iB
INFORMATIEBEVEILIGING
jaargang 14 - 2014
#8

DREIGINGEN & KWETSBAARHEDEN

NCSC Interview

Vulnerability scanning in de praktijk

De volgende fase van SIEM

SSL Configuraties

Forensic Intelligence Network of Excellence (FINE)

Secure Link
Infrastructure Security Solutions



Gezocht!
Security Engineer

SecureLink is sterk groeiende en is daardoor 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 veel ruimte om zelfstandig complexe security oplossingen te pre-stagen, implementeren en onderhouden.

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



Integrated Networking Security Solutions

SecureLink is een vooraanstaande Benelux georiënteerde security en networking integrator. SecureLink onderscheidt zich door haar geïntegreerde security en networking specialisatie, voorname vendor statussen, managed services en hoge klanttevredenheid.

Go Secure!

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

INEFFICIËNTE INFORMATIE-OVERLOAD

Het nadeel van level in de digitale tijd is dat in bewerkingsprocessen veel meer informatie verwerkt wordt dan daarvoor. Nu is veel van die informatie ongetwijfeld nodig of nuttig, maar ik kan me niet onttrekken aan de indruk dat er soms meer gevraagd wordt, veel meer. Of dat er informatie gevraagd wordt die al bekend was of afgeleid kon worden. Kleine ergernissen zijn de eis om twee keer mijn wachtwoord in te vullen in een webformulier. Het tweede veld is dan zelfs 'beveiligd' tegen het inplakken van mijn e-mailadres. Bij een wachtwoord snap ik het, maar een e-mailadres? Erger is het bij online selfservice systemen. De hoeveelheid vragen die je iedere keer te beantwoorden krijgt bij een incidentmelding of de aanmelding van een change is overweldigend. En op lang niet alle vragen weet ik wat het goede antwoord is, dus kies je wat werkt. Er ontstaat een informatievermoeidheid. Je zet je niet langer in om de juiste gegevens in te vullen, je zorgt dat je er zo snel mogelijk vanaf komt. Voor degene die die informatie wil gebruiken is dit niet goed. De rapportages en analyses voor procesoptimalisatie zijn niet langer betrouwbaar. Zonde van al die extra ingevoerde informatie. Toch kan het anders: Als ik bij 123inkt.nl weer inktpatronen bestel, weten ze na mijn inloggen meteen wat ik in het verleden heb besteld en hoe ik dat afgehandeld wil hebben. Als daar niets in wijzigt, dan ben ik in drie klikken klaar.

Zo kan het dus ook! Als beveiligers hebben we hier ook een handje van. Als we gebruikers vragen om documenten te classificeren, dan is dat vaak een hele last voor de gebruiker. Bepalen wat de classificatie is, wanneer deze herijkt moet worden, en hoe de markeringen in het document én de metadata aangebracht moet worden. Er zou toch makkelijk bepaald kunnen worden wat naar alle waarschijnlijkheid de documentklasse is en de gewenste herijkingsperiode. En hoe voor dit type de markering aangebracht wordt. Toch ben ik zo'n slim documentclassificatieinstrument nog niet tegengekomen...
In identity management systems (IdM) zie ik in de opzet ook veel (historische) inefficiënties - denk aan naamconventies van administrator accounts en de vele uitzonderingen daarop. Waardoor het beheer meer werk is, omdat elke uitzondering specifiek en apart ingebracht moet worden. Dit stelt ook extra eisen aan de functionaliteit en flexibiliteit van die IdM-systemen. En het heeft verwerkingsfouten tot gevolg.
Mijn professionele nieuwjaarswens: Zorg voor zinvolle registraties, vraag niet te veel van de gebruiker, bereken waarden automatisch waar mogelijk en houdt vast aan standaarden. De gebruiker zal je danken en je datakwaliteit wordt beter. Wat wil je nog meer?

Lex Borger, hoofdredacteur

In dit nummer

NCSC: ‘HONDERD PROCENT VEILIGHEID BESTAAT NIET’

Jaarlijks brengt het Nationaal Cyber Security Centrum een lijvig trendrapport uit: het Cybersecuritybeeld Nederland. Het geeft een beeld van ‘cyber’ in Nederland over het afgelopen jaar en komt voort uit een samenwerking met maar liefst 80 partijen. Het is bijzonder dat de overheid komt met zo’n specialistisch document. Hoe komt het CSBN tot stand? Een interview met hoofdredacteur Rogier van Wanroij, eindredacteur Koen Sandbrink en auteur Kas Clark.

Chantal Craandijk is bedrijfsjournalist. Chantal is bereikbaar via contact@craandijk.com


Rogier van Wanroij


Koen Sandbrink


Kas Clark

De eerste Nationale Cyber Security Strategie (juni 2011) benadrukte het groeiende belang van cybersecurity en de behoefte aan een Nationaal Cyber Security Centrum (NCSC) waarin kennis en expertise uit publieke en private partijen bij elkaar wordt gebracht. Volgens de strategie is het NCSC ook verantwoordelijk voor het creëren van één gezamenlijk en integraal beeld van de actuele dreigingen van ICT, het zogenaamde Cybersecuritybeeld Nederland (CSBN). Deze rapportage komt tot stand in samenwerking met publieke en private partners. De inzichten uit het CSBN bieden houvast om waar nodig de digitale weerbaarheid van Nederland te versterken of lopende cybersecurity-programma's aan te scherpen. Het CSBN gaat jaarlijks naar de Tweede Kamer. De afgelopen editie, de vierde, bestrijkt de maanden april 2013 tot en met maart 2014.
De gegevensverzameling voor het CSBN blijkt nog niet zo lastig, vertelt hoofdredacteur Rogier van Wanroij: "Het NCSC analyseert maandelijks cybersecuritytrends dus we zitten al op die informatie." Wat het complex maakt om tot een eenduidig en gedegen document te komen, is dat er maar liefst 80 publieke en private partijen meewerken aan het CSBN. Denk aan brancheverenigingen als NL-ICT, de bedrijven die zij weer vertegenwoordigen en overheidsorganisaties als de Belastingdienst, het ministerie van Defensie en de AIVD. Rogier: "Ieder jaar is het een uitdaging die de nodige tact vereist, want we maken een onafhankelijk cybersecuritybeeld en we willen ook dat onze partners er nu én in de toekomst aan willen blijven bijdragen. Daarom werken we heel transparant."

Mission impossible?

Hoe houd je dat werkbaar? Tachtig partijen inspraak geven, is dat geen mission impossible? "Nee. We werken met een brede klankbordgroep van negen partijen die samen een dwarsdoorsnede zijn van alle partners," legt eindredacteur Koen Sandbrink uit. "We leggen de nadruk op de feiten. Daarnaast zeggen we verder altijd wat we hebben gedaan met iemands' input en waarom. Dat helpt want dan krijg je meer onderling begrip. En dus een duurzame samenwerking."
Het Cybersecuritybeeld Nederland moet voor het reces bij de Tweede Kamer liggen; een harde deadline en vooral tegen het einde "elk jaar weer een logistieke puzzel", zegt Koen, die dit jaar voor de tweede keer heeft meegewerkt aan het document. "Ons grote voordeel is dat het NCSC onafhankelijk is dus we komen er gelukkig altijd wel uit." Rogier: 'Om het zo werkbaar mogelijk te houden, presenteren we feiten en ontwikkelingen vanuit een holistisch perspectief. Dit perspectief wordt gevormd vanuit de oogpunten van de verschillende betrokken partijen en natuurlijk vanuit de kennis en expertise van het NCSC. Immers Defensie kijkt naar cybersecurity vanuit het oogpunt van de hoofdtaken van Defensie en een telecombedrijf doet dat vanuit klantoogpunt en netwerkveiligheid. Wij geven een trendbeschrijving van de cyberwereld en duiding daaraan maar het is daarna aan de ministeries en bedrijven zelf wat zij met die informatie doen." Geeft het NCSC dan helemaal geen advies? Rogier: "Als we het document opsturen naar de Tweede Kamer worden in een aparte brief wel de beleidsimplicaties gepresenteerd. Verder brengt het NCSC jaarlijks veel adviezen uit, die we bijvoorbeeld publiceren als factsheet op onze website." Zorgen dat het CSBN er komt, blijkt een tijdrovende klus. Lachend: 'eigenlijk kunnen we nauwelijks uitrekenen hoeveel tijd het kost." Rogier: "We zijn er zeker een half jaar mee bezig. En ondanks dat we veel inhoudelijke informatie al in huis hebben, is het veel werk om 80 partijen op één lijn zien te krijgen en te houden. En de cyberanalyses lopen natuurlijk door." Koen: "Er zijn twee reviewrondes: één interne, één externe en dan moeten we alle informatie verwerken, wat bepaald geen misselijke klus is."'
Kas, de man van de statistieken, houdt zich vooral bezig met 'het goed en duidelijk presenteren' van de informatie. Niet altijd gemakkelijk, zo blijkt. "Soms bestaan er geen harde cijfers, want hoe maak je 'veiligheid' meetbaar? Samen met universiteiten zoeken we dus steeds naar manieren om dat in de volgende edities van het CSBN te verbeteren."

Steeds belangrijker: responsible disclosure

Via responsible disclosure-meldingen geven hackers ontdekte zwakheden door aan de betreffende partij, voor zij het kenbaar maken aan de buitenwereld, zodat de organisatie eerst zelf orde op zaken kan stellen.

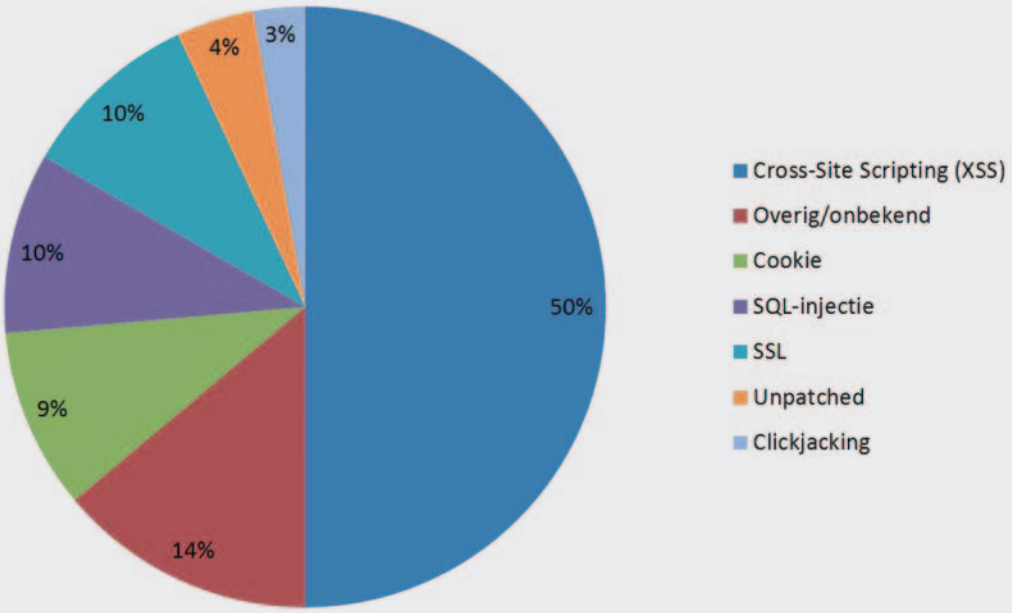
De cijfers

- **95 responsible meldingen aan het NCSC tussen april '13 en maart '14; een stijgende lijn**
- **76% van die meldingen ging over een websitekwetsbaarheid (vaak Cross-Site Scripting)**
- **17% over een configuratieprobleem**
- **4% betrof een 'false positieve'; er was geen probleem**
- **2% was een kwetsbaarheid in software**
- **1% was een 'overige' melding**

Hoe werkt het?

Een voorbeeld van een kwetsbaarheid die via responsible disclosure is gemeld, was er een in Microsoft Internet Explorer. Onderzoeker 'Hoodie22' meldde het NCSC in september '13 misbruik te zien van deze tot dan toe onbekende zwakte die kon leiden tot een gecorrumpeerd geheugen en daarmee het uitvoeren van willekeurige code (CVE-2013-3897). Via het NCSC werd de melding anoniem doorgezet naar Microsoft waarna de softwaregigant in oktober '13 een patch uitbracht om de kwetsbaarheid te verhelpen. In Microsofts advisory (MS13-080) werd 'Hoodie22' expliciet bedankt voor zijn bijdrage.

Bron: NCSC



Welke websitekwetsbaarheden worden het meest gemeld?

Eye-opener: ict-duurzaamheid

Dit jaar nam het NCSC voor het eerst een aantal vitale sectoren zichtbaar mee in het CSBN, zoals transport, telecom, energie en zorg. Het CSBN bevat dit jaar vier kernbevindingen. Sommige zijn een vervolg op voorgaande jaren, zoals dat de impact van cyberaanvallen en verstoringen verder toeneemt door de verdergaande digitalisering. Andere zijn volledig nieuw, zoals risico's die ontstaan door het gebrek aan ict-duurzaamheid. Rogier: "Ict is verantwoordelijk voor de aansturing en werking van bijna alle fysieke apparaten, zoals cv-ketels, auto's en medische apparatuur. De software van deze apparatuur bevat beveiligingslekken en het oplossen en updaten van deze kwetsbaarheden is niet eenvoudig. Ook zal niet alle software gedurende de gebruikstijd van de apparatuur onderhouden

Het CSBN bevat dit jaar vier kernbevindingen. Sommige zijn een vervolg op voorgaande jaren, zoals dat de impact van cyberaanvallen en verstoringen verder toeneemt door de verdergaande digitalisering.

kunnen worden. Hierdoor ontstaat een potentieel probleem met het waarborgen van de maatschappelijke veiligheid, zeker omdat de apparatuur steeds meer aan internet is gekoppeld. Dit is een gebrek aan duurzaamheid, of houdbaarheid, van ict." De risico's lijken fors. Denk aan aanvallen via internetverbindingen op systemen met een fysieke werking, zoals auto's of medische apparatuur. Dat heeft directe gevolgen voor de persoonlijke veiligheid van gebruikers of de economische continuïteit van organisaties. Een pasklare oplossing is er niet. De traditionele manier van updaten, onderhouden en tijdig vervangen werkt vaak niet voor deze systemen en daarom moet er nu worden nagedacht over de omgang met de veroudering van apparatuur, volgens het NCSC.

Wat geeft de meeste dreiging?

In het CSBN is aandacht voor ongewenste activiteiten van statelijke actoren. Is dit waar Nederland zich als eerste tegen moet wapenen? Moeten we banger zijn voor een land als China dan voor een cybercrimineel in Barendrecht? Rogier: "Kijkend naar dreigingen zijn ze allebei 'spannend' en zeker belangrijk. De ene organisatie is veel kwetsbaarder voor spionage dan de andere. Banken hebben meer te duchten van cybercriminelen dan van een land, terwijl een farmaceutisch bedrijf juist vaak gevoeliger is voor spionage vanwege zeer waardevolle concurrentiegevoelige informatie. Qua maatregelen maakt het minder uit; je beveiliging tegen relevante dreigingen moet gewoon op orde zijn, of dat nou voor een cybercrimineel is of voor een statelijke actor."
De praktijk laat zien dat eindgebruikers moeilijk weerbaarder zijn te maken. Betekent dat dat al die berichten over '5 dingen die je moet doen tegen cybercrime', al die gadgets, al die tips en trucs zinloos zijn? "Nee," zegt Rogier. "Maar het kan anders. Mobiele devices bijvoorbeeld zijn steeds belangrijker in onze samenleving. Die kunnen we een stuk veiliger maken. Kijk bijvoorbeeld naar auto's. Die zijn nu veel veiliger dan vroeger. We zien dat er op dit gebied langzaam stappen worden genomen, bijvoorbeeld door leveranciers van smartphones. De tijden veranderen dus dat soort zaken moeten mee veranderen." Aan de andere kant is dat ook lastig: aanvallen worden steeds geavanceerder. Nieuw is bijvoorbeeld ransomware, waarbij een cybercrimineel informatie zoals foto's versleutelt en daarmee onbereikbaar maakt en ze pas vrijgeeft als het slachtoffer geld betaalt. Koen: "Om te voorkomen dat we achter de nieuwste ontwikkelingen aanhobbelen, moeten we goed letten op wat er gebeurt in de hacker- en academische wereld. Zij lopen vooruit op dit gebied, op basis van theorieën en praktisch onderzoek. Daar kun je dan maar beter goed op reageren want cybercriminelen lezen die onderzoeken ook en proberen dan meteen te profiteren."

Waar houdt security op en begint privacy?

Een tijd terug was in één week toevallig veel aandacht voor overheidsmaatregelen tegen cybercrime en criminaliteit in het algemeen. De overheid wil big data preventief gebruiken voor bijvoorbeeld het opstellen van 'risicoprofielen' van gewone burgers. Een ander voorbeeld is de Belastingdienst die haar gigantische database gebruikt bij het opsporen van fraudeurs. Waar houdt security op en begint privacy? Kas: "Ik kom uit de onderzoekswereld. Er gaat nu veel geld naar onderzoeken over de balans tussen security en privacy. Het is een kwestie die nu speelt en dat veel partijen daar nu mee bezig zijn. En de overheid wil dat faciliteren. Dat vind ik een geruststellend gevoel." Koen: "Cybersecurity verandert steeds. Het is de kunst niet alleen reactief te zijn, maar ook proactief en preventief. En vooral niet te vergeten dat 100 procent veiligheid gewoon niet bestaat."

Je kunt het Cybersecuritybeeld Nederland 4 downloaden van de website van het NCSC via https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-4.html

VULNERABILITY SCANNING

Praktijkervaringen binnen een academische omgeving

Dreigingen veranderen met de minuut. Om goed inzicht te krijgen aan welke risico's een organisatie bloot staat, is regelmatig onderzoek naar kwetsbaarheden vereist. Alleen dan kunnen passende corrigerende acties genomen en verrassingen voorkomen worden. Uitdaging hierbij is het om de gevonden kwetsbaarheden op de juiste manier binnen je organisatie te laten landen. Draagvlak van de organisatie en beheerders is hierbij cruciaal.

Kwetsbaarheidsscans ofwel vulnerability scanning is het geautomatiseerd zoeken naar kwetsbaarheden in software en bijbehorende configuraties. Penetration testing gaat een stap verder en probeert actief binnen te dringen in een specifieke applicatie. Met dit artikel deel ik onze ervaringen, zoals wij die hebben opgedaan bij de implementatie en het gebruik van de Rapid7 Nexpose kwetsbaarheden scan tool bij de Wageningen UR.

Aanleiding voor de implementatie was het vaststellen van een technisch auditplan voor de centrale IT-omgeving. Hierin staan uitgangspunten opgenomen en is grofweg aangegeven wanneer welke scans en interne/externe audits uitgevoerd dienen te worden. Kwetsbaarheden tests zijn één van de aandachtspunten hierbij. Verder komt kwetsbaarheden scanning terug als kritieke controlemaatregel op bijvoorbeeld de Critical Security Controls for Effective Cyber Defense lijst van SANS[1] of in de ISO 27002 standaard. Het wordt zodoende algemeen beschouwd als een belangrijke maatregel in de bescherming van informatie.

Initieel werden alle penetration tests en vulnerability scans extern uitbesteed. Echter, om eigen kennis en ervaring te kunnen opbouwen en omdat kwetsbaarheden scanning een continue of minimaal periodiek (bijvoorbeeld maandelijks) proces dient te zijn, is besloten om deze scans zelf te gaan uitvoeren. Verder speelde het feit dat bleek dat een eenmalig rapport met een lange lijst van mogelijke kwetsbaarheden door de beheerders lastig te interpreteren is op relevantie en specifieke lokale omstandigheden. Ofwel, in hoeverre zijn de gevonden kwetsbaarheden ook daadwerkelijk uit te buiten in onze situatie? Een andere reden was de reductie van externe kosten voor kwetsbaarheden scans en de mogelijkheid om de kwetsbaarheden tool te kunnen inzetten ter ondersteuning van penetration tests.

Selectie

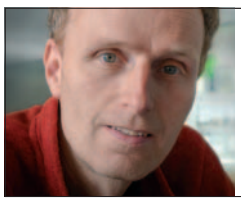
Nadat het besluit genomen was om kwetsbaarheden scanning zelf te gaan uitvoeren is onderzocht welke producten er op de markt zijn en waarin ze verschillen. Het bleek nog niet zo eenvoudig om een helder beeld te krijgen van de verschillen tussen de diverse leveranciers. De functionaliteit verschilt sterk, zo is de ene tool beperkter en enkel gericht op netwerk of webscanning en biedt de andere tooling uitgebreidere functionaliteit om het hele vulnerability managementproces te ondersteunen. De Wageningen UR heeft specifieker gekeken naar de mogelijkheden die o.a. Nessus, QualysGuard, Core Impact, Nexpose/Metasploit boden. Er is uiteindelijk gekozen voor Rapid7 Nexpose in combinatie met Metasploit. Voor specifieke applicaties zoals web-applicaties en SAP blijven aanvullende specifieke tools nodig.

Selectiecriteria

- bewezen technologie en dus geen nieuwkomer op de markt
- grote, actuele en gevalideerde kennisbank van kwetsbaarheden
- bij voorkeur mogelijkheid voor lokale installatie
- goede mogelijkheden tot rapportages op verschillende niveaus (management maar ook detail en achtergrond informatie over de bevindingen en praktische instructies hoe de kwetsbaarheden op te lossen zijn)
- mogelijkheden voor goede en snelle support en partnership met de producent en leverancier
- prijs
- weinig false positives
- mogelijkheid om te valideren dat kwetsbaarheden daadwerkelijk uit te buiten zijn
- stabiliteit en betrouwbaarheid van de tool ten aanzien van verstoringen op gescande omgevingen

Implementatie

Na de keuze voor de tooling diende deze geïnstalleerd te worden en geconfigureerd te worden op basis van onze eigen wensen. Hieronder een toelichting op een aantal van onze keuzes en aandachtspunten waar wij tegen aan liepen. Nadruk ligt hierbij op de ervaringen met Nexpose en minder op Metasploit.



Raoul Vernède. Raoul is werkzaam als security manager bij Wageningen UR.
Hij is te bereiken via raoul.vernede@wur.nl

Installatie van Nexpose en Metasploit werd gedaan op een eigen managed Linux server en verliep relatief makkelijk. De integratie tussen Nexpose en Metasploit werkt jammer genoeg nog niet optimaal.

Scans kunnen uitgevoerd worden als externe non-authenticated scans (oogpunt van externe hacker) met een beperkte resultaat. Anderzijds kunnen de scans draaien met de toegangcredentials van de servers (geauthentiseerde scans) en zo extra en meer diepgaande informatie vergaren.

Wij hebben er voor gekozen om al onze scans authenticated te draaien. Het is dan natuurlijk cruciaal dat de wachtwoorden zorgvuldig beschermd worden binnen de scantool en tijdens het inlogproces. Een optie hierbij is om een apart specifiek account voor de scantool te gebruiken waarbij het wachtwoord periodiek gewijzigd wordt. Check in hoeverre de vulnerability applicatie is gepentest door de leverancier of voer zelf een penetratietest uit. Zorg er verder natuurlijk voor dat updates op OS- en Rapid7-niveau snel uitgerold worden.

in hoeverre zijn de gevonden kwetsbaarheden ook daadwerkelijk uit te buiten

Al onze fysieke en virtuele servers in beide datacentra van zowel de productie als ook OTA (ontwikkel-, test- en acceptatie) omgevingen worden maandelijks gescand. Het scannen gebeurt overdag omdat bij eventuele problemen direct ingegrepen kan worden. Wij scannen niet tegen bepaalde standaard policies, zoals die bijvoorbeeld in de bankenwereld vaker gehanteerd worden (bijvoorbeeld PCI). In de planning van de scans houden wij rekening met de maandelijkse updates van Microsoft. Zodoende gebruiken we Nexpose ook om te controleren of alle updates en patches zijn uitgerold. Tussen het scannen van de OTA en de productie omgeving zit een week; mogelijke verstoringen zoals datacorruptie door SQL-injection komen dan vroegtijdig aan het licht. Bedoeling is om op een later tijdstip ook de decentrale servers buiten de datacentra te gaan scannen. In geval van ontdekking van ernstige nieuwe kwetsbaarheden (denk aan Heartbleed) dient tussentijds gescand te worden.

Bij de inrichting van Nexpose is het mogelijk IP-ranges automatisch in kaart te brengen (via discovery). Er is geen integratie met bijvoorbeeld Active Directory of DNS om servers automatisch te provisionen. Er is een koppeling met VMware mogelijk maar dit werkt alleen voor virtuele machines.

Het ontbreken van een dergelijke integratie veroorzaakt voor ons veel administratief werk. Feitelijk importeren we nu uit de CMDB een serverlijst in Nexpose. Het blijkt hierbij in de praktijk wel lastig om de serverlijst (of asset-lijst) in Nexpose up-to-date te houden. Heeft men wel een up-to-date CMDB, dan kan Nexpose gebruikt worden om rogue apparaten te ontdekken en om de CMDB op correctheid te checken.

Bij de inrichting van Nexpose hebben wij er voor gekozen om een verbinding te maken tussen de verschillende teams en beheerders en anderzijds de servers die zij beheren. Dit is voor ons cruciaal. Hierdoor is het makkelijker om de bevindingen van de scans (via specifieke rapportages) terug te koppelen aan de verantwoordelijke teams (bijvoorbeeld database, web, etc.) met hun technische beheerders. De beheerder kent de servers die hij beheert en kan de bevindingen interpreteren en eventueel corrigerende maatregelen nemen. Beheerders hebben het vaak erg druk met het uitrollen van nieuwe functionaliteit en andere dagelijkse werkzaamheden. Hierdoor ontstaat het risico dat de resultaten van de scan (te) lang blijven liggen.

De DNS naamgeving van onze servers bestaat uit een letter/nummer combinatie. Daarnaast staat er in de CMDB ook een korte beschrijving, maar deze kan standaard jammer genoeg niet ingelezen worden. Voor de beheerders is het vaak lastig om enkel aan deze server-ID vast te stellen om welk type server het gaat. Wij hebben er daarom voor gekozen om via een API van Nexpose deze aanvullende gegevens uit onze CMDB in te lezen. Voor het ontwikkelen en testen van deze interface is een aparte Nexpose omgeving nodig. Hierbij dienen vooraf heldere afspraken gemaakt te worden over het licentiegebruik.

De initieel gevonden aantallen gelijke kwetsbaarheden over diverse servers is relatief groot. Er is daarom besloten om de gevonden kwetsbaarheden niet automatisch om te zetten in tickets van ons eigen service management system (dit zou kunnen via e-mail of XML). Ook is er voor gekozen om niet het ticketsysteem binnen Nexpose te gebruiken. Dit zou tot verwarring kunnen leiden bij de beheerders. Bevindingen uit Nexpose worden via het standaard changeproces verder afgewikkeld. De beheerder van de server is verantwoordelijk om gevonden kwetsbaarheden te analyseren en corrigerende maatregelen te initiëren.

Het bleek jammer genoeg, dat het scannen van virtual appliances binnen onze Citrix omgeving niet mogelijk is. Tevens bleek door een bug het juist scannen van Microsoft SharePoint omgevingen voorlopig niet mogelijk te zijn. Ernstige tekortkomingen van Nexpose.

Wat heel handig is binnen Nexpose is de mogelijkheid om tijdsgebonden ontheffingen te registreren. Kwetsbaarheden die om specifieke redenen niet van toepassing zijn of later opgepakt worden, kunnen zodoende tijdelijk verwijderd worden uit de rapportages. Goedkeuring van de door de beheerders aangevraagde ontheffingen gebeurt centraal door de security manager.

Het blijkt binnen Nexpose niet mogelijk te zijn om op een webserver alle aanwezige websites automatisch te detecteren en af te scannen. Een IP-adres kan verbonden zijn aan meerdere hostnames en verder bemoeilijken loadbalancers en reverse proxy ook detectie. Enige oplossing is om alle relevante URL's en IP-adressen uit de CMDB of andere bron in te voeren in Nexpose. Een optie is ook om de gegevens via een aparte crawler tool te verzamelen. Doordat bij ons de CMDB op dit punt niet compleet is, worden wij gedwongen om onze interne en externe DNS-gegevens uit te lezen en om te zetten. Commerciële partijen zullen waarschijnlijk scherper hebben welke externe websites ze hosten maar binnen een academische omgeving bestaan er eenvoudig weg te veel sites. Aan de andere kant is het ook voor ons cruciaal om grip te krijgen op deze sites en verouderde omgevingen te upgraden, dan wel af te sluiten. Mogelijk biedt Metasploit meer functionaliteit dan Nexpose ten aanzien van web applicatie scanning.

Takeaways

- Meten is weten; begin met scannen op kwetsbaarheden
- Wees niet verbaasd en word niet ontmoedigd als veel tot heel veel kwetsbaarheden gevonden worden
- Prioriteer, maak keuzes en begin met de belangrijkste kwetsbaarheden
- Besteed veel aandacht aan de manier van presenteren; goede overzichtelijke rapporten zijn cruciaal
- Zorg dat verantwoordelijkheden ten aanzien van het verhelpen van kwetsbaarheden helder zijn over de hele software-stack heen
- Realiseer je dat je nooit klaar bent

Resultaten

Inmiddels draait Rapid7 tooling bijna een jaar en is het een goed moment om terug te kijken naar de gemaakte keuzes en ervaringen.

Bij het scannen worden initieel substantiële hoeveelheden kwetsbaarheden gevonden. Deze variëren van urgente tot minder belangrijke aandachtspunten. Indien men de kwetsbaarheden optelt per server ontstaan er enorme aantallen. Doordat ergens bijvoorbeeld een update mist die meerdere bugs verhelpt, kunnen er veel kwetsbaarheden ontstaan. Voor een drukke beheerder werken de grote aantallen kwetsbaarheden afschrikkend. De beheerder wil weten wat er moet gebeuren en is niet zo zeer geïnteresseerd hoeveel kwetsbaarheden dat oplost. De insteek bij Nexpose, maar waarschijnlijk ook bij andere tools, is echter enkel kwetsbaarheden en niet zozeer een overzicht van oorzaken en te ondernemen acties. Het is dus belangrijk om passende rapporten te maken voor de beheerders.

Bij het scannen van onze servers werden relatief veel verouderde "client"-software (denk aan Adobe reader, diverse browsers, Java) op servers gevonden. Dit gaat tegen ons beleid in. Deze software dient verwijderd te worden of in uitzonderingsgevallen, indien nodig voor het functioneren van de server, geüpdate te worden.

Het aanpassen van bestaande standaard rapporten dan wel het maken van nieuwe passende rapporten is best lastig. Het is echter wel cruciaal voor de bruikbaarheid voor en draagvlak bij de beheerders. En de wensen zijn verschillend; de ene beheerder wil het zo en de ander zo. Denk ook goed na welke rapporten er voor het management gemaakt dienen te worden. Nexpose biedt hierin echter veel mogelijkheden. Wees er alert op dat overzichtsrapporten door bijvoorbeeld teamcoördinatoren ook geïnterpreteerd kunnen worden als een soort controlerapporten van hun werkwijze. Dit kan weerstand opleveren.

Het is verstandig om productieverstoringen te vermijden om in principe eerst de OTA-omgeving en pas naderhand de productieomgeving te scannen. Wij scanden na het uitkomen van de Heartbleed kwetsbaarheid direct alle servers. Maar door een bug in de meest recente update van de engine werden echter veel van onze servers onbereikbaar. Dit leverde veel extra werk op en zorgde voor de nodige kritiek op Nexpose.

Maak een onderscheid in specifieke kwetsbaarheden die een individuele beheerder kan oppakken en anderzijds in meer generieke kwetsbaarheden. Denk bij deze laatste categorie aan zaken als de generieke instellingen van de TLS/SSL versie,

self-signed certificates, SMB configuratie of het gebruik van verouderde ciphers. Doordat de impact op de hele omgeving bij aanpassing groot en complex is, dienen dit soort zaken als project opgepakt te worden. Deze bevindingen kunnen wel gebruikt worden om de huidige dan wel toekomstige (bijvoorbeeld server 2012) configuratie template van een standaard managed server verder aan te scherpen.

Doordat de applicatiebeheerders bij de Wageningen UR per domein/kolom (verticaal) en de systeembeheerders per OS (Linux/Windows) (horizontaal) zijn ingedeeld, is het belangrijk om te bepalen wie welke kwetsbaarheid oppakt. In vele gevallen is het helder, maar zeker bij overlappende zaken dient er helderheid van verantwoordelijkheden te zijn. Als voorbeeld hier het punt dat Apache Tomcat op Linux machines normaal gesproken automatisch meeloopt met de updates, maar dat er ook installaties zijn op Windows machines waarbij dat niet het geval is.

Diverse softwareleveranciers leveren beperkte of soms geen ondersteuning dan wel willen geen garanties afgeven dat hun applicatie functioneert op een geüpdate versie van het OS of de middleware. Denk hierbij bijvoorbeeld aan nieuwere versies van Java, Tomcat Apache of Oracle. Enkel tegen extra kosten en/of na langere tijd worden de pakketten aangepast. Zeker voor specialistische onderzoek en onderwijs-software van deels kleine leveranciers zorgt dit voor beperkingen om tijdig te kunnen upgraden en zodoende kwetsbaarheden te verhelpen.

Binnen Metasploit Pro is er de mogelijkheid om (nep-)phishing e-mail campagnes te simuleren. Het inrichten van zo'n campagne werkt handig en geeft heldere overzichten of de ontvangers de mail ontvangen hebben, op de link geklikt hebben en of ze inderdaad een wachtwoord ingevuld hebben. De tool is ook in staat om eenvoudig bijvoorbeeld een bedrijfsspecifieke OWA (Outlook Web Access) site te klonen. Naar de kopie site kan dan verwezen worden in de nep-phishing mail. Wageningen UR heeft rond de 5000 nep-phishing mails verstuurd. Hiervan gaven een substantieel aantal ontvangers daadwerkelijk ook hun wachtwoord af. Dit was hoger dan verwacht en zorgde ervoor dat er een bewustwordingscampagne gestart is voor eindgebruikers. Phishing mails zijn iets waarvan managers en beslissers de impact makkelijk snappen. Zodoende lukt het om informatiebeveiliging hoger op de agenda te krijgen.

onderscheidt kwetsbaarheden die een individuele beheerder kan oppakken van de generieke

Het verdere gebruik van Metasploit is bij Wageningen UR nog relatief beperkt en wij zouden waarschijnlijk grotendeels ook uit de voeten kunnen met de community versie. De integratie met Nexpose is slechts beperkt en levert nog weinig meerwaarde.

Op basis van de opgedane ervaring en kaders dienen de security eisen helder en formeel vastgelegd te worden in een vulnerability management policy. Hierin dienen zaken te zijn opgenomen als periodiciteit, vorm van scannen, omgang met uitzonderingen en ontheffingen, opvolging van bevindingen et cetera.

Conclusies

Wees niet te ambitieus en realiseer je dat voor de beheerder kwetsbaarheden extra werk betekent. Er ontstaat daarom initieel weerstand en de roep om veel extra menskracht. Maar wees realistisch en probeer te focussen op de meest belangrijke kwetsbaarheden en stapje voor stapje verder te komen. Verschillen tussen beheerders over de belangrijkheid en invulling van veilige servers komen ook aan het licht. Voor de ene beheerder is functionaliteit en tevreden gebruikers belangrijker dan security, en vice versa. Gebruik van een kwetsbaarheden tool zorgt dus ook voor het vergroten van de bewustwording bij beheerders. Blijf herhalen en uitleggen; het duurt enige tijd voordat beheerders de resultaten uit de scantool systematisch gaan gebruiken. De tool is enkel een hulpmiddel; de beheerders en een bijbehorend proces moeten het verschil gaan maken.

- **gebruik tool is lastiger dan gedacht**
- **problemen doken op waarover niet van te voren nagedacht**
- **meer ook een proces met mensen**
- **extra werk levert weerstand op**
- **last van beperkingen tool en support**
- **meer aandacht en draagvlak uiteindelijk voor security**
- **mogelijkheid om snel te kunnen scannen op specifieke kwetsbaarheden**

Links

[1] SANS Critical Security Controls for Effective Cyber Defense: http://www.sans.org/critical-security-controls

JE ZULT MAAR ZIEK ZIJN

Ik ben ziek. Al een tijdje. Wat er precies aan de hand is weten de dokters niet, maar met zorg wordt gezocht naar een mogelijke oorzaak. Hoe langer het voortduurt hoe meer mensen zich met mijn zaak gaan bemoeien. En waar ik eerst nog alleen maar op oorzaak, aanpak en herstel gericht was, begin ik me nu de laatste dagen in toenemende mate ook zorgen te maken over mijn privacy. Beroepsgedeformeerd. Daar leid ik in ieder geval aantoonbaar aan.

Familie en vrienden zijn op de hoogte van het reilen en zeilen. Maar ook mijn eigen huisarts, de tweede huisarts die erbij geroepen werd voor een beoordeling van de uitslagen van testen. De verpleegkundige die alle testen afnam. Mijn direct leidinggevende, het hoofd van de afdeling waar ik werk. De arbo-arts. De telefoniste van de arbo-instantie. Mijn secretaresse. De internist in het ziekenhuis. Wellicht straks ook nog specialisten in tropische ziektes. En vast nog meer verpleegkundigen. En de apotheker en de zorgverzekeraar. De lijst groeit elke week door.

De arbo-instantie heeft (net als mijn eigen arts) een medisch dossier over mij samengesteld. Dat dossier bewaart de instantie 10 jaar. De termijn gaat lopen na ons laatste contact. Ik vind dat erg lang. Maar, het is binnen de regels die het CBP daar zelf voor heeft opgesteld, zij stelt zelfs een nog langere termijn voor, namelijk 15 jaar. Ik vraag me oprecht af of het noodzakelijk is om mijn medische gegevens (het zijn immers ook nog eens gevoelige gegevens) zo lang te bewaren. Dat mijn huisarts mijn medisch dossier onder zich heeft voelt voor mij prima. Maar waarom de arbo-instantie zo lang het dossier onder zich moet houden?

Afgelopen november vond er een Algemeen Overleg in de Tweede Kamer plaats over de decentralisatieslag van onze overheid. Gemeenten krijgen er vanaf januari 2015 een aantal taken bij, waaronder de zorg voor langdurig zieken. Meerdere malen heeft het CBP dit jaar haar ernstige zorgen daarover uitgesproken. Gemeenten gaan aantoonbaar niet goed om met persoonsgegevens, hebben de zaakjes vaak niet op orde en het ontbreekt regelmatig aan een goede beveiliging. Dat is des te nijpender nu het gaat over medische gegevens omdat deze met nog meer zorg moeten worden behandeld dan "gewone" persoonsgegevens.

Vlak voor dit overleg bleek overigens dat het nieuwe Landelijk Schakel Punt (LSP) – de opvolger van het elektronisch patiëntendossier – medische gegevens uitwisselt zonder toestemming van de patiënt. Althans, zo bleek in een aantal door het CBP onderzochte gevallen. Het euvel is inmiddels opgelost, maar ook nu weer blijkt het toch niet helemaal goed te zitten met het al zo lang geplaagde vastleggen en uitwisselen van patiëntengegevens. Daar kwam nog eens bovenop dat veel commerciële verzuimbedrijven de privacy van zieke werknemers schenden doordat telefonistes een medisch dossier aanleggen, allerlei zaken kunnen inzien en dat ook werkgevers daar toegang toe hebben. Hetgeen bij wet verboden is.

Een patiënt zou zich over alle bovenstaande zaken geen zorgen moeten hoeven maken. Die heeft namelijk al genoeg aan zijn hoofd. Gelukkig is niet iedere zieke een beroepsgedeformeerde privacy officer, maar het zou al heel veel helpen als naast het CBP ook anderen zich hierover eens zorgen gingen maken.

Mr. Rachel Marbus,
@rachelmarbus op Twitter

DE VOLGENDE FASE VAN SIEM: SITUATION AWARE SECURITY OPERATION CENTER

DE CONVERGENTIESLAG

De bekende security industrieanalist en visionair Steve Hunt schreef er in 2005 al over, convergentie tussen SIEM en PSIM. In de visie van Steve Hunt levert integratie van SIEM met PSIM veel efficiency voordelen op. Immers incidenten en events kunnen grotendeels door hetzelfde proces worden afgehandeld. Er ontstaat vanuit één centraalpunt een overzicht over alle ICT en non-ICT security incidenten [1].

Door het continue monitoren en analyseren van systemen en logging kan men veel proactiever handelen op mogelijke security issues. Geheel volgens de visie van Steve Hunt introduceerden technologie providers zoals NICE [2] en Proximex [3] (onderdeel van TYCO security) in 2011 de eerste commercieel verkrijgbare SIEM/PSIM oplossingen gedreven vanuit de NERC-CIP regelgeving.

In november 2013 startte de Europese Unie het project Situation AWare Security Operation Center (SAWSOC) [4]. Doel van het SAWSOC is vaststellen en implementeren van technieken die nodig zijn voor de convergentie tussen physical en cybersecurity. SAWSOC is een samenwerkingsproject tussen een aantal onderzoeksinstellingen, universiteiten en IT bedrijven uit Ierland, Engeland, Israël, Finland, Duitsland en Polen. Dit project wordt gesponsord door de Europese Commissie vanuit het FP7-SECURITY Programma (SEC-2012.2.5-1 Convergence of physical and cybersecurity – Capability Project). De gedachte achter SAWSOC is dat door de holistische benadering en verbeterde technieken bewuster en betrouwbare (d.w.z. juist, tijdig en betrouwbaar) detectie en analyse van aanvallen kan plaatsvinden. Dit dient uiteindelijk te leiden tot het verwezenlijken van de twee grote belangrijke doelstellingen van SAWSOC.

1. **De belofte voor bescherming/beveiliging van burgers en goederen**
2. **Het verbeteren van de perceptie van veiligheid door burgers**

Het totale SAWSOC-project duurt 30 maanden en kent een budget van ongeveer 5 miljoen euro, waarvan 3,4 miljoen wordt bijgedragen door Europese commissie. Het project kent 11 partners uit 7 landen. Het project SAWSOC dient in mei 2016 een platform op te leveren op basis waarvan systemen kunnen worden ontworpen en wat echte convergentie van physical en cyber security technologieën bewerkstelligd en wat verdere versnippering voorkomt.

Wasdom

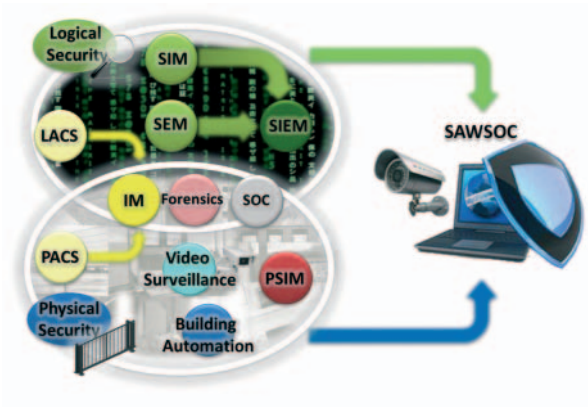
Willen we echt wat kunnen met SAWSOC dan is het van belang dat de drie belangrijkste elementen in SAWSOC tot wasdom komen. De belangrijkste elementen binnen SAWSOC zijn:

1. **Security Information & Event Monitoring (SIEM)**
2. **Physical Security Information Management (PSIM)**
3. **Identity Management (IM)**

Security Information & Event Monitoring (SIEM) is binnen de ICT security ondertussen een geworteld begrip. Een SIEM geeft grip en inzicht in alle mogelijke netwerkbeveiliging risico's en bedreigingen. SIEM maakt het geautomatiseerd monitoren en controleren van het beveiligingsbeleid van een organisatie mogelijk. Een SIEM doet dit door real-time informatie te verzamelen uit logfiles van netwerk- componenten, tools, security-componenten, servers, laptops, desktops, applicaties en databases en deze vervolgens te correleren en te analyseren en te presenteren en om security threats te detecteren. Een belangrijk aspect hierbij is de correlatie, waarbij verbanden tussen logs gezocht worden. Hierdoor geeft een SIEM een overzichtelijk beeld van de actuele status van de ICT security. Wat een

Ronald Eygendaal. Ronald is freelance verslaggever en tijdschriftschrijver. Hij schrijft sinds 1999 in de vakbladen over informatiebeveiliging, elektronische & technisch beveiliging, fraude detectie & bestrijding en bewaking & beveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsprofessionals Nederland (VBN).

SIEM doet in de ICT security wereld, doet een PSIM (Physical Security Information Management) voor de physical security wereld.



Een PSIM is een software platform dat verschillende losse (beveiliging)systemen integreert die beheert worden via een uitgebreide meestal grafische gebruikersinterface. Hierdoor kan men dagelijkse operationele handelingen, incident management en crisisbeheersing op een duidelijke, gestructureerde en controleerbare wijze uitvoeren. Zo worden camerasystemen, toegangscontrole, inbraakdetectie en ander soortgelijke systemen samengebracht in PSIM. In de basis hebben een SIEM en een PSIM een vijftal identieke hoofdfuncties, te weten:

1. Collection - via onafhankelijke device management software kan het systeem gegevens verzamelen van een willekeurig aantal uiteenlopende beveiligingssystemen en apparaten.
2. Analyse - het systeem kan gecollecteerde informatie zoals data, gebeurtenissen, alarmen en andere belangrijke gegevens, analyseren en correleren.
3. Verificatie - de gegevens uit de analysefase worden gefilterd, geïdentificeerd en geperiodiseerd op zodanige wijze dat ze inzichtelijk worden voor de security operators
4. Resolutie (incident response) - het systeem voorziet in een unieke set van standaard operationele procedures (SOP's) welke afgeleid zijn van beleid en best practices afspraken van de organisatie. Door deze stap-voor-stap instructies zijn security operators in staat de gebeurtenissen af te handelen in het geval van een noodsituatie.
5. Rapportage - het systeem verzamelt niet alleen informatie aan het begin, maar regisseert ook alle informatie en overzicht van genomen acties en maatregelen. Dit kan achteraf worden gebruikt voor rapportage doeleinden.

In SAWSOC komen SIEM en PSIM echt samen.

Identity Management

Voor de convergentie tussen SIEM en een PSIM is het hebben van één identiteit in zowel de physical en cyberwereld noodzakelijk. Immer hoe kan je anders relatie leggen tussen de virtuele en fysieke persoon. Sinds 2009 is er een trend gaande om Logical Access Control Systems (LACS) en Physical Access Control Systems (PACS) samen te voegen tot Identity Management. Convergentie naar één identiteit brengt onder meer authenticatie naar een hoger model.

Zo kun je naast de drie klassieke authenticatie-elementen (wat je weet, wat je hebt, wie je bent) nu ook een vierde element namelijk 'waar je bent', in het authenticatieproces worden gebruikt. Een ander groot voordeel van convergentie naar één identiteit is kostenreductie. Geïsoleerde oplossingen bieden onvoldoende garantie: gaten in proces van uitgifte en inname van rechten kunnen gemakkelijk ontstaan. Door convergentie tussen de physical en cybersecurity werelden kunnen de processen rond rechtenbeheer worden vereenvoudigd en verbeterd en worden kosten bespaard. Kortweg betekent convergentie meer veiligheid tegen minder kosten.

Conclusie

SAWSOC zal een geavanceerde Security Operations Center (SOC) platform opleveren. Hierdoor kunnen accurate, tijdige en betrouwbare detectie en diagnose van aanvallen worden ondersteund. Daarnaast kan met correlerende gebeurtenissen uit een breed scala van fysieke en logische beveiligingsbronnen een verbeterde situational awareness worden ontwikkeld.

Echter, in de dagelijkse praktijk zien we nog een stringente scheiding tussen de physical en cyber domeinen. Zo worden PSIM systemen geleverd door de elektrotechnische beveiligingsinstallateurs en SIEM wordt veelal geleverd voor de IT security bedrijven. Bedrijven die in beide werelden succesvol actief zijn, kan men op één hand tellen en succesvolle samenwerkingen tussen deze bedrijven zijn gering. Gezien de huidige legacy, de vervangingscyclus (10 jaar) en de wet en regelgeving ten aanzien van fysieke beveiliging zal het zeker nog een aantal jaren duren voordat convergentie tussen PSIM en SIEM zal plaatsvinden. Ook de benodigde convergentie naar één identiteit kent nog de nodige obstakels. Ook bij deze convergentie is de stringente scheiding tussen de domeinen één van de grootste obstakels. Dit wordt nog verstrekt doordat we qua organisatorische bedrijfsindelingen vaak de twee domeinen nog gescheiden houden. Zo is veelal facilities verantwoordelijk voor physical Security en IT voor ICT security. Pas als al deze hobbels genomen zijn kan SAWSOC tot wasdom komen.

Tenslotte, binnen het SAWSOC project ontbreken de grote leveranciers uit zowel de PSIM en SIEM securitywereld, vraag blijft daarom: gaat SAWSOC echt zorgen voor de volgende fase van SIEM? Of verbranden we 3,4 miljoen Europees geld voor niets?

Links:

[1] http://www.surveillance-magazine.com/2014/01/05/the-converging-roles-of-physical-and-it-security-and-the-rise-of-psim
[2] http://www.nice.com/news/newsletter/more2.php?page_id=467&edition=11_9s
[3] http://www.securitysquared.com/2010/03/psim-and-siem-proximex-arcsight.html
[4] http://www.sawsoc.eu/

ANALYSEREN EN AANPASSEN VAN SSL CONFIGURATIES

De afgelopen maanden zijn we opgeschrikt door verschillende kwetsbaarheden in onze SSL software. Eerst was daar Heartbleed: het lek in OpenSSL waarmee toegang tot stukjes uitgewisselde data uit SSL sessies van derden kon worden verkregen. In oktober kregen we te maken met POODLE: het lek dat een definitief einde maakte aan het SSLv3 tijdperk.

Uit onderzoeken blijkt regelmatig dat veel websites hun SSL configuratie nog niet op orde hebben. Dit artikel biedt handzame tips om SSL configuraties te controleren en te verbeteren.

Online analyse van kwetsbaarheden

Een erg bekende online scantool die zich op SSL kwetsbaarheden richt is de SSL Server Test van Qualys (https://www.ssllabs.com/ssltest/). Deze scantool geeft je binnen een paar minuten zicht op hoe krachtig de SSL configuratie van jouw website is en op wat er eventueel verbeterd kan worden.

Om de tool te kunnen gebruiken moet de website echter wel met internet verbonden zijn. En dit is natuurlijk niet het geval op het moment dat je een SSL configuratie wilt testen die enkel op het interne netwerk in gebruik is.

Offline analyse van een SSL configuratie

Om een interne SSL configuratie te controleren kan er natuurlijk gebruik worden gemaakt van commerciële kwetsbaarheden scanners, zoals Nessus, Nexpose of QualysGuard. Maar er zijn ook diverse gratis, open source tools te vinden die zich specifiek op SSL controles richten.

Nmap

Aan de Nmap Scripting Engine (NSE) zijn verschillende scripts toegevoegd die kunnen helpen om heel snel een grote hoeveelheid systemen te controleren op bijvoorbeeld de actieve SSL ciphers of de Heartbleed kwetsbaarheid. Nmap is zowel beschikbaar voor Unix, Windows als Mac gebruikers. Het gebruik van Nmap is eenvoudig:
Ciphers: nmap --script ssl-enum-ciphers -p 443 www.classity.nl
Poodle: nmap -sV --version-light --script ssl-poodle -p 443 www.classity.nl
Heartbleed: nmap --script ssl-heartbleed -p 443 www.classity.nl

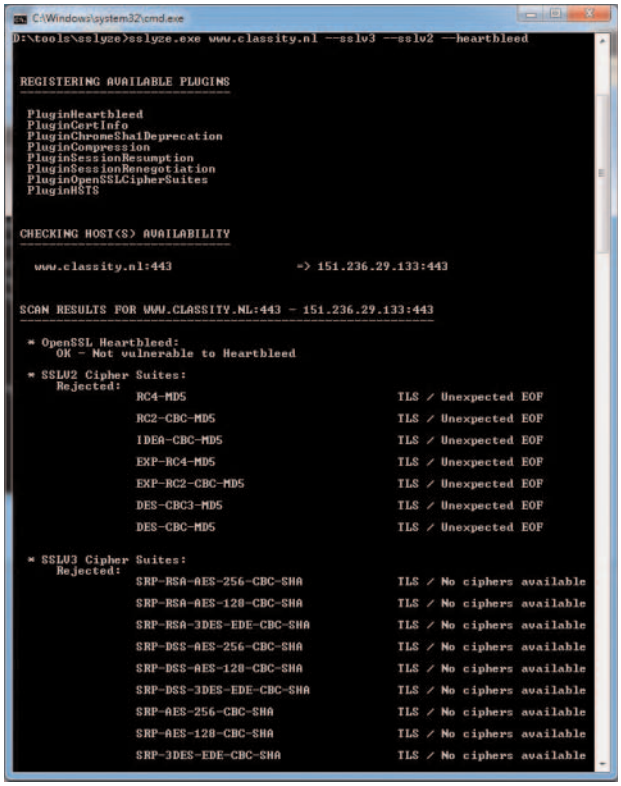
Sslyze

Sslyze is een SSL Scanner welke oorspronkelijk ontwikkeld is door het bedrijf iSECpartners. Recent is de verdere ontwikkeling van de tool overgenomen door een freelance ontwikkelaar die regelmatig aan de code bijdroeg.

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

Om de standaard SSL configuratie in Apache te verbeteren, zijn er vaak slechts een paar kleine aanpassingen nodig.

De tool is geschreven in Python, waardoor ook deze tool eenvoudig op meerdere besturingssystemen, waaronder Mac, Windows en Linux, gebruikt kan worden. De ontwikkelaar heeft ook binaries ter beschikking gesteld. Dus als je weinig ervaring met scriptingtalen hebt, hoeft je niet eerst je hele Python installatie op orde te brengen voordat je de tool kunt gebruiken. Met Sslyze kunnen diverse SSL configuratie-eigenschappen onderzocht worden. Heartbleed, POODLE, HSTS, geconfigureerde CipherSuites en ondersteuning voor secure renegotiation: ze maken er allemaal onderdeel van uit.
Je gebruikt het, bijvoorbeeld op Windows, eenvoudig vanuit de command prompt:
D:\sslyze.exe www.classity.nl --sslv3 --sslv2 –heartbleed



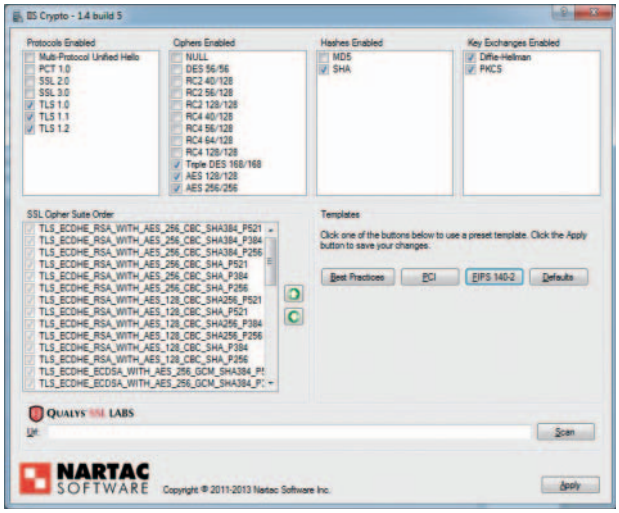
SSL configureren in Apache

Om de standaard SSL configuratie in Apache te verbeteren, zijn er vaak slechts een paar kleine aanpassingen nodig. Hieronder volgt een voorbeeld van een SSL configuratie waarin de zwakkere SSLv2 en SSLv3 protocollen zijn uitgeschakeld en sterkere TLS protocollen als voorkeursprotocol zijn gemarkeerd. Daarnaast zorgt deze voorbeeldconfiguratie ervoor dat zwakkere versleutelingsvormen zoals "null ciphers" en "RC4" niet meer actief zijn.

```
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder On
SSLCipherSuite
EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:ECDHE-RSA-
AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH
```

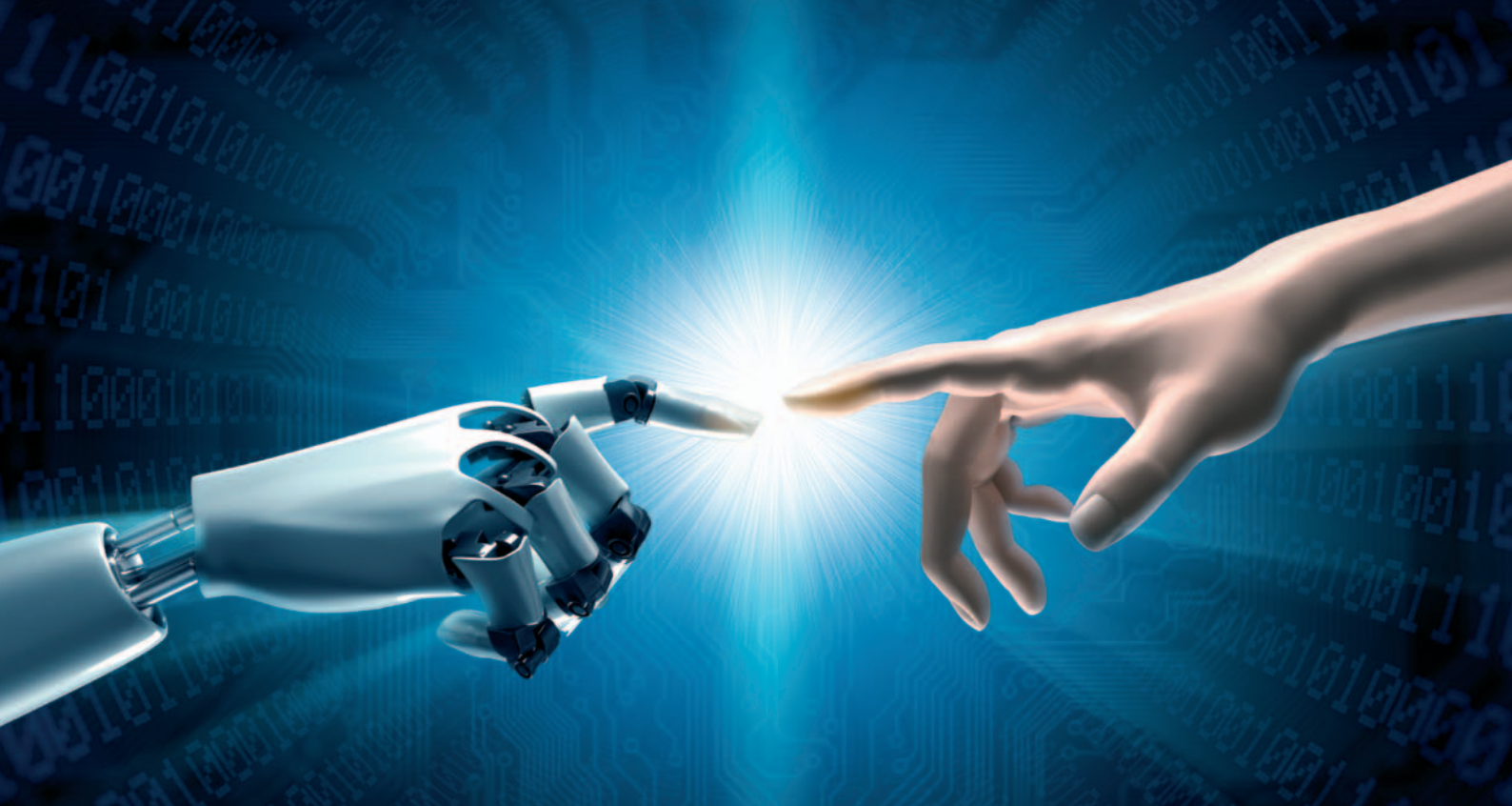
SSL Configureren in Windows

In Windows configureer je de SSL-configuratie over het algemeen via registersleutels. Deze sleutels kunnen via Group Policies eenvoudig over de verschillende servers verspreid worden. Er zijn echter ook tools beschikbaar die je in een overzichtelijke interface exact tonen hoe je SSL configuratie er nu uitziet en daarnaast de mogelijkheid bieden om het meteen aan te passen. Een voorbeeld van zo'n tool is IISCrypto, van Nartech (https://www.nartac.com/Products/IISCrypto/).



SSL implementaties breder dan HTTPS

Hoewel we ons, waar het kwetsbaarheden in SSL configuratie betreft, vaak op onze websites richten, is het gebruik van SSL natuurlijk breder dan dat. Vergeet daarom niet om bijvoorbeeld ook de e-mail configuratie te controleren. Ook protocollen als SMTP, IMAP en POP maken vaak intensief gebruik van SSL. Als we in al onze systemen onze versleutelingsinstellingen versterken is onze eigen informatie (en die van onze klanten) wederom een beetje beter beschermd.



HET FORENSIC INTELLIGENCE NETWORK OF EXCELLENCE (FINE)

De digitalisering van de maatschappij heeft een enorme impact op het Safety en Security domein. Het voorkomen en detecteren van criminaliteit wordt steeds meer gedreven door de data die beschikbaar is via het Internet of in bestanden die worden aangetroffen bij een verdachte. Deze data vormen een enorme bron van informatie, maar alleen als deze op de juiste wijze kan worden ontsloten en de informatie op juiste waarde kan worden geschat.

Marcel Worring en Cor Veenman

Het veld heeft een sterke behoefte aan Intelligente Data Analyse (IDA) technieken die met behulp van beschrijvende en inferentiële statistiek ondersteuning bieden aan dit proces van dataontsluiting en informatie extractie. Dit is een complex proces dat reikt van het beschikbaar maken van de data tot het betekenis geven, het uitfilteren van de relevante informatie en het betrekken van de onderzoeker/analist door interactie en visualisatie, waarbij juridische randvoorwaarden rond de verwerking van persoonsgegevens gewaarborgd moeten worden.
Er zijn vele partijen die een rol spelen in de keten van criminaliteitsbestrijding. Politie, justitie, veiligheidsdiensten, financiële instellingen, en verzekeraars zijn allemaal betrokken in het voorkomen en detecteren van criminele activiteiten en het adequaat hier op reageren. Nu deze taken steeds meer (big) data-gedreven zijn, is de rol van technologische ontwikkelingen rond Intelligente Data Analyse steeds groter. En met de toenemende omvang en complexiteit van de data zijn bestaande oplossingen lang niet altijd toereikend en zijn wetenschappelijke instellingen van belang om de nodige kennis voor de lange termijn te waarborgen. De diversiteit aan betrokkenen is groot, zowel ten aanzien van de rol in de keten als ten aanzien van gebruik van IDA technologie en ontwikkeling ervan. Hierdoor komen samenwerking en kennisdeling in het veld niet vanzelfsprekend tot stand.

Het bij elkaar brengen van partners in de keten ligt aan de basis van het Forensic Intelligence Network of Excellence (FINE). FINE is de beroepsvereniging voor alle professionals die zich ergens langs de keten bezighouden met data analyse op het terrein van Safety en Security. De vereniging is in 2012 opgericht met vertegenwoordigers van NFI, Achmea, ING, IBM, Microsoft en Fox IT en sindsdien is het bestuur uitgebreid met Deloitte en UvA. Het doel van de vereniging is het ontwikkelen van het vakgebied Intelligente Data Analyse gericht op het terugdringen van criminaliteit, het ondersteunen van de beroepsbeoefenaren in dit vakgebied, en het stimuleren van samenwerking en kennisuitwisseling tussen deze beroepsbeoefenaren.

Werkwijze

FINE ontplooit diverse activiteiten om haar leden te ondersteunen in hun werk. Het meest zichtbare is de jaarlijkse conferentie waar gastsprekers uit het veld hun inzichten delen en waar de leden knelpunten en mogelijkheden kunnen aangeven om technologische ontwikkelingen te stimuleren. Maar de beroepsvereniging biedt veel meer. Van groot belang zijn de werkgroepen die zich elk bezighouden met een specifiek onderdeel van het veld. Op dit moment zijn de volgende werkgroepen actief:

- Conferenties en Thematours: naast de hierboven genoemde jaarlijkse conferentie organiseert deze werkgroep thematours. Bij de thematours gaan diverse groepen leden vanuit de praktijk, de technologie, en de wetenschap rond een specifiek thema met elkaar in gesprek. Hierbij worden gezamenlijk bezoeken gebracht aan bedrijven of organisaties die in dit thema actief zijn.
- Arbeidsmarkt & Opleidingen: deze werkgroep stimuleert nieuwe initiatieven binnen het onderwijs rond intelligente data analyse en brengt aanbieders van intelligente data analyse stageplaatsen en kandidaten voor deze posities bij elkaar.
- Diensten: de diensten werkgroep is een wegwijzer voor de Openbare Orde en Veiligheid sector en helpt vraag en aanbod bij elkaar te brengen. Door middel van trendanalyses probeert de werkgroep een stevige fundering voor IDA te bieden voor nu en in de toekomst.
- Juridisch: deze werkgroep richt zich op de complexe wet- en regelgeving rondom IDA, in het bijzonder rond zaken als privacy van individuen en organisaties als informatie wordt vergaard binnen een strafzaak dan wel voor preventie of detectie.
- Research & Development: deze werkgroep richt zicht op de langere termijn visie voor het veld en hoe deze kan worden beïnvloed middels het richting geven aan nieuwe landelijke onderzoeksprogramma's .

Themabijeenkomst Forensic Intelligence op 9 december

Op 9 december organiseerde FINE samen met het PvIB een themabijeenkomst over Forensic Intelligence. Op deze avond toonden Hans Henseler, Marcel Worring en Wim Tip wat FINE in hun respectievelijke vak inhoudt. Na een korte inleiding over FINE nam Hans in de wereld van E-Discovery en de slimme analyse van digitaal bewijs. Marcel liet ons zien hoe Multimedia Analyse synergie creëert tussen expert en algoritme die nodig is om uit bergen beeldmateriaal bewijzen boven tafel te halen. Wim sloot af met een kijkje in de keuken van Real-time Fraude detectie bij ING.

Voor meer informatie bezoek de website www.finenet.nl of neem contact op via info@finenet.nl.

ARTIKELEN SCHRIJVEN IN DIT MAGAZINE

De redactie is op zoek naar meer artikelen voor dit magazine. Artikelen over een actueel onderwerp of een inhoudelijk rapport. Artikelen mogen gericht zijn op een breed publiek, maar mogen ook gericht zijn op een expertise binnen informatiebeveiliging.

Uit de recente ledenenquête kwam naar boven dat leden interesse hebben in de volgende onderwerpen. Hier willen we graag artikelen over publiceren:

- **Privacy wetgeving en risicomanagement**
- **Identity & Access Management in relatie met de cloud**
- **Supply chain informatiebeveiliging en hoe om te gaan met leveranciers en outsourcende partijen**
- **Malware in allerlei vormen (gegevensdragers, software)**
- **Internet of things**
- **Samensmelting tussen kantoorautomatisering en procesautomatisering**
- **Forensisch onderzoek in de cloud**
- **De nieuwe ISO norm en inrichten ISMS hiervoor**
- **Governance van informatiebeveiliging**
- **Security Architectuur**

Auteurs gezocht

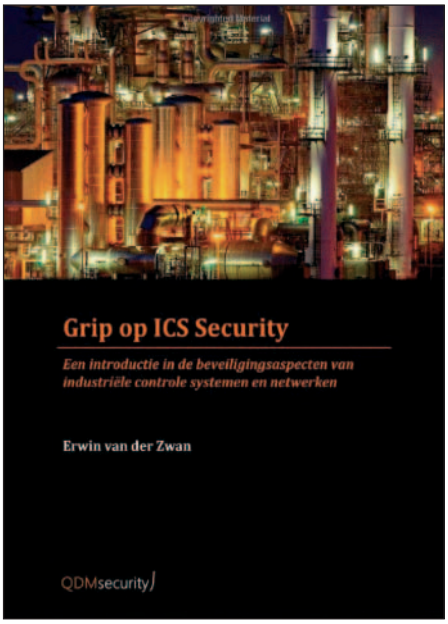
De redactie is altijd op zoek naar nieuwe denkbeelden in het vakgebied. En ze zijn er van overtuigd dat die volop aanwezig zijn. Het is verder nuttig om auteurs er op te wijzen dat het schrijven van een artikel wellicht de meest eenvoudige manier is om CPE-punten te vergaren voor het bijhouden van professionele certificaties zoals CISSP en CISA. Het bewijs is eenvoudig te leveren in de vorm van een tastbare publicatie. Hiernaast kun je de wetenschap plaatsen dat je een bijdrage levert aan kennisdeling met en voor professionals, op het gebied van informatiebeveiliging, maar vaak ook breder. De redactie snapt dat je niet zomaar een artikel in elkaar zet. Dit is een proces, en nota bene een proces waar consultants niet per se goed in zijn. Het is heel anders om een rapport te schrijven voor een opdrachtgever of een artikel voor een professioneel publiek. Dat is dan ook de reden dat er altijd een begeleidend redacteur meeleest met jouw artikel en indien nodig adviezen geeft. En heb je eenmaal een artikel geschreven, dan ding je ook nog eens mee naar één van de prijzen voor 'Artikel van het jaar'. Een onafhankelijke jury beoordeelt de winnaar uit een shortlist, samengesteld door de redactie.

Auteursinstructies

Voor een auteur is het prettig om te weten wat de redactie verwacht wanneer een artikel aangeleverd wordt. Het is voor de auteur eenvoudiger om naar toe te werken en voor de redacteur efficie?nter in de begeleiding en beoordeling van het artikel. De auteursinstructies [1] beginnen met een uitleg welk soort artikelen in het magazine worden gepubliceerd en wat het publicatieproces is na ontvangst door de redactie. In de ervaring van de redactie zijn vooral de instructies met betrekking tot opmaak van de tekst en illustraties/tabellen heel nuttig, met name het gegeven dat afbeeldingsmateriaal voor drukwerk veel meer resolutie moet hebben dan webpublicaties. Als je als auteur een bijdrage zou willen leveren aan het magazine, neem contact op met de redactie (ibmagazine@pvib.nl). Wij helpen je graag verder.

Links

[1] Auteursinstructies: https://www.pvib.nl/auteursinstructies



Productdetails
Titel: Grip op ICS Security
Auteur: Erwin van der Zwan
ISBN: 9789082024500
Rechtstreeks te bestellen bij Lulu.com

"GRIP OP ICS SECURITY"
van Erwin van der Zwan

De naam van de auteur van dit boek zal bij veel mensen bekend zijn, temeer daar hij een paar jaar geleden bij de 'Artikel van het jaar' verkiezing van dit blad de prijs mee naar huis nam. Dat Erwin kan schrijven weten we dus wel en dat hij verstand heeft van informatiebeveiliging is ook wel duidelijk.
Sinds een aantal jaar houdt Erwin zich bezig met een vakgebied dat tegenwoordig veel aandacht krijgt, maar waarvan weinig mensen echt op de hoogte zijn: het door hackers op afstand bedienen van sluizen en verwarmingsinstallaties van gymzalen. Dit soort hacks heeft de pers wel een paar keer gehaald. Maar hoe we om moeten gaan met ICS- (Industrial Control Systems) en SCADA-systemen is een ander verhaal.

Het boek "Grip op ICS Security" heeft volgens de achterflap als doelgroep personen die werkzaam zijn in industriële bedrijven en bedrijven in de vitale infrastructuren. Maar dat mag voor mij eigenlijk wel iets worden opgerekt naar security professionals in het algemeen. Ik heb door het lezen van dit boek wel nieuwe dingen geleerd die mij helpen om de grote cyberdreigingen beter te kunnen analyseren (lees relativeren...). Maar de groep security professionals hoeft volgens mij dan niet het hele boek te lezen. De laatste twee grote hoofdstukken gaan namelijk over risicomanagement en informatiebeveiliging. Die beide onderwerpen kunnen PvIB leden eigenlijk wel overslaan.
Maar de eerdere hoofdstukken kunnen ook ons genoeg nieuws leren over ICS en SCADA. Daar moet je wel wat voor doen, want, zoals Erwin aangeeft, het is een introductie in dat vakgebied. En misschien is dat meteen ook het grootste zwakke punt van dit boek. Als je kijkt naar de grote hoeveelheid opsommingen en bullets, dan begrijp je dat het uitwerken daarvan een aanzienlijke uitbreiding van de stof met zich mee had gebracht. En een tweede bezwaar voor security professionals die niet werkzaam zijn bij de doelgroep, is dat er heel veel afkortingen worden gebruikt die pas wat later worden uitgelegd en toegelicht. Gelukkig worden de relevante begrippen duidelijk uitgewerkt en leidt dat tot de behoefte aan meer verdieping, maar het leest even wat lastig.

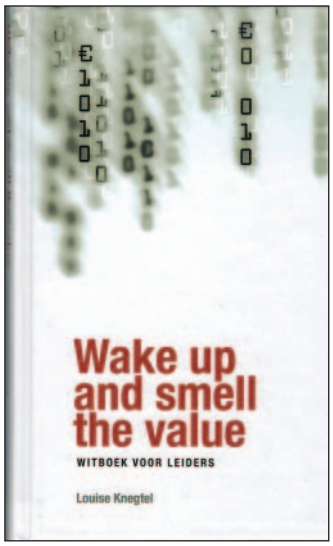
Het boek geeft de samenstelling van ICS-systemen duidelijk weer. De componenten, van veldapparatuur tot de Human Machine Interface, krijgen een plek. De bedreigingen en kwetsbaarheden met betrekking tot ICS/SCADA-systemen worden op basis van het MAPGOOD-model (Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten) stuk voor stuk toegelicht. Een groot aantal bekende, maar ook onbekende, security incidenten wordt met voorbeelden uitgelegd. Vervolgens wordt de bijbehorende security architectuur uitgewerkt, maar dit hoofdstuk is voor IB-professionals niet het meest spannende. De ons bekende begrippen als firewall, SIEM, security awareness, worden wel geprojecteerd op het ICS-model.

In het Nederlandse taalgebied was er nog niet eerder zo'n uitvoerige beschrijving van ICS/SCADA security en die leidt eigenlijk tot de wens van meer verdieping. Ik heb nu wel behoefte aan een bredere uiteenzetting van het ISA99-model (waarin de standaard ICS-architectuur is beschreven) en een verdere uitwerking van het onderliggende security model.

Het boek is in eigen beheer verschenen bij lulu.com en sinds de eerste uitgave in 2012 zijn we inmiddels bij de 4e druk aanbeland (al gaat deze recensie uit van de 2e druk). Er is een uitgebreide woordenlijst als bijlage bijgevoegd, evenals een overzicht van de van toepassing zijnde normen en standaarden.

Per saldo: het boek "Grip op ICS Security" is een waardevolle introductie van een relatief onbekend vakgebied en zou alleen daarom al als naslagwerk in een aantal boekenkasten een plek moeten hebben. Maar het roept eigenlijk ook om een vervolg dat op verschillende aspecten de diepte ingaat. Dat lijkt me een mooie uitdaging voor Erwin.

André Koot. André is consultant bij Strict BV en redacteur van dit blad. Hij is bereikbaar via a.koot@strict.nl



Boek: Wake up and smell the value - Witboek voor leiders
Gebonden, 115 pagina's
Auteur: Louise Knegtel
Uitgever: BtoB Booksellers, Nunspeet
ISBN: 978-94-91453-01-4
Prijs: €18,95
Beoordeling: ★★★✪✪

"WAKE UP AND SMELL THE VALUE"

van Louise Knegtel

Je komt in de informatiebeveiliging niet vaak een compact, gemakkelijk te lezen boek tegen. Dit is juist wat "Wake up and smell the value" is, gericht op de manager die zich afvraagt waarom hij geld en aandacht moet besteden aan beveiliging - of dit zou moeten besteden. In dit verband is het boekje vergelijkbaar met klassieke werken als "The One Minute Manager" en "Who Moved My Cheese?", maar dan voor informatiebeveiliging. Het boek is een mooie verschijning: netjes gebonden, gezet in een moderne letter, met regelmatig een pagina met een wijze spreuk of praktisch verhaal ter illustratie.
De eerste vier hoofdstukken zetten uiteen dat informatie waarde heeft, wie belang heeft bij de vaststelling van die waarde en uiteindelijk waar dan de bedrijfswaarde zit. Dit deel vertelt prachtig hoe je waarde kunt vinden, helemaal los van de automatisering. Het beschrijft methodes die aansluiten bij de belevingswereld van managers en die ze eenvoudig kunnen toepassen. Het doet me denken aan het werken met business attributen, zoals SABSA dat doet om waarde vast te stellen. Waarde wordt niet uitgedrukt in termen van vertrouwelijkheid, integriteit en beschikbaarheid, maar in business-termen. Louise schrijft ze op als vragen, bijvoorbeeld: "Intellectueel eigendom: Vormt unieke (eventueel gepatenteerde) kennis onderdeel van jouw product of dienst?" De volgende drie hoofdstukken belichten de zaak vanuit de bedreiging van die waarde. Louise beschrijft de algemeen bekende bedreigingen: computercriminaliteit, software, USB-sticks, saboterende medewerkers, enz. Dit deel schiet in mijn ogen te kort, omdat het gebaseerd is op FUD-denken.
FUD (fear, uncertainty and doubt) is old-school, het werkt niet optimaal in de wereld van vandaag om goede management aandacht te krijgen. We nemen inderdaad maatregelen om ons te beschermen tegen kwetsbaarheden, maar we nemen ook maatregelen om veilig nieuwe activiteiten te ontplooien. Waarde krijgt daarmee nieuwe kansen en de effectieve maatregelen tegen bedreigingen kunnen directer gekozen worden.

Het mooi opgebouwde verhaal over de waarde van informatie verliest hierdoor aan kracht, die juist in het eerste deel zo goed opgebouwd was. Het boekje sluit met een woordenlijst en een lijst van maatregelen. De maatregelen worden als uitputtende lijst gepresenteerd, wat maakt dat de manager niet meer creatief zal nadenken over mogelijke alternatieve maatregelen. Een sterk begin dus, met een zwakker slot. Het resultaat blijft een boekje dat ik best cadeau durf te doen aan een manager.

Lex Borger. Lex is consultant bij i-to-i en hoofdredacteur van dit blad. Hij is bereikbaar via l.borger@i-to-i.nl

JUSTIFIED

Sometimes when applying SABSA Business Attributes to a business scenario we need to consider some deeply philosophical and moral issues. This time we shall examine the attribute 'justified' in the context of what sort of security surveillance should we allow our governments to carry out and how does this conflict with the right of citizens to personal privacy.

Recently on 3rd November 2014 Richard Hannigan took over as the new Director of the Government Communications Headquarters in the UK (GCHQ). Next day he published an Opinion Piece in the Financial Times [1].

The main thrust of this opinion piece is that new terrorist organisations (such as ISIS) are attracting young idealistic converts who have never experienced life without the internet and hence they have a level of internet savvy-ness never before available to terrorist groups. These people are on their home ground in cyberspace. They are 'digital natives' whereas most of the people in government office and the security services (and most citizens) are 'digital immigrants' [2].

Mr Hannigan tells us that governments have little chance of success in fighting against terrorism and organised crime unless we as citizens are willing to sacrifice personal privacy. He also complains that the Western technology companies who largely control the use of the internet are not cooperating enough with Western governments by not providing the kind of surveillance that the government security agencies would find most helpful. He continues:

"To those of us who have to tackle the depressing end of human behaviour on the internet, it can seem that some technology companies are in denial about its misuse. I suspect most ordinary users of the internet are ahead of them: they have strong views on the ethics of companies, whether on taxation, child protection or privacy; they do not want the media platforms they use with their friends and families to facilitate murder or child abuse."

Good point, but it does beg several questions: What is misuse? What defines an 'ordinary user'? Should a Western technology company have loyalty only to its customers in Western democracies or to its wider international customer base? Where should the line be drawn between governments entitled to ask for surveillance and those not so entitled? Every nation or group claiming nation status (such as ISIS) will argue that their cause is 'justified' because they have 'God on their side' – but whose God and which 'side' should an international technology company serve? Is a technology company (such as Google) even 'justified' in taking sides or should it remain apolitical and amoral?

Mr Hannigan says: "As we celebrate the 25th anniversary of the spectacular creation that is the world wide web, we need a new deal between democratic governments and the technology companies in the area of protecting our citizens. It should be a deal rooted in the democratic values we share. That means addressing some uncomfortable truths."

However, there are good historical reasons for citizens to have only conditional trust in their own governments, and because of this, good law-abiding citizens feel entitled to some personal privacy, including privacy from government surveillance of their online activities. Not all Western governments have always been benign, or indeed democratic. Who can predict the future?

So can SABSA thinking help with making these "urgent and difficult decisions"? Increasingly the challenge laid down by Mr Hannigan will become more relevant to all commercial enterprises that leverage digital technology to enable their businesses. They all will need to consider these issues and decide at what level security surveillance and cooperation with government agencies is 'justified'. This type of ethical debate is necessary for society to agree on how it will make use of digital technologies in the future and what actions are 'justified'. As always, SABSA does not attempt to provide prescriptive answers, but ensures that all the important questions are properly addressed and that the decisions made are rational, traceable and fair, and indeed, 'justified'.

The Attributer

Links

[1] Director GCHQ writes an opinion piece for the Financial Times: http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/Director-opinion-piece-financial-times.aspx

[2] Digital Natives, Digital Immigrants: http://www.marcprensky.com/writing/Prensky - Digital Natives, Digital Immigrants - Part1.pdf

Verantwoorde onthullingen #11

BEG EN DE BUG BOUNTY

Laatst was ik bij een bijeenkomst over de toekomst van het cybersecurity onderwijs. Een hoogleraar begon met de bekende klaagzang: te weinig studenten, leraren te oud en verkokering van academische specialismen. De oplossing: meer samenwerking met bedrijven, multidisciplinair en iets leuks met jongeren. Daar zullen we het allemaal wel mee eens zijn. Maar wat te doen met briljante jonge hackers, die op de een of andere manier het vwo zijn misgelopen en de sector zeker veel te bieden hebben? Is er een soort zij-instroom programma?

Nee, dergelijke moeilijke materie moet je wel op niveau behandelen volgens de hoogleraar. Liefst universitair. Aan het hbo wordt gewerkt, maar dat loopt nog wat moeilijk. Een van de weinige hackers in het gezelschap riep enthousiast: doe iets met hackerspaces, daar ligt zoveel kennis en dat vinden jongeren leuk! Iedereen keek haar glazig aan: "Hackerspaces, waar zijn die dan?" Zucht. Lieve mensen: H4ck3rs z13N d3 d1ng3N v44k g3w00N N3t 13ts 4Nd3rs d4N 4Nd3r3N. Moeite met deze zin? Lees dan vooral even door, want dit is vooral belangrijk voor gewone security specialisten als jij.

In mijn onderzoek naar ethisch hackers komt ik vaak dit levensverhaal tegen: slechte cijfers ondanks uitzonderlijke intelligentie, dan maar naar het vmbo, misschien nog een mbo-certificaat of een cursusje erachteraan, gevolgd door een stage. Dan ineens gebeurt het: bingo, ze zijn de bink want het blijkt dat niemand computers zo goed begrijpen zoals zij. OK, er zitten jongens bij met ADHD of Asperger. Vooral dyslexie komt vaak voor. Maar eigenlijk zijn dit vooral labels vanuit een maatschappij die niet weet wat ze aan moet met mensen die anders denken en hen daarom maar pathologiseert. Volgens mij hebben ze niet iets tekort, ze hebben juist iets extra's en dat komt pas op latere leeftijd echt goed aan het licht.

Hier een voorbeeld: @smiegles, ook wel Olivier Beg. Hij is net 18 jaar geworden en nummer 1 in de Hall of Fame van Yahoo. School ging niet makkelijk vanwege zijn dyslexie en hij vond de lesstof verre van interessant. Dus werd hij naar het vmbo gestuurd. Daar ging hij tijdens de les zitten hacken, vooral uit verveling en omdat de school een snelle internetverbinding had. Als hij beveiligingsproblemen in het schoolnetwerk ontdekte, meldde hij dat netjes. Verder zei niemand er wat van als hij tijdens de les op zijn laptop werkte. Ook zijn ouders begrepen niet echt wat hij deed, maar lieten hem zijn gang gaan.

Tijdens ons gesprek kom ik erachter dat hij een van de melders was tijdens Lektober, de maand oktober 2011 waarin Webwereld elke dag een lek meldde. Ik zal niet zeggen welk lek, want hij bleef toen,

Chris van 't Hof
Voor meer verantwoorde onthullingen.
www.cvth.nl/vo

net als de meeste melders, liever anoniem. Wel weet hij me vertellen dat het CMS van Webwereld zelf niet helemaal veilig was. Hij ontdekte namelijk dat hij via Cross-Site Request Forgery het account van de journalist kon overnemen. Het zou best grappig zijn geweest als hij dan namens die journalist een artikel op de site had gezet, maar hij was volwassen genoeg om dat niet te doen. Hij was toen dus nog maar 14 jaar.

In de jaren daarna treedt Olivier steeds meer naar buiten met zijn meldingen en dat zijn er heel wat. Zo'n beetje alle grote Nederlandse banken: ABN Amro, ING, SNS, RABO, ASN, Regiobank, Van Lanschot bank. Meestal kreeg hij wat VVV bonnen en een spreekverbod. Bij de Telco's had hij ook veel onthullingen. UPC, Ziggo en KPN namen zijn meldingen netjes in ontvangst, zonder beloningen te geven. Bij XS4all kreeg hij nog wel een appeltaart. Zijn melding bij T-Mobile is nog echter nog steeds onbeantwoord.

Hij ontdekte ook kwetsbaarheden bij de Nederlandse overheid, bijvoorbeeld op de site van de Belastingdienst. Daar bleek een oude Adobe Flash Player te draaien waar je een XSS zou kunnen doen. Deze videoapplicatie werd bovendien gebruikt bij verschillende andere overheidssites, waaronder ook het NCSC. Hij meldde het daarom bij het centrum. Het was zondagavond 22.50, kreeg een reactie om 23.10 en zag dat het om 23.30 gefixed was. Ook bij de Belastingdienst. Opmerkelijk, want zo'n vlotte reactie verwacht je niet van de overheid. Als dank kreeg Beg een beker van de Belastingdienst, met de tekst: "I hacked the state government and never got a refund." En natuurlijk een T-shirt van het NCSC, waarvan hij er inmiddels acht heeft.

Vergeleken met de Lektober periode is er veel veranderd. Bij zowel de overheid als het bedrijfsleven is er nu beleid om verantwoorde onthullingen op een goede manier af te handelen. Sommigen reiken zelfs beloningen uit, maar dan niet te scheutig, want we zijn natuurlijk wel Hollanders. Hoe anders verging het dit jonge talent bij Yahoo. Ook daar kon hij een XSS doen en het netjes melden. Tot zijn verbazing hier geen VVV bon, T-shirt of beker, maar gewoon keiharde cash: $ 1000,- per melding. Hij deed er zeventien, dus tel uit je winst. Het Parool kopt begin dit jaar trots: "17-jarige Amsterdammer voert hackerslijsten aan". En inderdaad, bij Yahoo staat hij op 1. Maar we treffen hem ook aan in de Hall of Fame van Google, Microsoft, Nokia, Apple, Adobe, AT&T, eBay…

Als ik hem vraag of hij liever gaat voor de bounty's of zich ook nog wel wil inzetten voor het Hollandse vrijwilligerswerk, zegt hij me dat het hem eigenlijk niet zoveel uitmaakt. Hij doet het vooral voor de erkenning. Hij wil de puzzel oplossen en aan anderen laten zien. Momenteel heeft hij overigens niet meer zoveel tijd voor ethisch hacken, want hij doet al de hele dag aan informatiebeveiliging op zijn stage. Nog een paar maanden en dan is hij klaar met het mbo. Wat gaat hij dan doen? Liefst een reisje door de VS om wat hackerscongressen te bezoeken. Daarna ziet hij wel verder. Hopelijk komt hij wel weer terug.

Mijn vraag aan jullie is dus: hoe houden we jongens als Olivier in Nederland? Aangepast onderwijs, een hackers gilde, bigger bounty's… Laten we beginnen met wat meer waardering voor hun werk. Bij dezen.

VERLEIDINGEN GENOEG...

VOORKOM DAT UW MEDEWERKERS TOEHAPPEN

FOX-IT verzorgt security awareness-campagnes om de weerbaarheid en het bewustzijn van uw medewerkers te vergroten. Voor meer informatie: bel Rombert Anjema op 015 2847 999 of mail naar academy@fox-it.com.

FOX IT

FOX-IT.COM

DE NIEUWE MALWARE AANPAK

De leveranciers van antivirus producten zeggen het al zelf: Het scannen naar malware op systemen is niet langer effectief. Dit komt doordat malware nu zoveel dynamisch gedrag bezit, dat het gevuld houden van een scandatabase niet meer te doen is. De scanners beperken zich al tot een scan naar actieve malware, in plaats van een totale scan. De antivirus scanner werkt technisch goed, maar is praktisch bijna failliet [1] & [2].

We hebben wel bescherming nodig tegen malware. Hoe kunnen we dat dan doen? We moeten onze IT-hygiene bijhouden. Wat houdt dit in? Zeker toch wel het volgende:

- **Systemen veilig configureren**
- **Systemen alleen aanpassen onder change management**
- **Een firewall gebruiken**
- **De uitgegeven autorisaties in de toegangsbeveiliging beperken**
- **Patches bijhouden**

In gestructureerde omgevingen is het mogelijk om de scan om te draaien. Voer white-list scanning uit in plaats van black-list scanning: identificeer dat alle geinstalleerde software ook op het systeem thuis hoort. Toch is dit lasting, want het bedrijf moet zélf bepalen waar op gescand wordt, niet de AV leverancier.

Niet scannen maar detecteren

Pak profijt van een tweede beveiligingslaag: het detecteren van malware wanneer het in actie komt. De allereerste antivirusproducten werkten ook zo. Ik kan me nog herinneren dat Norton je waarschuwde dat er naar de bootsector van de harde schijf werd geschreven. Jij moest dan zelf bepalen of dat correct was. Vandaag de dag kun je de opvolging van een detectie echt niet overlaten aan een eindgebruiker, maar heb je een speciale onderzoekers nodig. Bij grote bedrijven leg je dit neer bij een CERT (computer emergency response team) of een SOC (security operations centre).

De detectie zelf moet automatisch gaan. En er zijn goede manieren om de activiteiten van malware te ontdekken: Systeem- en netwerkconfiguraties kunnen gescand te worden op ongeautoriseerde aanpassingen. Allerlei logs kunnen gescand worden op verdachte activiteit. Je kunt een intrusion detection systeem (IDS) of een security information and event management (SIEM) systeem inzetten.

Al deze systemen volwassen producten in de markt. Je komt een heel eind met de inzet van zulke systemen, gecombineerd met de juiste mensen. Er is echter één type aanval die hiermee nog steeds moeilijk te detecteren is. Dit is de advanced persistent threat (APT), een aanval waarbij de aanvaller onder de radar probeert te blijven. Hierbij wordt op maat gemaakte malware gecombineerd met specifieke aansturing door hackers om een voet binnen de deur te krijgen zonder opgemerkt te worden. Zo zijn de spraakmakende cyberkraken gezet in het afgelopen jaar, zoals de inbraken bij Amerikaanse winkelketens Target en Home Depot. En bij het ter perse gaan van dit nummer bereikte ons het bericht dat er een ultiem APT-malware product is ontdekt, Regin [3]. Dit gaat vast nog een staartje krijgen.

APT aanpakken

Hoe detecteer je een APT aanval? Er is een dataverzameling in het netwerk die voor deze detectie gebruikt zou kunnen worden: de flowdata. De flowdata wordt gebruikt door een netwerkbeheerder om de netwerkcapaciteit te beheren. Als bekend is wat normaal netwerkgedrag is, zijn de afwijkingen, veroorzaakt door een APT aanval, eenvoudig waar te nemen. En omdat flowdata structureel opgeslagen kan worden, is het ook mogelijk om in het verleden terug te kijken, zodat je een aanval kunt analyseren, zeker wanneer je deze informatie combineert met big data over actuele cyberaanvallen. Zo krijgen we, bij het wegvallen van antivirus scanners, een nieuw segment in de markt dat verder gaat en de APTs effectief zal kunnen aanpakken.

Links:

[1] http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html

[2] http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/

[3] http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance

Lex Borger. Lex is consultant bij i-to-i en hoofdredacteur van dit blad. Hij is bereikbaar via l.borger@i-to-i.nl

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

TERUGBLIKKEN EN VOORUIT KIJKEN

Aan het eind van het jaar is het een goed moment om terug te kijken en vooruit te kijken. De redactie reageert op de vragen: Wat was een opvallende ontwikkeling (qua bedreiging of maatregel) in 2014? En wat gaat 2015 ons brengen op dat gebied?


Lex Borger


Tom Bakker


Maarten Hartsuijker


André Koot

Maarten Hartsuijker

Vooruitkijken is altijd lastiger dan terugkijken. En in de IT-industrie lijkt een jaar soms wel een eeuwigheid. Wie had eind 2013 kunnen vermoeden dat in 2014 de ene aan SSL gerelateerde kwetsbaarheid over de andere heen zou rollen? Ik vraag mij voor 2015 af hoe ons vertrouwen in de cloud zich gaat ontwikkelen. Er staat een nieuwe Europese privacy wet in de stijgers, Safe Harbor blijkt een wassen neus en de Amerikaanse tech-bedrijven ageren (of doen tenminste alsof) tegen de wijze waarop de inlichtingendiensten hun businessmodel verstoren. Tegelijk zien we die diensten reageren op een wereld die aan het verharden is. Al leven we, als we 2014 met de voorgaande eeuwen vergelijken, niet in de slechtste tijd (enig positief perspectief kan geen kwaad). Ik zie zelf voor 2015 veel kansen in de verbetering van encryptie en zero-knowledge technologie. Maar gaat deze techniek onze gegevens beschermen en privacy redden? Of gaat het sneuvelen door in wetten gesmeden backdoor-verplichtingen? Vooruitkijken blijft afwachten. Vergeet niet om eerst nog even van 2014 te genieten.

Lex Borger

Cryptolocker is weliswaar voor het eerst waargenomen in September 2013, maar in 2014 zette het flink door. Malware die cryptografie goed toepast, een losgeld vraagt in Bitcoin en ook daadwerkelijk de versleutelde bestanden weer vrijgeeft na betaling. Met zelfs een servicedesk, mocht je hulp nodig hebben bij het ontsleutelen. De opbrengst? Minstens tientallen miljoenen euro. De ultieme business case voor computercriminaliteit. Het probleem voor de samenleving is groot. Menig particulier en MKB-er heeft zijn back ups niet genoeg op orde en kiezen om losgeld te betalen. Ook bedrijven en overheidsinstanties hebben er last van. Fox-IT en FireEye vinden een gat in de crypto en stellen gratis een ontcijferprogramma beschikbaar. Cryptolocker was in 2014 een game-changer.
De game-changer voor 2015 zou wel eens een nieuwe productcategorie kunnen zijn: de anti-APT scanner. De afgelopen jaren zijn er met regelmaat spraakmakende hacks geweest van grote bedrijven, waarbij ook veel gegevens buitgemaakt werden. Al deze hacks werden uitgevoerd onder de radar van de gevestigde scanners: antivirus, IDS en SIEM. Ik denk dat we een nieuw soort scan-product op de markt gaan zien, die de activiteiten van een APT in uitvoering wél betrouwbaar zullen detecteren. De beveiligingswereld heeft het nodig.

André Koot

Het kan niet anders dan dat mijn terugblik op dit jaar gaat over de ophef die is ontstaan over de kwetsbaarheden in open source software die op zeer grote schaal gebruikt wordt. We hebben het er in de afgelopen nummers regelmatig over gehad, er is ook flink over gediscussieerd, dus het was ook echt wel een dingetje. En apart is eigenlijk wat je daarbij moet constateren: steeds weer worden we verrast door kwetsbaarheden en lekken in componenten die we eigenlijk altijd vertrouwd hebben. Doet me een beetje denken aan de aloude Diginotar case, ook iets waar we niet bij stilstonden dat er iets fout zou kunnen zijn, we namen altijd maar gewoon aan dat het oké was. Net als bij OpenSSL en die andere dingen. We blijven wat argeloos als het aankomt op security.

Vooruitkijkend blader ik even terug naar nummer 1 van dit jaar. Ik gaf aan dat 2014 het jaar van PGP zou gaan worden. Dat lijkt nog iets te optimistisch. Ik denk dat we volgend jaar meer en meer cryptografische toepassingen gebruikt zullen zien worden. PGP natuurlijk, maar ook Tor zal op grotere schaal gebruikt gaan worden. De doe-het-zelf privacybescherming gaat echt wel groeien. Op corporate niveau zal outsourcing van de security processen op nog grotere schaal gaan gebeuren. Dat is natuurlijk niet echt een voorspelling, eerder een trend. Die zie ik op steeds grotere schaal ook op het gebied van identiteitenbeheer plaatsvinden. Identity as a Service zal in elk IAM project een reguliere optie worden.

Tom Bakker

Als ik terugblik naar het afgelopen jaar dan vond ik het meest opvallend de OpenSSL-lekken die vlak na elkaar ontdekt werden en daar al jaren ongemerkt zaten. En vooral ook de discussies die daar op volgden; ook in dit blad. Hoe veilig is Open Source eigenlijk? Die discussie ga ik hier niet voeren. Wat vooral opviel en juist tegenviel was de lauwe reactie van gebruikers en bedrijven. Private keys, wachtwoorden, bankgegevens zouden allemaal gelekt kunnen zijn door met name Heartbleed. Certificate Service Providers zouden overspoeld worden met verzoeken om SSL-certificaten te vernieuwen. Niets van dat alles. Men ging er blijkbaar van uit dat de kans klein was dat er gelekt is. De kans was inderdaad klein maar toch... Zekerheid eerst!
Niet nieuw, maar heel vervelend voor betrokkenen en schrikbarend toenemend, is identiteitsdiefstal en -fraude. Als je dat overkomt, is dat een nachtmerrie. Het is heel moeilijk om je onschuld te bewijzen. Volgens mij komt het ook door het grenzeloos vertrouwen in onze informatiesystemen. Wat in het systeem staat is altijd de waarheid! Doet me denken aan de succesvolle serie 'Little Britain' waar op elke vraag 'the computer says no' als antwoord komt en dat als definitief en altijd waar beschouwd wordt. Men vergeet dat die alwetende computer wel gevoed is met (foute) informatie ingebracht door 'domme' mensen. Denk maar laatst aan de man die een tijd ten onrechte in de gevangenis heeft gezeten, omdat men zijn DNA verwisseld heeft met die van een ander. Uiteindelijk toch weer een menselijke fout. Ik ben bang dat de kans op menselijke fouten in 2015 niet zal veranderen. Met alle gevolgen van dien.

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)
Ronald van Erven (Timeos Pensioendiensten)
Maarten Hartsuijker (Classity)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)
Martijn Veken (SNS REAAL)

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

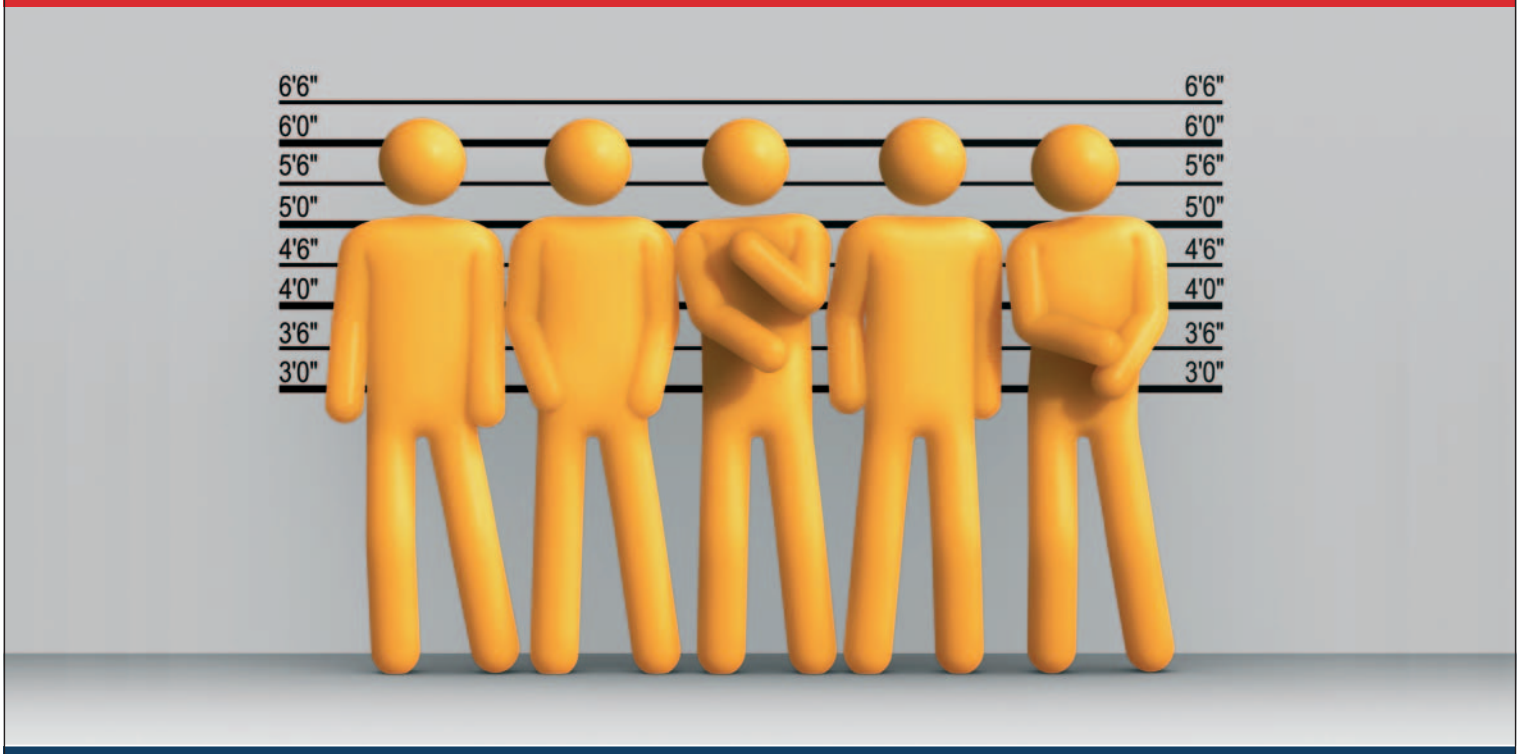
VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

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 2014
De abonnementsprijs in 2014 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



WIE IS U?

Er zijn al vele initiatieven geweest die moeten voorkomen dat ik mij uitgeef voor iemand anders of dat iemand anders als "Berry" door het leven gaat. Een probleem dat de laatste jaren sterk in opkomst is en steeds populairder wordt, is de zogenaamde identiteitsfraude. Als je vroeger een bankrekening wilde openen dan zocht je een bank uit (in mijn jeugd had je nog een uitgebreide keus), zocht je het dichtstbijzijnde gebouw op (vroeger hadden banken gebouwen) en ging je gewapend met paspoort of rijbewijs naar het betreffende gebouw. De mevrouw achter de balie keek je eens diep in de ogen en vergeleek die met rijbewijs of paspoort. Er worden wat nummers van het document over genomen en je loopt weg met een banknummer en zit de rest van je leven bij die bank.
Dat is allemaal wel een beetje veranderd door de komst van internet, tegenwoordig kom je al een heel eind als je een inlognaam weet en een wachtwoord. Nu zijn de meeste wachtwoorden geheim, maar als een website een beetje lek is en jouw wachtwoord heeft gelekt dan is de kans heel groot dat je daarmee toegang hebt tot veel meer sites die je slachtoffer gebruikt. Wachtwoorden worden namelijk heel veel hergebruikt of zijn erg eenvoudig te raden: "123456" is het meest gebruikt, "12345678" is de moeilijke variant. Nee, dat stelt allemaal niet veel voor, vreemd dat DiGiD deze combinatie ook veelal goed vindt, want daarmee kun je op de meeste Nederlandse (semi) overheidssites wel terecht. Sommige instanties vinden de combinatie te beperkt en willen ook een SMS authenticatie, best noodzakelijk, maar dat kost wel 10 eurocent per sms. Tja, dan misschien toch maar niet?
In Nederland zijn veel zaken goed georganiseerd met betrekking tot de uitgifte van officiële documenten, het doorvoeren van naamsveranderingen of allerlei mutaties die van invloed kunnen zijn op het bepalen van een identiteit. In andere landen (zelfs die van de Europese unie) is het allemaal iets eenvoudiger, bij het overleggen van een paar euro ga je als meneer de Vries naar binnen en kom je als meneer Pieters naar buiten, inclusief paspoort en dergelijke. Met hetzelfde gemak kom je als meneer de Vries binnen en ga je als mevrouw de Vries naar buiten, vervolgens reis je naar Nederland en sta je in de rij voor dezelfde toelage die meneer de Vries sinds de vorige week al krijgt. Naar behoefte is dit te herhalen en te herhalen en te herhalen… Overdreven? Nee hoor, google maar eens op toeslagenfraude. Bij nader inzien zou ik dat maar niet doen, heel blij word je er niet van.
Zoals ik eerder ook wel heb aangegeven, we zullen nooit meer terug gaan in de tijd, de bankgebouwen blijven leeg en identiteitsfraude blijft bestaan en zal alleen maar toenemen als er niet snel een dichte en robuuste internationaal erkende werkwijze komt om een identiteit te registreren en te authenticeren. Met de daadkrachtige Europese unie gaat dat vast wel lukken.

Berry

The Internet of Things

Informatiestromen worden steeds complexer. Hoe houdt u dit onder controle? Is uw data nog secure?

Waar zitten uw risico's in het ICT-landschap? Adequate beveiliging door een ervaren, betrouwbare en loyale partner is meer dan ooit noodzaak.

CRYPSYS is ruim 25 jaar toonaangevend op het gebied van IT security.

CRYPSYS secure computing

CRYPSYS secure computing 25 years

CRYPSYS Data Security BV Edisonweg 4 4207 HG Gorinchem **tel** +31 (0)183 62 44 44 **fax** +31 (0)183 62 28 48 **mail** sales@crypsys.nl **web** www.crypsys.nl

CRYPSYS is officieel distributeur van: Sophos, SMS Passcode, Norman, Tenable en Cyberoam.