng op dit onderdeel van het programma was groot. Eén paper en presentatie van prof. Jan van den Berg en collega's ging over de opzet van het curriculum van de Cyber Security Academie en hoe dit past in een lange termijn visie zoals het symposium beoogde. De programmacommissie kende voor deze bijdrage overigens de "Best Paper Award" toe.
Marcel Spruit, lector Cyber Security & Safety bij de Haagse Hogeschool, gaf inzicht in Nederlandse aanpak om te komen tot een internationaal gedragen certificatie voor informatiebeveiligingsprofessionals.

In de discussie kwam naar voren dat Defensie in het Verenigd Koninkrijk inmiddels eisen stelt aan universitaire cyber security opleidingen. Deze moeten een brede basis hebben. Als er sprake is van slechts één of enkele hoogleraren op cyber-securitygebied, dan voldoen de universiteiten niet aan de norm. Inmiddels zijn een aantal vakgroepen verhuist naar andere universiteiten zodat er een grotere bundeling komt van kennis, activiteiten en kruisbestuiving.
Een ander discussiepunt was hoe je tot internationale harmonisatie kan komen van opleidingen en hoe je eerdere kennis en ervaring borgt.

Conclusie

De bedoeling van het symposium was niet om kant-en-klare oplossingen te leveren, wel het bouwen aan een langetermijnvisie. Het symposium heeft dat doel bereikt. Het geeft de deelnemers veel stof tot nadenken gegeven. Landen als de Verenigde Staten en het Verenigd Koninkrijk zetten inmiddels in op het ontwikkelen van Cyber Security Science door het stimuleren van een bundeling van universiteiten. Nederland kent een aantal uitstekende kernen van onderzoek, ontwikkeling en onderwijs. Toch betreft het veel 'puntoplossingen'. Een nationale discussie over hoe gekomen kan worden tot een fundamentele volgende stap op het terrein van cyber-security lijkt wenselijk om de noodzakelijke stap te maken van kunst naar kunde: Cyber Security 2.0.

Dit artikel is eerder verschenen in het blad Beveiliging.

NEAR FIELD COMMUNICATION RUKT OP...

Deuren openen met je mobiel

Veel moderne smartphones zijn voorzien van NFC (Near Field Communication)-technologie. Met NFC kan men informatie overbrengen tussen een telefoon en andere NFC-apparaten, zoals andere telefoons, NFC-betaalsystemen en toegangscontrolesystemen. Maar ook kan men met behulp van NFC bijvoorbeeld webadressen, contacten, telefoonnummers, muziektracks, video's of foto's delen.

Volgens het Amerikaanse onderzoeksbureau ABI Research zal het aantal gebruikte NFC-apparaten in 2014 de 500 miljoen overstijgen. Analistenbureau Gartner denkt dat NFC pas gemeengoed begint te worden in 2016. In dat jaar zou er een markt moeten zijn van 448 miljoen gebruikers die gezamenlijk 617 miljard dollar betalen via NFC. Vele belangrijke mobiele providers in de wereld, verenigd in de koepelorganisatie GSM Association (GSMA), hebben verklaard achter het gebruik van de NFC-technologie te staan. De GSMA verwacht in 2015 110 miljard euro aan betalingen via NFC-chips in mobieltjes.
De verwachtingen van NFC zijn hooggespannen. Mede daarom hebben een aantal vooraanstaande spelers zich in het verleden gebundeld in het NFC Forum. Zo zijn fabrikanten voor NFC-chips nodig, dienen GSM operators hun netwerken aan te passen en is de ondersteuning van hard- en softwarefabrikanten vereist. Kortom: het NFC Forum is een bont gezelschap van ongeveer 170 partijen die als doel hebben het gebruik van NFC-technologie in consumentenelektronica, mobiele apparaten en pc's te bevorderen. Onder andere Philips, Sony, NXP, Nokia maar ook VISA en Mastercard zijn lid. Rond 2004 heeft het NFC Forum de Near Field Communication-technologie ontwikkeld en gestandaardiseerd. De laatste jaren zijn de daar de fabrikanten van toegangscontrolesystemen bijgekomen, hierover later meer. De NFC-chip kent verschillende verschijningsvormen. Zo bestaan er aparte chips die in de toestellen gebouwd worden. Daarnaast is op verzoek van de GSMA de mogelijkheid ontwikkeld om een NFC-chip te integreren in een SIM-kaart. Hierdoor ontstaat een verhoogde security. Doel van de NFC-chip is contactloze tweeweg-communicatie tussen twee apparaten die niet meer dan 10 cm van elkaar verwijderd zijn. NFC maakt gebruik van de ISM-frequentieband op 13,56 MHz en heeft een snelheid van 212 kilobit per seconde. Een NFC-chip kan in drie verschillende standen werken:

- Kaartemulatie-mode waar de NFC-chip zich gedraagt als een contactloze smart-card,
- Reader/Writer-mode waar het NFC-device zich gedraagt als een reader en NFC-tags kan lezen of beschrijven
- Peer-to-peer-mode waarbij het mogelijk is om te communiceren tussen twee NFC-apparaten (bijvoorbeeld uitwisselen van visitekaartjes of andere kleine dataoverdracht).

Zoals beschreven kan een NFC-chip zich gedragen als een contactloze smart-card. Software maakt het mogelijk dat een NFC-chip een MIFARE-kaart kan emuleren. MIFARE is de meest gebruikte contactloze chipkaart ter wereld en een handelsmerk van NXP Semiconductors. De technologie is gebaseerd op de

Ronald Eygendaal. Ronald is werkzaam als senior security consultant bij KPN Trusted Services en is sinds 1990 actief in informatiebeveiliging, elektronische & technisch beveiliging, fraude detectie & bestrijding en bewaking & beveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsprofessionals Nederland (VBN). Ronald is te bereiken via ronald@eygendaals.nl.

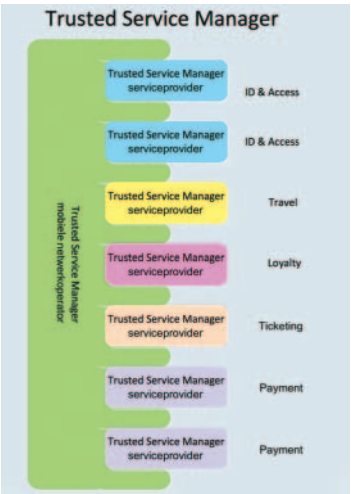
ISO 14443 Type A 13.56 MHz contactlozechipkaartstandaard. MIFARE kent vele dialecten zoals; Ultra, Classic / Standard, Plus, DESFire, ProX, SmartMX, DESFire EV1. De meest gebruikte daarvan zijn Classic, DESFire en DESFire EV1. MIFARE wordt gebruikt in meer dan één miljard chipkaarten en tien miljoen lezers. Zo maken creditcardmaatschappijen zoals VISA en Mastercard gebruik van de MIFARE DESFire EV1 standaard en werkt de OV-chip met de MIFARE Classic. Talloze toegangscontrolesystemen werken op basis van MIFARE Classic. Om MIFARE-kaarttechnologie goed te laten samenwerken met NFC is het definiëren van een standaard noodzakelijk. Vanuit deze optiek heeft de MIFARE4mobile Industry Group, welke bestaat uit zeven toonaangevende spelers in de NFC-arena, besloten de MIFARE4Mobile standaard te ontwikkelen. Een van de doelen van de MIFARE4Mobile-standaard is te komen tot specificaties welke gebruikt kunnen worden voor het beheer van toepassingen die MIFARE-chips gebruiken in mobiele apparaten, zoals smartphones. MIFARE4Mobile biedt toestelfabrikanten en mobiele operators, en daarmee ook applicatiemakers, een enkel technologisch aanspreekpunt (API) om NFC te gebruiken. MIFARE4Mobile ondersteunt drie MIFARE-dialecten te weten Classic, DESFire en DESFire EV1.

De Trusted Service Manager

Zoals eerder aangegeven zijn er voor NFC aanpassing in de GSM-netwerken nodig. Om het NFC-ecosysteem goed te laten werken is mondiaal draagvlak nodig. Zo dienen de GSM-netwerken te worden uitgerust met een zogenaamde Trusted Service Manager (TSM) en dient er roaming te zijn tussen de netwerken. Binnen het eerder genoemde NFC Forum zijn een aantal fabrikanten van TSM's actief. Deze spelen een belangrijke rol want een TSM is een cruciaal onderdeel van het NFC ecosysteem. Een TSM faciliteert als neutrale bemiddelaar tussen diensten leverancier en de netwerk operators (MNO's). De TSM stelt diensten leveranciers in staat om op afstand hun dienst, welke als software op de NFC-chip aanwezig is, te distribueren en te beheren. De TSM vergemakkelijkt distributie en beheer van toepassingen die zich bevinden op een onderdeel in de GSM. De belangrijkste rollen van een TSM zijn:

- Interconnectie tussen netwerkoperators en de dienstenleveranciers
- Faciliteren van end-to-end-security
- Lifecycle-management
- Uitrol van nieuwe gebruikers
- Faciliteren van download Over-The-Air-applicaties
- Personaliseren Over-the-air-applicaties
- Activeren / Deactiveren diensten
- Update User Interface
- Management van de NFC-klantendatabase
- Bijhouden van de counters voor betalingen en logging
- Faciliteren van toegevoegdewaardediensten zoals; ticketing, toegangscontrole, betalen etc..etc.

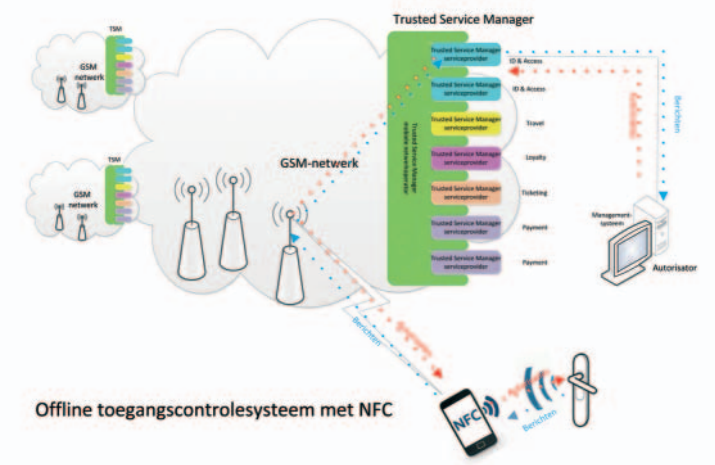
Inwendig is een TSM op te delen in een domein voor de diensten leverancier en domein voor de netwerk operator. Op één TSM kunnen meerdere dienstenleveranciers worden aangesloten. Onderlinge verbinding tussen de TSM 's van verschillende netwerkoperators is van dus groot belang. Sterker nog, hoe meer TSM's met elkaar verbonden zijn hoe beter het NFC-ecosysteem functioneert.



Toegangscontrole systemen

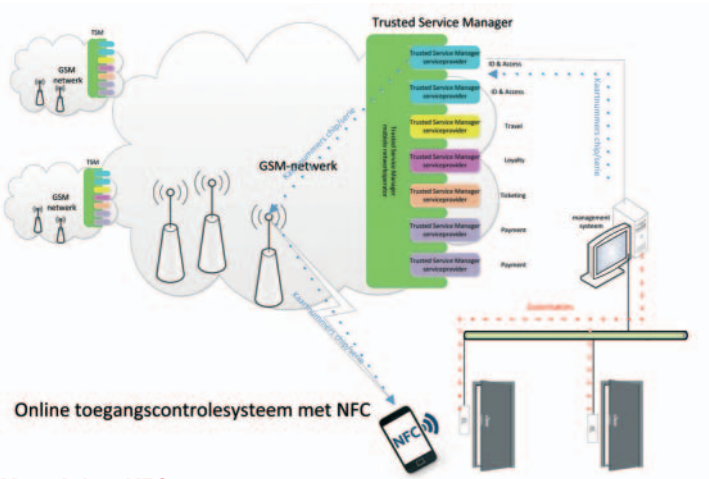
Toegangsbeheer is vereist in vele situaties, kantoorgebouwen, datacenters en parkeergelegenheden zijn slechts enkele voorbeelden. De voornaamste doelstelling van goed toegangsbeheer is het adequaat en klantvriendelijk organiseren van de toegankelijkheid van een terrein, gebouw of ruimte.
Het uitgeven en beheren van toegangspassen is een vaak een rompslomp. NFC kan hier een uitkomst zijn. Een NFC-chip kan via een Over-The-Air (OTA)-verbinding, in de kaartemulatie-mode worden geschakeld waardoor de NFC-chip zich gedraagt als een contactloze smart-card en MIFARE4Mobile zorgt er voor dat MIFARE Classic, DESFire en DESFire EV1 kunnen worden ondersteund.
NFC kan zowel bij online als offline toegangscontrole worden toegepast. Offline systemen zijn zelfstandig functionerende toegangscontrolesystemen waarbij autorisatie wordt bepaald door de offline lezer. Offline lezers hebben een eigen intelligentie en verlenen aan de hand van autorisaties autonoom toegang. In de offline lezer is dan de leeseenheid zelf, een batterij voor de voedingsspanningen en een eenvoudige verwerkingseenheid ingebouwd. Offline lezers en zijn er in verschillende verschijningsvormen. Daarbij moet men denken aan varianten die zijn ingebouwd in het deurbeslag, losse kaartlezers maar modellen die dienst doen als inbouwslot. Bij de offline lezers is er geen noodzaak om aanvullende bekabeling te leggen en vervallen de kosten van bekabeling (230 Volt en datakabel).
Bij veel offline toegangscontrolesysteem worden autorisaties van alle kaarthouders, met behulp van een softwareprogramma, op de toegangspas geschreven. Vaak gebeurt dit via een

zogenaamde update-lezer. Wanneer een toegangspas wordt aangeboden aan een offline lezers wordt de kaart in zijn geheel uitgelezen en worden de autorisaties opgeslagen in het geheugen van de offline lezer. Op deze manier verspreiden de autorisaties zich over alle offline lezers binnen het systeem. Via dit zelfde communicatiepad kunnen offline lezers berichten sturen naar het managementsysteem. (Hierbij moet worden gedacht aan log- en statusmeldingen, maar ook 'battery low'-meldingen.)
Dit neemt niet weg dat bij een offline situatie nog altijd toegangspassen uitgegeven en beheerd moeten worden. Zoals eerder aangegeven kan met behulp van een NCF-geschikte-telefoon en het NFC-ecosysteem de NFC-chip opdracht krijgen zich te gedragen als een toegangspas voor een offline systeem. Op deze wijze kunnen NFC-gebruikers met hun mobiel toegang krijgen.



Online systemen

Naast offline toegangscontrolesysteem zijn er ook online systemen. Deze systemen hebben als kenmerk dat er een er een centrale verwerkingseenheid (managementsysteem) aanwezig is die het mogelijk maakt om alle deuren centraal te beheren met behulp van programmatuur. De sturing voor de ontgrendeling wordt geïnitieerd vanuit het managementsysteem waarna het een en ander lokaal bij een deur wordt verwerkt. Bij dit type systemen worden de kaarten voorzien van codering, vaak het chip-serienummer en/of een fabrikant-gebonden nummers en een soms nog vercijferde sleutels. De nummers en sleutels kunnen met behulp van het managementsysteem op een toegangspas worden geschreven. De autorisaties worden vanaf het managementsysteem doorgegeven aan de intelligentie bij de deur. De intelligentie bij de deur checkt of de aanbieder van de pas gerechtigd is om toegang te verkrijgen en indien gerechtigd wordt toegang verleend. Voor NFC-toepassingen worden de benodigde gegevens via het managementsysteem en een Over-The-Air (OTA) verbinding weggeschreven op een NFC-chip welke voldoet aan MIFARE4Mobile. In dit scenario zal de NFC-chip zich gedragen als een MIFARE kaart met de vereiste codering en sleutels zodat toegang wordt gekregen.



Voordelen NFC

We gaan meer en meer flexwerken. Arbeidscontracten vervagen en werk wordt uitbesteed aan ZZP-er. De vraag naar het op een flexibele en veilig manier verkrijgen van toegang wordt hierdoor steeds actueler. Het gebruik van NFC technologie kan hierin een cruciale rol spelen. Immers via de Over-The-Air (OTA) verbinding kan eenvoudig een virtuele sleutel worden uitgegeven en/of ingetrokken. Met deze virtuele sleutel kan de bezitter van de NFC telefoon zich dan toegang verschaffen tot de gewenste locatie. Het NFC ecosysteem zorgt er voor dat oplossingen provideronafhankelijk werken.
(tk)De marktontwikkelingen
Volgens marktonderzoeksbureau securityinfowatch ontwikkelt de markt voor toegangscontrole op basis van NFC-technologie zich zeer snel. Zo geeft Blake Kozak, senior analyst bij marktonderzoeksbureau IHS Technology, aan dat de adoptie van offline systemen de markt zal domineren. Grote traditionele toegangscontrolespelers zoals HID, KABA, ASSA-ABLOY en SALTO zijn klaar voor NFC. Met name de laatste drie hebben grote stappen gemaakt met NFC-technologie. Zo maakt KABA met haar Legic divisie TSM's, heeft ASSA-ABLOY met haar SEOS standaard de NFC sleutelbeheer verder gestandaardiseerd en heeft SALTO veel NFC-systemen, zonder TSM-koppeling in het veld staan. In 2014 zullen de netwerkoperators TSM's in de netwerken plaatsen en zal de markt in nog hogere versnelling komen.

Links

http://www.securityinfowatch.com/article/11177765/access-control-experts-talk-nfc-hosted-solutions-and-interoperability-at-asis?page=3
http://www.sourcesecurity.com/news/articles/co-5188-ga.12743.html
http://www.hidglobal.com/blog/could-mobile-phone-signal-end-pocketful-keys-and-cards

KEEPASS: EEN EINDE AAN WACHTWOORD-ERGERNISSEN

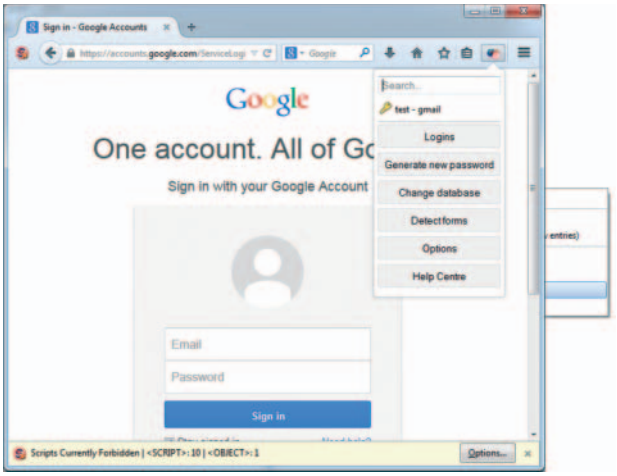
Misschien is het wel één van de grootste ergernissen van IT-gebruikers: wachtwoorden. Niet zelden heb je tientallen verschillende accounts. En met zulke hoeveelheden is onthouden bijna geen optie meer, tenzij je overal (of op vele plekken) hetzelfde wachtwoord gebruikt. En dat daar risico's aan zijn verbonden zien we regelmatig. Als jouw accountgegevens op een slecht beveiligde website worden gestolen moet je niet raar staan te kijken als de hacker ermee op iTunes of Paypal probeert in te loggen. En zijn al die systeembeheerders van websites waar je een account aan moet maken eigenlijk wel te vertrouwen? Het kan geen kwaad om meer variatie in wachtwoorden aan te brengen. Een tool die ons daarmee kan helpen is KeePass.

Sterke wachtwoorden

Op het moment dat je een nieuw account aan KeePass toevoegt, genereert KeePass standaard een willekeurig gekozen krachtig wachtwoord voor dat account. Je kunt dit wachtwoord vervangen door een zelf gekozen wachtwoord, maar waarom zou je? Met KeePass hoef je het wachtwoord niet meer te onthouden en kun je elk account beschermen met het door KeePass voorgestelde wachtwoord van 20 karakters lang. De criteria die KeePass gebruikt om wachtwoorden te genereren zijn in de applicatie aan te passen.

Veilig documenten bewaren

In de KeePass-database kun je naast wachtwoorden ook documenten bewaren. Ga je bijvoorbeeld op reis en wil je overal veilig een kopie van je paspoort bij de hand hebben? Dan is KeePass vele malen veiliger dan een onversleuteld kopietje in je DropBox of Google Drive.



Toegankelijkheid

KeePass is oorspronkelijk ontwikkeld als stand alone applicatie voor Windows PC's. Inmiddels zijn er verschillende plugins ontwikkeld die het mogelijk maken om de KeePass-database vanuit andere applicaties of vanaf andere devices aan te spreken. Zo zijn er ports naar onder andere Android, IOS, Mac OS X en Linux. En zijn er plugins die je helpen om de database aan Chrome, Firefox of Internet Explorer te koppelen.

Portable

KeePass is beschikbaar als portable executable. Hiermee kun je KeePass op elke Windows PC gebruiken, ook als je op de zaak bijvoorbeeld geen beheerrechten op je PC hebt. De wachtwoorddatabase zelf kun je eenvoudig tussen systemen uitwisselen door het op een USB-stick of je mobieltje mee te nemen. Of via een door jou vertrouwde Cloud. In theorie is de database, mits jij het hoofdwachtwoord goed genoeg kiest, zelfs nog veilig als hij in verkeerde handen terecht komt. Maar de vraag is of jij een aanvaller de kans wilt geven om jouw wachtwoord te raden of de 128bits AES encryptie te kraken.

Wat de beveiliging van het product ook ten goede komt is dat KeePass ook zijn deel van het computergeheugen versleutelt. Daarnaast schoont het niet langer gebruikte geheugendelen continu op. Een aanvaller die op je PC weet in te breken en daar een geheugendump maakt, heeft daardoor niet zonder meer toegang tot je wachtwoorden.

Als je je KeePass-database op een centrale netwerkschijf hebt staan hoef je je geen zorgen te maken dat het onversleutelde SMB-protocol (van Windows filesharing) ervoor zorgt dat je wachtwoorden onbeschermd over het netwerk worden getransporteerd. Op het moment dat je de wachtwoorddatabase vanaf je werkstation opent, wordt database in zijn versleutelde vorm over het netwerk getransporteerd om daarna direct in het beschermde geheugen te worden geladen en verwerkt.

Onthouden of opslaan?

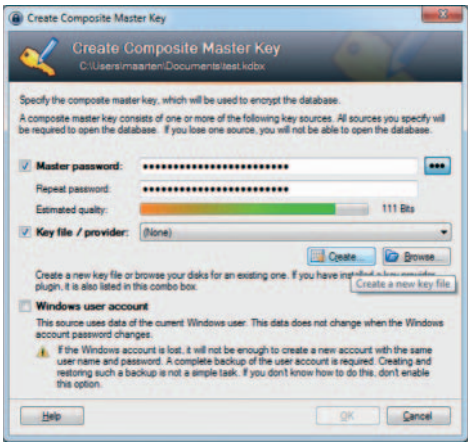
Het bijhouden van wachtwoordlijstjes is iets dat je als informatiebeveiliger liever niemand aanraadt. Maar zijn er werkbare alternatieven? Is het beter om overal hetzelfde wachtwoord te gebruiken? Of om met eenvoudige varianten te werken? Om een Excellijstje bij te houden? Of een lijstje in een kladblok?

In de ruim 10 jaar dat ik nu regelmatig wachtwoordaudits uitvoer is mij één ding duidelijk geworden: het merendeel van ons kiest uit zichzelf geen sterk wachtwoord. Dit geldt voor doorsnee gebruikers, die je van onwetendheid zou kunnen verdenken, maar ook voor beheerders, die exact weten waarom ze eigenlijk een sterk wachtwoord moeten kiezen. Een tool als KeePass, waarbij de wachtwoordgeneratiefunctie wordt benut, biedt dan een enorme stap vooruit.

Persoonlijk heb ik al verschillende wachtwoordaanpakken geprobeerd. Zo ben ik bijvoorbeeld gestopt met het onthouden van wachtwoorden op de vele internetshops. De wachtwoordresetknop is daar veelal ook een prachtig authenticatiemiddel. En heb ik mij gespecialiseerd in ingewikkelde manieren om unieke wachtwoorden te maken die ik toch denk te kunnen onthouden (maar vaak ook weer vergeet). Mocht je daar ook last van hebben: wellicht heb je iets aan KeePass.

KeePass-versleuteling en -authenticatie

KeePass is een gratis en open source wachtwoordmanager. In essentie is het een kleine, eenvoudige, database. Deze database is versleuteld met krachtige encryptie. Binnen de database sla je al je wachtwoorden op, die je vervolgens kunt groeperen en sorteren.



De KeePass-wachtwoorddatabase bescherm je met een master-wachtwoord. In theorie is dit vanaf het moment dat je met KeePass gaat werken nog het enige wachtwoord dat je hoeft te onthouden. Als je een zeer krachtig wachtwoord kiest is je database goed beschermd. Kies je een zwak wachtwoord, dan loop je het risico dat een gestolen database toegang biedt tot je complete collectie aan accountgegevens.

Als je een zelf gekozen wachtwoord onvoldoende vindt voor de bescherming van je wachtwoorddatabase, kun je de database ook met een zgn. keefile beschermen. Door deze keefile separaat van de wachtwoorddatabase te bewaren, verklein je de kans op misbruik van een gestolen wachtwoorddatabase. In de praktijk vraagt het gescheiden bewaren van database en keefile veel van de discipline van de KeePass-gebruiker.

Binnen bedrijfsomgevingen kan de database ook geïntegreerd worden met de Windows-authenticatie. Het wachtwoord wordt dan afgeleid van details van het computer- of domeinaccount van de gebruiker. Deze optie biedt gebruikers veel gemak, maar kent ook twee belangrijke nadelen. Ten eerste is het wachtwoordbestand ontoegankelijk op het moment dat het Windows account corrupt raakt of verwijderd wordt. Omdat het database wachtwoord onder andere wordt opgebouwd uit het SID van het account, kun je niet zomaar een nieuw account met dezelfde gebruikersnaam aanmaken. Daarnaast zouden systeembeheerders hun rechten kunnen gebruiken om de wachtwoordbestanden te unlocken. Dit geldt ook voor hackers die op het domein hebben weten in te breken.

Brute-force-aanvallen

Zelfs als er een zwak wachtwoord is gekozen om de KeePass-database te beschermen, zijn er basismaatregelen aanwezig die het brute-forcen van dat wachtwoord moeilijker maken. Een wachtwoord wordt nadat het in een wachtwoordhash is omgezet nog verschillende malen versleuteld. Standaard is dit 6000 keer. Omdat het tijd kost om het wachtwoord 6000 keer te versleutelen heeft een aanvaller ook meer tijd nodig om het wachtwoord van een gestolen wachtwoorddatabase met brute kracht te kraken. Je kunt als gebruiker zelf kiezen hoe vaak deze versleuteling plaats moet vinden. KeePass kan je helpen om op jouw PC uit te rekenen hoeveel iteraties er nodig zijn om een inlogvertraging te realiseren van 1 seconde. Maar als je op een hele snelle desktop PC een vertraging van 1 seconde inbouwt, kan het betekenen dat je op je mobieltje erg lang moet wachten voor je succesvol ingelogd bent.

Shoulder Surfing

Eén van de standaard risico's van het bijhouden van wachtwoordlijstjes is dat iemand anders het wachtwoord op je scherm mee kan lezen. KeePass toont opgeslagen wachtwoorden daarom niet op het scherm. Met je rechtermuisknop kopieer je het wachtwoord eenvoudig naar het Windows kladblok. En vanaf daar plak je het in het wachtwoordveld van de applicatie. Na (standaard) 10 seconden maakt KeePass het kladblok weer leeg. Het aantal seconden kan desgewenst aangepast worden.

Onbewaakte PC

Je bepaalt zelf hoe lang KeePass na het ingeven van het wachtwoord geopend blijft. Dit kan oneindig zijn, of elk gewenst aantal seconden. Door KeePass de database na gebruik automatisch te laten blokkeren voorkom je dat er op een onbewaakt achtergelaten PC ongeautoriseerde toegang tot de wachtwoorddatabase kan worden verkregen.

Maarten Hartsuijker is beveiligingsconsultant en ethisch hacker bij Classity en bereikbaar via pvib@classity.nl.


Lex Borger


André Koot


Maarten Hartsuijker

we hebben hier goede vooruitgang geboekt. Standaarden worden zorgvuldig gekozen en protocollen kunnen goed aangeven welke cryptoalgoritmen ze wel en niet ondersteunen. Het is nog wat wennen voor systeembeheerders dat je werkende functionaliteit blokkeert, maar het is in ieder geval future proof. Een probleempunt, maar erkend en aan de beterende hand.
En dan last, but not least: Vertrouwen in de certificaat-keten. Dit deel is nog niet echt aan de orde geweest. Maar het is potentieel de zwakste schakel. Dat het OS en de browser honderden certificaten standaard vertrouwen is vreemd te noemen. Certificaat-pinning helpt een beetje, maar is meer symptoombestrijding. De lijst van vertrouwde certificaten zou meer naar een whitelist-situatie toe moeten: de gebruiker/beheerder bepaalt expliciet welke certificaten vertrouwd worden. En dit mechanisme bestaat: Web of trust. Ik ben klaar voor de omschakeling.

Maarten Hartsuijker

Met de techniek achter PKI is, tot het tegendeel bewezen is, naar mijn idee niets mis. We hebben op dit moment geen betere aanpak voor het borgen van goede versleuteling en berichtsintegriteit. Maar PKI draait wel om vertrouwen. Om vertrouwen in de uitgevers en ondertekenaars van certificaten en de mate waarin zij er in slagen om hun centrale sleutelmateriaal te beschermen en er integer mee om te gaan. Als eindgebruikers vertrouwen wij veelal blind op de keuzes die leveranciers voor ons maken. Microsoft bepaalt welke CA's mijn browser groen mogen kleuren. En KPN, Vodafone en TMobile bepalen het sleutelmateriaal waarmee mijn mobiele verkeer wordt beschermd. Zolang zo centraal bepaald blijft in wie wij vertrouwen hebben, is het niet vreemd dat deze zwakke centrale schakels een aantrekkelijk doelwit zijn.

Bij een klant krijg ik regelmatig de vraag voorgeschoteld: mogen we hier een certificaat uit de eigen CA voor gebruiken, of moeten we hier een certificaat voor kopen? Op zich een goede vraag, indien deze gesteld zou worden vanuit een trust-perspectief. Ik merk echter dat bij velen nog het gevoel leeft dat gekochte certificaten een hogere beveiligingswaarde vertegenwoordigen. Het concept achter PKI wordt vaak slecht begrepen.

Dus back to basics: bij een belangrijke verbinding hoort niet per definitie een duurder certificaat. Meer zelfregie op het genereren, signeren en valideren van certificaten kan ook veel bijdragen.

André Koot

Zeker kunnen we PKI nog vertrouwen. Een Public Key Infrastructure is immers niet meer dan het platform waar we vertrouwen aan willen ontlenen. Zolang PKI-sleutels niet kunnen worden gekraakt, is er niets aan de hand met het platform als zodanig en het lijkt erop dat we nog steeds wel even door kunnen. Probleem is dat PKI natuurlijk voor verschillende doeleinden kan worden gebruikt. Daar lopen we nu tegenaan. Zoals ik al eerder constateerde (IB 4:2012), is het gebruik van een certificaat als digitale handtekening iets anders dan een certificaat dat wordt gebruikt om een website te identificeren.

Wat we niet meer kunnen vertrouwen, zijn de verschillende 'te vertrouwen' partijen. En dat hebben we eigenlijk pas sinds Diginotar in de gaten. Toen pas ontdekten we dat de certificaatuitgevende partijen, de CA's, een factor zijn om rekening mee te houden. En pas toen bleek dat wij, de gemeenschap, de maatschappij, daar nooit rekening mee hebben gehouden. Toen bleek dat er zo'n 600 CA's voor ons als betrouwbaar werden aangemerkt, namelijk de CA's die de leveranciers van browsers voor ons al in hun browser installeerden, zonder dat daar een passende analyse van had plaatsgevonden.
En toen bleek ook pas dat we niet weten hoe we om moeten gaan met het beheer van sleutels. Want ja, dat hoefden we niet zelf te doen, want die sleutels waren te vertrouwen. Niets bleek minder waar. De 'root'-CA's, zoals Diginotar en Comodo, hadden hun eigen sleutelbeheer niet op orde. Maar wij wisten dat niet. Sterker, de browserleveranciers waar wij blind op vertrouwden wisten dat niet.

Sleutelbeheer had altijd al een extra kwetsbaarheid: de gebruiker. Je kunt zelf sleutels beheren. Je kunt zelf sleutels toevoegen. En daar mag je dan zelf voor kiezen. Ik heb zelf een aantal certificaten van websites aan mijn browser toegevoegd, omdat ik die certificaten en die websites expliciet wil vertrouwen.

Dit nieuwe incident toont ons een nieuwe kwetsbaarheid. Niet alleen kunnen we de leveranciers van browsers niet meer vertrouwen, ook anderen kunnen zomaar besluiten om certificaten te installeren van partijen die we daarmee automatisch vertrouwen. Dat hadden wij niet zo bedacht.

We kunnen dit incident dan ook niet zomaar als een incidentje beschouwen; het is eigenlijk een oproep aan het CA-/browser-forum om opnieuw alle root-CA's tegen het licht te houden om te beoordelen of ze echt wel passen binnen de PKI zoals we die willen gebruiken.

Ik vrees alleen dat dat niet gaat gebeuren. Het is namelijk een heel kostbare zaak en ik vraag me af of er iemand is die deze kar wil trekken.

Achter Het Nieuws

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

SUPERFISH

Het gebruik van certificaten voor identificatie van websites en het versleutelen van de verbinding met de bezoeker van die site is één van de belangrijkste beveiligingsmechanismen die we kennen. Het garandeert de identiteit van de website-eigenaar en zorgt er voor dat de communicatie niet afgeluisterd kan worden. Maar we hebben de afgelopen jaren een paar akkefietjes gehad. Diginotar, Comodo, Turktrust en een DRM-gevalletje bij Sony. En nu hebben we dan #Superfish. Een adware-programmaatje, dat bij nadere beschouwing een root-certificaat van het bedrijf Komodia in de browser importeert, waardoor die adware in staat is om ook in te breken in beveiligde verbindingen om een 'optimale gebruikerservaring' te bieden. Tja. Optimaal voor wie? In ieder geval loopt Lenovo, die Superfish installeerde op miljoenen laptops, flinke imagoschade op, maar het blijkt dat ook andere partijen diezelfde Komodia-certificaten gebruiken. Kunnen we PKI nog wel vertrouwen?

Lex Borger

PKI omvat een aantal elementen. De vier belangrijkste: de cryptografie, de implementatie daarvan, de protocollen en de keten van vertrouwen van het certificaat. De crypo kunnen we volgens Bruce Schneier vertrouwen en ik ben het helemaal met hem eens.

De implementatie daarvan omvat het correct coderen van de crypto in libraries, het correct gebruiken van die cryptofuncties en het geheimhouden van de privésleutel. Dit blijft een kwestie van kwaliteit van softwareontwikkeling. Veel kwetsbaarheden komen hier uit voort, maar ze zijn te patchen - ook al zijn het soms ingrijpende patches, zoals Heartbleed en Shellshock. Hier hebben we allemaal mee te maken, maar ik durf te stellen dat dit meer zegt over de kwaliteit van software algemeen. PKI is hier niet de boosdoener.

De crypto/PKI-protocollen hebben wat problemen gehad, maar

www.helpendehackers.nl
ISBN 978-90-823462-0-6

HELPENDE HACKERS

In deze uitgave geen "verantwoorde onthullingen". Dat is niet omdat er geen onthullingen meer zijn, maar omdat Chris van 't Hof druk bezig geweest met het omzetten van de columns naar een boek, wat in april wordt gelanceerd.

In dit boek komen hackers, gehackten, ICT-ers, journalisten, managers, politici en juristen aan het woord die betrokken zijn geweest bij een ethische hack. Ze schetsen een digitaal polderlandschap waarin iedereen een beetje, maar uiteindelijk niemand volledig verantwoordelijk is voor de informatiebeveiliging. De persoonlijke verhalen geven een kijkje in de mysterieuze wereld van cyber security en laten zien hoe hackers ons kunnen helpen.

Kortom, het is een verlenging van de columns en daarmee wordt het een beschrijving hoe de beweging rondom responsible disclosure in Nederland ontstaan en gegroeid is.

We zijn nog met Chris bezig om een speciale aanbieding voor PvIB-leden te regelen...

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
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

REDACTIERAAD
Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Maarten Hartsuijker (Classity)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)

ADVERTENTIE ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
(Motivation Office Support)
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 2015
De abonnementsprijs in 2015 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

WINKELEN, ZOLANG HET NOG KAN

Toen ik op school zat (en dat is al een tijdje geleden) leerden wij dat de industriële revolutie het begin was van ons huidige tijdperk van economische groei. Voor de statistici onder ons: het begon in 1750. Ik geloof dat helemaal. De somberen onder ons geloven dat we nu aan het einde van dit tijdperk staan.
De industriële revolutie was het begin van mechanisering. De mechanisering ging door en door en werd op een gegeven moment gecombineerd met computertechniek en dat gaat het begin van het einde worden. De verdiensten werden al fors verhoogd door mechanisering maar in combinatie met IT zouden die verdiensten fenomenaal worden, heerlijk gewoon. Het klopte, de economische groei begon inmiddels perverse vormen aan te nemen, getuige een select aantal mannen (en een nog selecter aantal vrouwen) die miljoenen op hun eigen rekening zien terecht zien komen terwijl ze hun bedrijf kost wat kost fors vooruit helpen en de aandeelhouders gelukkig maken. Breng vervolgens de verwerkingskosten naar beneden en de winsten worden nog kolossaler.
De voorbeelden van de leegstaande marmeren bankfilialen en verzekeringskantoren heb ik hier al eens besproken.
Winkelstraten staan ook grotendeels leeg. Soms heb je een paar winkels, die wel allemaal bij een grote keten horen. Onbekend is wie eigenaar is van welke keten en vaak zijn er meerdere ketens in eigendom van één eigenaar. Maar ook daar zijn nu enorme klappen aan het vallen. Zo klaagt de Hollandse Eenheidsprijzen Maatschappij Amsterdam (HEMA) al jaren. V&D zal tegen de tijd dat dit gepubliceerd wordt waarschijnlijk failliet zijn. De Schoenenreus is al omgevallen en ga zo maar even door. Allemaal omdat ze geen klanten meer hebben? Nee dat is het niet, kijk maar eens op een mooie zaterdag bij de bovengenoemde winkels (zolang het nog kan); de winkels zijn helemaal vol. Er wordt alleen niet meer genoeg verkocht.
Ik denk dat ik wel weet wat er echt aan de hand is. Winkeliers richten alles op internet. Als je hierin wilt investeren doe het dan wel op tijd en doe het op een andere manier dan Neckermann, want dat liep ook via internet niet goed af. HEMA investeert inmiddels ook in internetactiviteiten. Hopelijk gaat hen dat beter af. Ik ben er van overtuigd dat je goedkoper een paar onderbroeken via internet kan verkopen dan vanuit een winkel. Denk aan de besparing in kosten aan personeel, gebouw, inboedel en dergelijke.

Ik zal het nog gekker maken: de supermarktoorlogen zullen niet meer via de hamsterweken en kiloknallers worden uitgevochten maar via het internet. Al jaren probeert de supermarktbranche er achter te komen wie die meneer is die weer een volle winkelwagen afrekent en altijd zijn bonuskaart is vergeten. Berry weet het wel: eigenlijk heeft hij er geen maar wil hij wel graag de korting. De supermarkten willen graag weten wie er door hun winkels lopen en waarom ze dát product kiezen in plaats van het vergelijkbare product waar de winkel meer marge op heeft. Daar hebben ze een geweldige oplossing voor gevonden: iedere week komt de klant naar jouw elektronische winkel. De boodschappen worden zorgvuldig uitgekozen, maar je kunt er eens een aanbieding tussendoor doen. Na een paar weken weet je dat de heer des huizes wel een lekker biertje lust en dat er ook nog een chocoladeliefhebber rondloopt. Handig. De bezorgservice komt er achter dat het bezorgen van boodschappen een enorme spurt neemt, vertelde men mij. Meneer de supermarkteigenaar gaat weer eens achter zijn calculator zitten en begint te dagdromen. Stel nu dat ik een aantal van mijn winkels sluit, ik koop op het platteland een loods, prop er een serie robots in, huur een paar bezorgers in, lease een paar bestelwagens en gaan met die banaan. Geen winkelhuur meer, veel minder personeel, efficiëntere afhandeling, minder en gerichtere voorraad. Zie hier het einde van de winkel.
Als mijn kinderen (misschien kleinkinderen) net zoveel grijze haren hebben als Berry zal ik ze nog eens laten zien hoe wij vroeger zelf de winkelwagentjes volgooiden en dat perverse gelddrang daar een einde aan gemaakt heeft.

Berry

Secure Link
Infrastructure Security Solutions



Gezocht!
Security Engineers

SecureLink groeit en is op zoek naar Security Engineers die ons team komen versterken!

Als Security Engineer heb je diepgaande kennis op het gebied van security en networking. De combinatie van enerzijds de security technologie en anderzijds de integratie met networking is iets waar jij al jouw energie en expertise in kwijt kunt. Je krijgt de ruimte zelfstandig complexe security en networking projecten van A tot Z uit te voeren.

Benieuwd? Kijk dan op www.securelink.nl/vacatures



Kom jij ons team versterken?

Sinds de oprichting van SecureLink in 2003 managen en realiseren wij als security en networking integrator met ruim honderdtachtig SecureLinkers, verdeeld over drie vestigingen in Nederland en België, enterprise security architecturen én een hoger security niveau.

Go Secure!

SecureLink Nederland B.V. | Trapezium 224 | 3364 DL Sliedrecht | T +31 88 1234 200 | info@securelink.nl