05/2011

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 5- 2011

IEDEREEN EEN SUPERCOMPUTER

DIGITALE TOEGANG VIA TRUSTED THIRD PARTY

PROFESSIONALS ZIJN ONMISBAAR IN ICT-OPLEIDING

DATA QUALITY WITH SOLVENCY II

TAGOLOGY, ÉÉN TAAL VOOR ALLES

FOX-IT

... for a more secure society

Fighting cybercrime

Protecting secrets

Finding digital evidence

Innovating internet interception

Voorkom illegaal meeluisteren van GSM gesprekken

GSM security is hot! Dit werd extra benadrukt toen de Voicemail berichten van Ministers gemakkelijk werden afgeluisterd en GSM gekraakt werd door hackers. De risico's van het afluisteren van versleuteld gsm-verkeer nemen toe. Met SecuVOICE biedt Fox- IT een unieke oplossing om illegaal meeluisteren te voorkomen. SecuVOICE werkt op basis van de Secusmart Security Card, een MicroSD-smartcard, die gesprekken tussen twee mobiele telefoons end-to-end versleutelt. Gesprekken zijn door deze versleuteling niet door derden af te luisteren en de afzender is niet te vervalsen.

AIVD goedkeuring Departementaal Vertrouwelijk

Fox-IT biedt met het product SecuVOICE een oplossing op de Nederlandse markt met een goedkeuring tot niveau Departementaal Vertrouwelijk voor beveiligd bellen via het GSM-kanaal. Deze goedkeuring is verstrekt op advies van het Nationaal Bureau voor Verbindingsbeveiliging (NBV), onderdeel van de AIVD. Deze goedkeuring bevestigt dat SecuVOICE voldoet aan de overheidsnormen voor beveiligd bellen,

Meer weten? Bel of mail met Ronald Westerlaken, Product manager via 015 -284 79 99 of westerlaken@fox-it.com

Fox-IT Olof Palmestraat 6 Delft 015 - 284 79 99 www.fox-it.com

VOORWOORD

De risicoanalyse… Iedere beveiliger heeft er wel mee te maken, in wat voor een vorm dan ook. En er zijn vele vormen, tegenwoordig. Ruim tien jaar geleden was een risicoanalyse in de praktijk een vodje papier waar wat ad-hoc aantekeningen op stonden, maar tegenwoordig is dat wel anders. Vandaag de dag is een risicoanalyse niet meer iets van de grote lijnen, maar een heel gedetailleerd document. Het is ook geen abstract document meer. Risico's worden gemeten aan de hand van reële, of zelfs echte aanval- en probleemscenario's. Daar waar we eerst nauwelijks een baseline aan maatregelen hadden, is een baseline vandaag voor 80% tot 90% allesomvattend. Het is tegenwoordig bijna uitzondering dat je grote infrastructurele beveiligingsmaatregelen moet toevoegen aan je projectactiviteiten. Daar zijn dan weer aparte projecten voor.

Ook de acceptatie van de uitkomst is veranderd met de tijd. Werd er voor het begin van dit millennium niet aan formele risicoacceptatie gedaan, nu verwacht business management dat er een acceptatiesessie is en willen ze graag weten welke risico's ze te accepteren hebben. Daar willen ze dan wel een mitigatieplan bij zien. Maar ook dat past zich aan. In het post-web 2.0 tijdperk komt men in een situatie waar risico's niet altijd meer onder eigen beheer te mitigeren zijn. Gebruikers zijn 'domme ganzen' die toch maar op iedere link in een e-mail klikken. Daar is niet veel aan te mitigeren… Het gebruik van internet direct door je klanten in je zakelijke processen brengt gewoon een niet-te-voorkomen inherent risico met zich mee. En we zijn bereid dat te accepteren.

Hiermee hebben we de business eindelijk aangehaakt aan het einde van de keten der risicoanalyse. Maar ook aan het begin is plaats voor de business. "Ja, we doen dan een business impact analyse (BIA)", hoor ik u al zeggen. Dat is een "Ja, maar…" De BIA wordt nog steeds op aangeven van informatiebeveiligers opgesteld over de assen van vertrouwelijkheid/exclusiviteit, integriteit en beschikbaarheid (CIA of BEI of BIV). De classificatie die uit deze beoordeling komt heet in de volksmond der beveiligers nog steeds zoiets als BIV-rating. Maar is dit ook de juiste aanpak? Zijn er andere manieren om dit te doen? Ja. Hoe worden business belangen uitgedrukt? In business drivers. En zo kan de BIA ook uitgedrukt worden. Daar verzetten wij ons nog tegen als beveiligers. Maar waarom toch?

Een BIA kijkt naar de impact van schending van vertrouwelijkheid, integriteit en beschikbaarheid. Maar de ene schending is de andere niet. Strategisch gedachtengoed van management is zwaar vertrouwelijk. Medische informatie van patiënten ook. Toch zijn de gevolgen bij schending heel anders. Wellicht moet ik daarom ook andere maatregelen nemen, in plaats van beide stukken informatie aan dezelfde baseline te onderwerpen. En als we een technisch veilige oplossing hebben zodat de directeur zijn managementinformatie op zijn mobiel mag zetten, dan wil dat nog niet zeggen dat de patiëntinformatie ineens ook op het mobieltje mag staan. Het hangt er dus vanaf. Misschien moeten we daar eens naar kijken, en niet weer eens kijken hoe we de baseline verder kunnen perfectioneren. Want we zien door de risico-scenariobomen het globale risicobos niet meer.

Lex Borger
hoofdredacteur

Foto omslag: Credits - CC by Wonderlane

INHOUDSOPGAVE

IEDEREEN EEN SUPERCOMPUTER

WAAROM SPELCOMPUTERS DE EFFECTIVITEIT VAN UW WACHTWOORDBELEID AANTASTEN

Martijn Sprengers MSc en Marc Smeets MSc CISSP CISA zijn beide werkzaam bij KPMG in de unit ICT Security & Control als IT-beveiligingsadviseur. Ze voeren o.a. penetratietesten uit waarbij wordt ingebroken op computersystemen. Het kraken van gevonden wachtwoorden is een veelvoorkomende taak en ze volgen de ontwikkeling omtrent GPU's dan ook op de voet. Ze zijn te bereiken op sprengers.martijn@kpmg.nl en smeets.marc@kpmg.nl.

Computers worden ieder jaar krachtiger. Zo ook pc's om spelletjes mee te spelen. Voor grafische toepassingen bestaan al jaren aparte insteekkaarten. Recente ontwikkelingen omtrent deze grafische kaarten zorgen niet alleen voor oogverblindend mooie spelletjes, maar hebben ook nog een effect waaraan wellicht niet iedereen denkt. Ze blijken uitermate geschikt om wachtwoorden mee te kraken. Hierdoor is het mogelijk dat wachtwoorden die we voorheen sterk genoeg achtten nu opeens gemakkelijk te achterhalen zijn door hackers. Maar ook door uw buurjongen met zijn spelcomputer.

In dit artikel bespreken de auteurs de wachtwoordschema's die uw computerprogramma's gebruiken voor het opslaan van wachtwoorden, de aanvalstechnieken die hackers gebruiken om wachtwoorden te achterhalen en waarom grafische kaarten voor deze taak zo geschikt zijn. Vervolgens komt aan de orde wat dit voor invloed heeft op uw wachtwoordbeleid en hoe u uw wachtwoordbeleid sterker en uw wachtwoorden veiliger kunt maken.

Wachtwoorden worden vrijwel nooit leesbaar in een database opgeslagen. Dan zou het wat al te gemakkelijk zijn om deze te achterhalen. Wanneer de gebruiker van een bepaalde service voor het eerst zijn of haar wachtwoord kiest, wordt deze door een wachtwoordschema versleuteld opgeslagen. Wachtwoordschema's zijn gebaseerd op cryptografische 'one-way'-functies. Dit zijn wiskundige functies die een gegeven input (wachtwoord) zo door elkaar husselen dat de uitkomst (wachtwoordhash) niet eenvoudig is terug te rekenen naar de invoer (fig. 4). Oftewel, van wachtwoord naar wachtwoordhash is te berekenen, van wachtwoordhash naar wachtwoord is vrijwel onmogelijk.

Wachtwoorden sneller gekraakt door doorbraak kracht grafische kaarten

Als een eindgebruiker inlogt op een service dan wordt de hash van het ingevoerde wachtwoord vergeleken met de reeds opgeslagen hash. Bij een match wordt toegang verleend. En omdat er geen wachtwoorden in platte tekst worden opgeslagen zijn alle wachtwoorden vooralsnog beschermd. Maar ondanks de wiskunde 'one-way'-functies vinden aanvallers toch altijd mogelijkheden om in te breken.

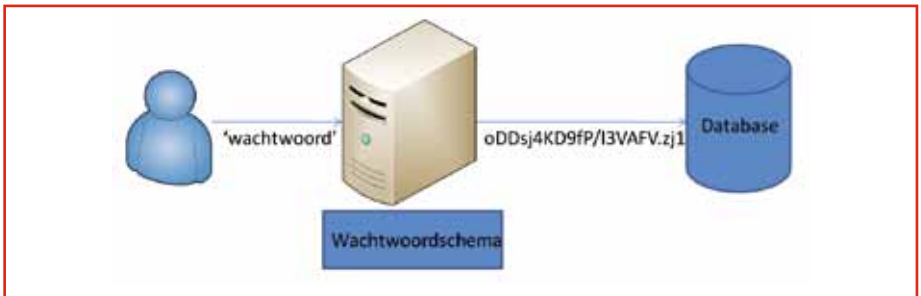


Fig. 1. Authenticatie via een wachtwoordschema. De gebruiker voert zijn wachtwoord in en het systeem genereert daar een wachtwoordhash van.

Aanvalstechnieken

Een hacker heeft een aantal manieren om in te breken in een systeem (bijvoorbeeld uitbuiten van kwetsbaarheden in software en social engineering). Maar het simpel inloggen met een juiste combinatie van gebruikersnaam en wachtwoord heeft toch vaak de voorkeur. Afhankelijk van de situatie heeft de hacker meerdere mogelijkheden om een wachtwoord te achterhalen. Op hoofdlijnen onderscheiden we twee aanvalscategorieën, online en offline. Online houdt in dat de hacker via het netwerk tracht in te loggen. Hij/zij heeft in dit geval nog geen toegang verkregen tot het systeem en probeert bijvoorbeeld combinaties van gebruikersnaam en wachtwoord op het inlogscherm van een website. Dit is een relatief trage manier van aanvallen aangezien het netwerk en tussenliggende applicatielagen ervoor zorgen dat men niet meer dan een paar pogingen per seconde kan doen.

Met miljoenen pogingen per seconde heeft de offline manier dan ook de voorkeur van de hacker. Dit vereist wel dat al toegang tot het systeem is verkregen en dat de wachtwoordhashes kunnen

worden gelezen. Dit kan, als de logische toegangsbeveiliging tot de database met die hashes niet afdoende is.
Maar zoals we eerder lazen kan de wachtwoordhash niet worden teruggedraaid tot het wachtwoord. Dus hoe achterhaalt de hacker dan de wachtwoorden? Heel simpel, de aanvaller genereert zelf wachtwoordhashes en vergelijkt deze met de te achterhalen wachtwoordhash. Bij een match weet de aanvaller het wachtwoord. Hij heeft het immers zelf berekend. Omdat de aanvaller tracht de versleuteling te kraken, wordt dit proces ook wel het kraken van wachtwoorden genoemd.
De invoer voor dit kraken zijn de kandidaatwachtwoorden. Voor de keuze van de kandidaatwachtwoorden kennen we drie methodes:

1. woordenboek waarbij bestaande woorden of een collectie van eerder gevonden wachtwoorden worden gebruikt (bijv. 'password');
2. op basis van woorden uit een woordenboek gecombineerd met getallen of vreemde tekens (bijv. 'Anne2002', of @nne02!);
3. uitputtend zoeken (brute force) waarbij alle mogelijkheden worden geprobeerd (bijv. van 'a' tot en met 'abcXYZ123!@#').

Uiteindelijk zal de aanvaller met behulp van deze laatste methode alle wachtwoorden kunnen kraken. Het kost alleen veel tijd.
Het kost een traditionele computer veel rekenkracht om wachtwoordhashes te kraken. Daarom beschouwen we wachtwoorden van ongeveer 8 karakters met kleine en grote letters, cijfers en vreemde tekens als vrij sterk. Vanaf 9 karakters worden de wachtwoorden zelfs al onkraakbaar binnen afzienbare tijd. Maar de grafische kaart brengt hier verandering in.

Rockyou Top 10 wachtwoorden

1	123456
2	12345
3	123456789
4	password
5	iloveyou
6	princess
7	rockyou
8	1234567
9	12345678
10	abc123

Waarom grafische kaarten?

Er zijn meerdere redenen waarom grafische kaarten pas sinds kort voor het kraken van wachtwoorden worden gebruikt. Ten eerste is er de constante vraag naar nog mooier en realistischer ogende computerspellen waardoor de rekenkracht van grafische kaarten ook moet toenemen. Ten tweede vindt er een verschuiving van focus plaats. Waar vroeger grafische kaarten alleen werden gebruikt voor grafische doeleinden, het berekenen van individuele pixels op je beeldscherm, kunnen ze tegenwoordig ook gebruikt worden voor meer algemene taken. De derde reden is de komst van gebruiksvriendelijke programmeerinterfaces. Deze bieden ook voor niet-grafische programmeurs kansen om de rekenkracht van grafische kaarten te benutten. De steeds groter wordende kracht van grafische kaarten is dan ook voor steeds meer doeleinden beschikbaar. Het grote verschil met de traditionele CPU is dat grafische kaarten geschikt zijn voor het doen van veel dezelfde parallelle berekeningen. Dit komt omdat dergelijke kaarten beschikken over honderden tot duizenden kleine 'cores' (miniprocessors). Dit in tegenstelling tot een traditionele processor, die maar een tot vier cores heeft (fig. 1.). Wel bestaat er een groot verschil in de architectuur. Daar waar de cores van een CPU onafhankelijk van elkaar verschillende soorten berekeningen kunnen doen, moeten de cores van een grafische kaart op ieder moment dezelfde soort berekening doen (hoewel ze deze berekeningen wel op verschillende data kunnen uitvoeren). Hierdoor zijn niet alle (wiskundige) toepassingen geschikt om op een grafische kaart geïmplementeerd en uitgevoerd te worden.

> Traditionele opvattingen over sterk wachtwoord zijn niet geheel toereikend meer

Wachtwoorden kraken is een toepassing die juist wel erg geschikt is om geïmplementeerd te worden op een grafische kaart. Dit komt omdat tijdens het kraken iedere core dezelfde soort taak moet uitvoeren (namelijk het versleutelen van een wachtwoord en deze versleuteling vergelijken met de te kraken versleuteling), maar wel op verschillende data. Bijvoorbeeld core 1 versleuteld wachtwoord 'aaaa', core 2 versleuteld wachtwoord 'aaab', etc. De cores hoeven onderling niet samen te werken waardoor al snel een grote snelheidswinst tegenover traditionele processors kan worden bereikt. Deze snelheidswinst verschilt per wachtwoordschema. In fig. 2 is te zien dat het snelheidsverschil bij het gebruik van wachtwoordschema MD5-crypt tussen de dertig en honderdmaal hoger is dan een traditionele processor met dezelfde prijs.
En 'dezelfde prijs' is hierbij ook nog eens een rekbaar begrip aangezien de ontwikkelingen, en daarmee de prijs,

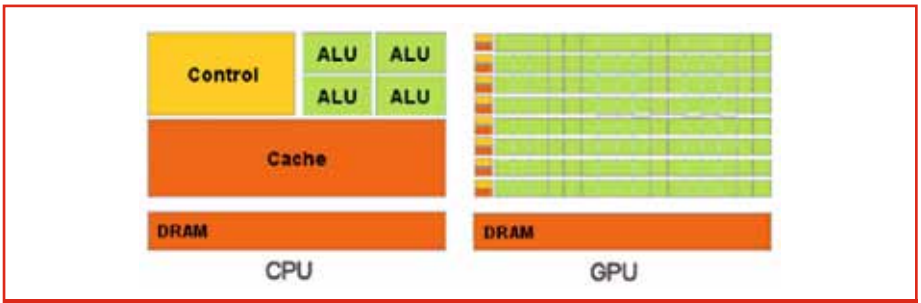


Fig. 2. Verschil in architectuur tussen grafische kaart (GPU) en normale processor (CPU). De groene ALU's zijn de rekeneenheden, ook wel cores genoemd. (Bron:[1])

op het vlak van grafische kaarten zich in hoog tempo opvolgen. De fysieke limieten zijn nog lang niet bereikt, zoals dit wel het geval is bij de CPU's, waar de ontwikkelingen veel minder snel gaan.

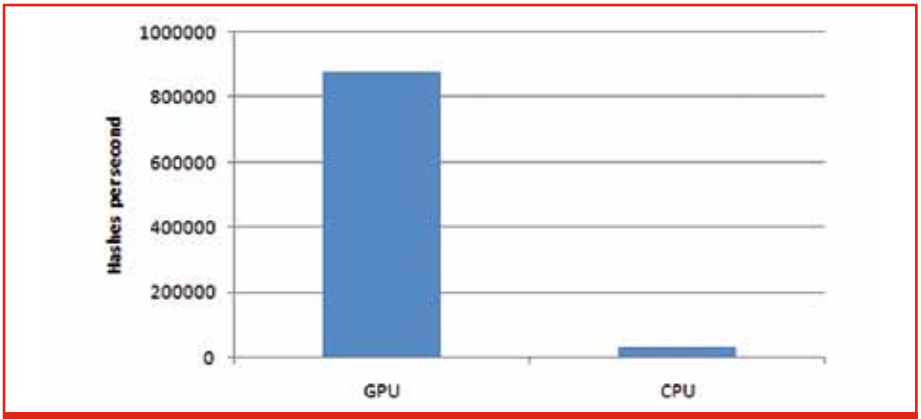


Fig. 3. Snelheid van MD5-crypt op verschillende hardware platformen. (Bron: [3])

Invloed op het wachtwoordbeleid

Wat betekent al deze rekenkracht van grafische kaarten nou voor de veiligheid van wachtwoorden? In fig. 4 wordt de kraaksnelheid van één grafische kaart vergeleken met de kraaksnelheid van één traditionele processor in dezelfde prijsklasse. Neem bijvoorbeeld de Rockyou.com database. Die is eind 2009 gehackt via een zogenoemde 'SQL-injection'. De wachtwoorden van de 32 miljoen gebruikers waren niet versleuteld opgeslagen en zijn een uiterst waardevolle bron van informatie voor de hedendaagse wachtwoordstatistiek omdat het hier echte wachtwoorden van eindgebruikers betrof. De figuur laat zien hoeveel procent van de wachtwoorden in de gelekte Rockyou.com database gekraakt kunnen worden in een bepaalde tijd als ze met het Windows (NTLM) wachtwoordschema versleuteld zijn. Het blijkt dat grafische kaarten ongeveer twintig tot dertig procentpunt meer wachtwoorden kunnen kraken in dezelfde tijd.

Het is al langer bekend dat gebruikers niet altijd in staat zijn om sterke wachtwoorden te kiezen[2]. Daarom implementeren veel organisaties een wachtwoordbeleid dat minimumeisen stelt aan de wachtwoordsterkte. Een voorbeeld van dergelijk beleid is het volgende:

- wachtwoorden hebben een minimumlengte van acht karakters;
- wachtwoorden bevatten ten minste één kleine letter, één hoofdletter, één cijfer en één speciaal teken;
- wachtwoorden dienen iedere vier maanden te worden gewijzigd.

Dit beleid zorgt ervoor dat er ten minste 948 x 6 biljard mogelijkheden zijn waaruit gebruikers (en dus ook aanvallers) kunnen kiezen. Zoals eerder beschreven doet een traditionele processor er 80 jaar over om al deze mogelijkheden af te lopen. Maar het programma OclHashcat kan in combinatie met een moderne grafische kaart van ATI meer dan 14 miljard mogelijkheden per seconde proberen. Dit zorgt ervoor dat alle wachtwoorden van acht karakters, versleuteld met het Windows(NTLM) wachtwoordschema, binnen vijf dagen gekraakt kunnen worden. De buurjongen die een spelcomputer heeft met meerdere grafische kaarten, beschikt dan ook eigenlijk over een supercomputer. Gelet op de investeringen en ontwikkelingen op het gebied van grafische kaarten zal een aanvaller, die wat meer te besteden heeft dan de buurjongen, in de nabije toekomst ook wachtwoorden van negen of tien karakters kunnen kraken.

Wachtwoorden zijn makkelijk te achterhalen door hackers en door buurjongen

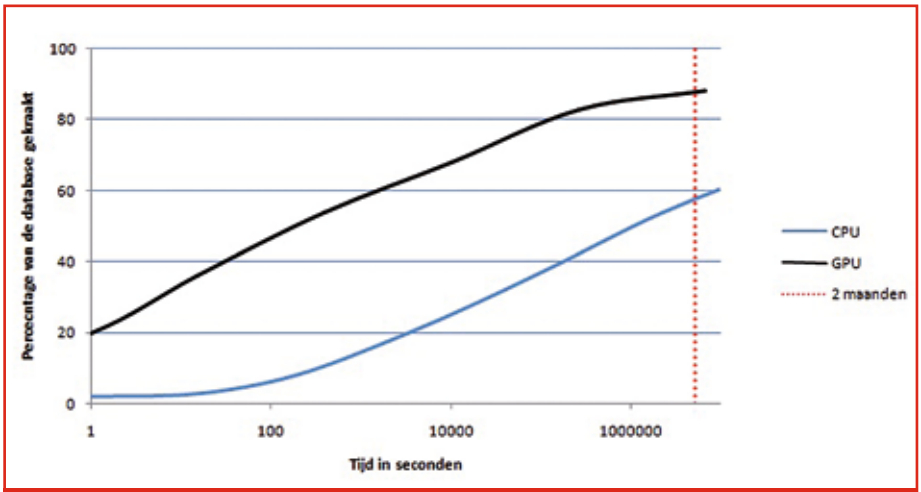


Fig. 4. De invloed van grafische kaarten op het kraken van de gelekte Rockyou.com database met 14 miljoen van de in totaal 32 miljoen gelekte wachtwoorden. (Bron: [3])

Oplossingen

De beste oplossing voor dit probleem zou bereikt kunnen worden als gebruikers meer willekeurige, maar vooral ook langere wachtwoorden zouden kiezen. Een wachtwoord van twaalf karakters zal niet in de nabije toekomst zomaar gekraakt kunnen worden. Hoewel een goed wachtwoordbeleid hierbij kan helpen, is het aangetoond dat gebruikers moeite hebben met het onthouden van lange wachtwoorden. Laat staan wanneer ze voor elke service een apart wachtwoord moeten onthouden, wat zal leiden tot een vermenigvuldiging van het aantal post-it's op beeldschermen en werkplekken.
Een mogelijkheid die uitkomst biedt voor gebruikers zijn tools voor het beheren van wachtwoorden, die random wachtwoorden kunnen genereren en

aan de gebruikerskant versleuteld kunnen opslaan. Een gebruiker hoeft dan alleen nog maar één sterk wachtwoord te onthouden dat toegang biedt tot al zijn andere wachtwoorden. Een nadeel van deze methode is dat de gebruiker altijd het versleutelde bestand paraat moet hebben om gebruik te maken van services en internetdiensten. Even snel je e-mail bekijken bij een vriend kan nu niet meer zonder je persoonlijke wachtwoorddatabase.

Oplossingen moeten niet alleen aan de gebruikerskant worden gezocht. Ook aan de servicekant kunnen verschillende oplossingen worden onderscheiden.

- Betere wachtwoordschema's. Nieuwe wachtwoordschema's maken gebruik van een speciale techniek die de complexiteit van de berekeningen verhoogt. Het is dan voor één gebruiker nog steeds mogelijk om het versleutelde wachtwoord te berekenen, maar voor een aanvaller, die veel mogelijkheden moet proberen, wordt het haast onmogelijk gemaakt. Omdat het verhogen van de complexiteit van de berekeningen afhankelijk is van de op dat moment geldende hardwarenormen, is het advies dan ook om periodiek te kiezen voor betere wachtwoordschema's.
- Multi-factor authenticatie. Dit betekent dat een gebruiker tijdens authenticatie niet alleen iets verstrekt wat hij weet, zoals een wachtwoord of pincode, maar ook iets wat hij heeft, zoals een fysieke token of smartcard, of wat hij is, zoals een vingerafdruk. Een aanvaller moet dan twee of meer factoren in handen zien te krijgen om zich toegang te verschaffen.
- Vaker wisselen van wachtwoord. Als een aanvaller zes maanden nodig heeft voor het kraken van een wachtwoord, maar de gebruiker het wachtwoord al na drie maanden dient te wijzigen, dan kan de aanvaller het wel kraken maar is het nutteloos voor de aanval. Vaak wisselen is dan ook het advies. Maar let bij het wisselen er wel op dat de wachtwoorden geen logisch vervolg van elkaar zijn (zie ook kader 'kiezen van een sterk wachtwoord').

Grafische kaarten geschikt voor veel dezelfde parallelle berekeningen

Het kiezen van een sterk wachtwoord

Het is vooral de lengte van een wachtwoord dat zorgt voor de sterkte. Het is daarom aan te raden een wachtwoord te kiezen dat zeker meer dan tien karakters bevat. Het wachtwoord wordt nog sterker wanneer het speciale tekens en cijfers bevat. Dergelijke wachtwoorden zijn erg moeilijk te onthouden.
Een techniek die helpt bij het genereren van een wachtwoord is de 'mnemonic phrase'. Kies een makkelijk te onthouden zin en neem van de woorden steeds de eerste of tweede letter. Het veiligste is een persoonlijke zin te kiezen en niet een die op het internet of in films te vinden is. Een voorbeeld van een mnemonic phrase is de volgende zin: 'Mijn zus Debby heeft 3 honden: Max, Boris en Klaus'. Het afgeleide wachtwoord is dan: 'MzDh3h:M,B&K'. Dit wachtwoord bevat twaalf karakters, met hoofdletters, kleine letters, cijfers en speciale tekens. Dit is zelfs voor een verzameling van grafische kaarten niet zomaar te achterhalen.
Let er tevens op dat u niet overal hetzelfde wachtwoord gebruikt. Het zou vervelend zijn als het gekraakte wachtwoord van uw account bij een webshop ertoe leidt dat een aanvaller ook toegang heeft tot uw internetbankieromgeving. Ook wordt het afgeraden opeenvolgende wachtwoorden te kiezen. Mocht een aanvaller onverhoopt uw wachtwoord 'Wachtwoord!01' kraken maar deze niet kunnen misbruiken omdat het is verlopen, dan begrijpt u vast dat de aanvaller zal proberen of u niet misschien 'Wachtwoord!02' als huidige wachtwoord heeft.

Conclusie

Eens in de zoveel jaar zijn er doorbraken in de wereld van computerkracht. De huidige doorbraak in de kracht van grafische kaarten in (spel)computers zorgt niet alleen voor oogverblindend mooie spelletjes, maar ook voor een doorbraak in de snelheid waarmee wachtwoorden kunnen worden gekraakt. Hackers maken hier dankbaar gebruik van en dat heeft nu impact op de veiligheid van uw wachtwoorden en daarmee van uw IT-omgeving. Dit zorgt ervoor dat traditionele opvattingen over een sterk wachtwoord (bijvoorbeeld minimaal 8 karakters met hoofd- en kleine letters, cijfers en speciale tekens) niet geheel toereikend meer zijn. Hoewel een aantal maatregelen te nemen is aan de kant van de technische configuratie van uw IT-omgeving zullen we hoe dan ook nog een flinke tijd met wachtwoorden werken. De voornaamste aanbeveling is dan toch ook om het gebruik van moeilijkere en vooral langere wachtwoorden (zie kader) af te dwingen. Daarmee bent u in ieder geval de komende tijd een stuk beter voorbereid op aanvallen van hackers en zelfs van uw buurjongen.

Literatuur

[1] *Compute Unified Device Architecture Programming Guide. Technical report, Nvidia Corporation, August 2010.*

[2] *W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. NIST Special Publication, 800:63, 2004.*

[3] *Martijn Sprengers. Gpu-based password cracking: On the security of password hashing schemes regarding advances in graphics processing units. Master's thesis, Radboud University Nijmegen, January 2011.*

[4] *J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. Security & Privacy, IEEE, 2(5):25–31, 2004.*

Link

OclHashcat: http://hashcat.net/oclhashcat/

DIGITALE TOEGANG VOOR UNIVERSITEITEN EN HOGESCHOLEN VIA TRUSTED THIRD PARTY

Eefje van der Harst van Surffederatie is per e-mail bereikbaar op Eefje.vanderHarst@surfnet.nl

Je kunt makkelijker afspraken maken met één ICT-organisatie, dan met vijftig onderwijsinstellingen of zevenhonderdduizend studenten. Dit eenvoudige gegeven verklaart het succes van de SURFfederatie. Dé authenticatiedienst voor hoger onderwijs en onderzoek.

Voor uitgevers die hun producten digitaal via internet willen aanbieden is het een groot dilemma. Hoe combineer je gebruikersgemak met de zekerheid dat je uitgaven alleen worden gezien door mensen die daar recht op hebben? Dat dilemma wordt nog groter als de abonnee een universiteit of hogeschool is. Jaarlijks stromen daar honderden of zelfs duizenden studenten in en uit. Hoe ga je om met dit soort eindgebruikers?

Een traditioneel middel om ze te authenticeren is IP-afscherming. Dan stelt een uitgever zijn content alleen open voor gebruikers die deze benaderen vanaf een internetadres van een universiteit die voor het abonnement betaalt.

Dat heeft echter twee nadelen. Ten eerste zijn universiteitsbibliotheken doorgaans openbaar toegankelijk. Iedereen kan daar binnenlopen en achter een pc gaan zitten. IP-afscherming is dus maar een zwak authenticatiemiddel.

Ten tweede is er een nadeel voor de eindgebruikers. Studenten studeren immers niet alleen in de bibliotheek of op de faculteit, maar ook thuis of in de trein. Via de iPhone of laptop is internet altijd en overal beschikbaar, maar met IP-afscherming moet je opeens weer op de fiets stappen als je even iets na wilt kijken in een boek of tijdschrift. Dat is niet meer van deze tijd.

Single sign-on

De oplossing van het Nederlandse hoger onderwijs voor dit probleem is de SURFfederatie. Daar zijn tientallen universiteiten en hogescholen bij aangesloten, én een snel groeiend aantal uitgevers, zoals Springer en Elsevier, en andere service providers. Op het moment dat een Delftse student toegang wil tot een uitgeverswebsite, wordt zijn verzoek automatisch doorgegeven aan de SURFfederatie. Die vraagt dan aan zijn universiteit of de bezoeker daar inderdaad als student staat ingeschreven en geeft het antwoord door aan de uitgeverssite.

> Eén wachtwoord is genoeg voor alle digitale diensten, binnen en buiten de universiteit

Dit alles gaat in een fractie van een seconde, zonder dat de student ziet wat er technisch op de achtergrond gebeurt. Hij hoeft slechts een inlognaam en wachtwoord te onthouden, namelijk die voor het netwerk van zijn instelling. Zodra hij daar online is, kan hij overal bij waar hij bij mág. Single sign-on is het motto. Dit is mogelijk door het gebruik van wereldwijde standaardprotocollen, waarvan Shibboleth en SAML de bekendste zijn. Een uitgever hoeft alleen te weten of een instelling een abonnement heeft op zijn producten. Met 'federatieve controle' is de authenticatie dan beter gewaarborgd dan met IP-afscherming, want als een student inlogt weet men zeker dat deze gebruiker ook bij deze instelling hoort. De student zal deze gegevens niet snel weggeven, hij heeft dezelfde

> De federatie is een discrete deurwacht

SURFfederatie

De SURFfederatie is in 2006 opgezet door SURF, de ICT-samenwerkingsorganisatie van de Nederlandse universiteiten, hogescholen en onderzoeksinstellingen. Inmiddels zijn daarvan 69 als identity provider aangesloten bij de federatie, goed voor meer dan 700.000 gebruikers.

Samen krijgen die langs deze weg toegang tot diensten van 60 service providers. Aan de uitgeverskant zijn dat naast MetaPress, Springer en Elsevier bijvoorbeeld ook EduPoort, het gezamenlijke toegangsportaal van Malmberg, ThiemeMeulenhoff en Noordhoff Uitgevers. EBSCO en Swets zijn eveneens aangesloten, evenals WebFeat, Zimbra en Google, dat zijn onderwijsdiensten langs deze weg heeft opengesteld voor het Nederlandse hoger onderwijs.

De aantallen gebruikers en aanbieders blijven gestaag groeien.

Open standaarden
De SURFfederatie is gebaseerd op wereldwijd gangbare protocollen die de uitwisseling regelen van gegevens tussen identity- en service providers. De belangrijkste protocollen zijn SAML en Shibboleth.
SAML (Security Assertion Markup Language) is een gestandaardiseerde taal die wordt gebruikt om binnen en tussen federaties informatie uit te wisselen voor authenticatie en autorisatie. Daarbij gaat het met name om attributen, ook wel aangeduid als claims. Dat zijn kenmerken van gebruikers op basis waarvan zij toegang kunnen krijgen tot informatie. Shibboleth beschrijft een vergelijkbare architectuur die federaties kunnen gebruiken om toegang te regelen via SAML. Zowel SAML als Shibboleth zijn open standaarden. Dit wil zeggen dat iedereen er vrijelijk en kosteloos gebruik van mag maken. Dat gebeurt dan ook wereldwijd, op grote schaal.

gebruikersnaam en wachtwoord namelijk ook nodig voor alle belangrijke studiezaken, zoals mail en cijferlijsten. Anderzijds worden ook zijn veiligheid en privacy gegarandeerd. Omdat er lokaal bij de instelling geauthenticeerd wordt, blijven alle inloggegevens op de server van zijn eigen universiteit. Persoonsgegevens worden alleen uitgewisseld tussen de instelling en de dienst als ze absoluut noodzakelijk zijn voor het gebruik van de dienst. In contracten met instellingen en dienstaanbieders maakt de SURFfederatie duidelijke afspraken over wat er wel en niet mag met deze persoonsgegevens. De federatie is dus een discrete deurwacht.

Aanzienlijke schaalvoordelen
Het is geen wonder dat er wereldwijd steeds meer federaties worden opgericht. Ze bieden namelijk aanzienlijke schaalvoordelen voor de service providers. Zodra de connectie er is tussen een federatie en een service provider, kunnen alle aangesloten instellingen meteen gebruikmaken van al diens producten. Voor zover ze erop geabonneerd zijn, uiteraard.

Ook als een aangesloten federatie wordt uitgebreid met nieuwe leden, kost dat de service providers weinig of geen inspanning. Een federatie is namelijk niet alleen een betrouwbare koerier, maar ook een tolk. Ze zorgt dat de gegevens van de aangesloten instellingen (de identity providers) allemaal in dezelfde vorm worden gepresenteerd aan de service provider. Een uitgever hoeft dan niets meer af te stemmen met een nieuwe universiteit die zich aansluit bij de SURFfederatie, want de benodigde vertaalslag neemt de federatie voor haar rekening.

> Laat de eindgebruiker zelf controleren welke gegevens naar de service provider gaan

Maatwerk bieden
De technische ontwikkelingen staan niet stil. Standaarden worden steeds verder verbeterd, en dat biedt uitzicht op nieuwe mogelijkheden. Momenteel wordt federated access vooral gebruikt voor authenticatie. Hoort deze inlogger bij deze klant? Bij IP-afscherming echter wordt bijvoorbeeld onderscheid gemaakt tussen faculteiten. Dat zou ook met de SURFfederatie kunnen. Dan zijn bijvoorbeeld medische tijdschriften alleen toegankelijk voor de faculteit Geneeskunde. Maar je zou ook kunnen zien waar de interesses liggen bij de diverse faculteiten. Of medewerkers zouden meer toegangsrechten kunnen

> Single sign-on is het motto

Service provider: snel rendement van noest handwerk voor Metapress
Is het werken met de SURFfederatie echt zo gemakkelijk voor een service provider? Zijn er nooit complicaties? Uitgever Springer laat zijn website met tijdschriften hosten door Metapress in de Verenigde Staten, een specialist in online uitgeven. Alle aspecten, van contentbeheer tot e-commerce, kan Metapress desgewenst namens de uitgever voor zijn rekening nemen. Woordvoerder Heather Klusendorf Stewart vertelt dat federaties hierbij een steeds grotere rol spelen. “We zijn daarmee begonnen in 2006. Eerst hebben we de grootste drie federaties aangesloten, die van het Verenigd Koninkrijk, Zwitserland en Duitsland. En daarna de nummer vier: de SURFfederatie.”
Wat komt daarbij kijken? Noest handwerk, zo blijkt. Bij authenticatie moeten namelijk allerlei gegevens worden uitgewisseld, zoals de gebruikersnaam en de naam van de instelling. Klusendorf: ‘Dit soort dingen vraagt tijd, want elke federatie heeft ze net iets anders gestructureerd. Bij de SURFfederatie ging het sneller dan anders, doordat de mensen in Nederland er echt bovenop zaten. Dat was erg plezierig.”
De tijdsinvestering betaalt zich snel terug, want als de verbinding met een federatie eenmaal draait is het verder smooth sailing, zo benadrukt Klusendorf. Geen wonder dus dat MetaPress blij is dat federaties steeds meer de norm worden voor het koppelen van universiteiten en andere grote organisaties aan uitgeversdiensten. Je slaat tientallen vliegen in een klap. “We werken nu met een kleine dertig federaties. Na Nederland volgden Spanje bijvoorbeeld, maar ook Frankrijk, Italië, Denemarken, Griekenland, Noorwegen, Portugal… Het is een lange lijst.“

krijgen dan studenten. Dan wordt de SURFfederatie dus gebruikt voor fijnmazigere autorisatie.
Uitgevers gebruiken nu nog weinig verfijningen om gepersonaliseerde collecties samen te stellen, maar er zijn heel veel theoretische mogelijkheden. Die kunnen werkelijkheid worden als er meer gebruik wordt gemaakt van attributen die opgeslagen worden door universiteiten. Voor- en achternaam, e-mailadres, vakgebied en noem maar op. Service providers kunnen veel meer persoonlijk maatwerk bieden zodat medewerkers en studenten gemakkelijk vinden wat ze nodig hebben, en tarieven wellicht worden verlaagd.

User controlled privacy

Van de andere kant roept zo'n gegevensstroom ook zorgen op over privacy. De SURFfederatie is daar heel duidelijk over. Service providers moeten contractueel vastleggen dat eventuele gebruikersgegevens uitsluitend dienen om de afgenomen dienst mogelijk te maken. Marketing valt daar bijvoorbeeld buiten.
Maar het is heel goed mogelijk dat veel gebruikers geen bezwaar zouden hebben tegen een meer persoonlijke dienstverlening. Als het om privacy gaat heb je immers drie soorten mensen: paranoïden, pragmatisten en zorgelozen. Laat de eindgebruiker zelf controleren welke gegevens naar de service provider gaan, en je houdt ze alledrie tevreden.

Paspoorten voor het internet

SURFnet, de 'technische' poot van SURF, heeft daarom samen met ICT-instituut Novay een grootschalige proef gedaan met user controlled privacy bij drie universiteiten. Gebruikers kregen een nieuwe interface op het scherm, die hun liet zien én controleren welke persoonsgegevens de universiteit naar afzonderlijke service providers stuurde. De uitdaging voor de onderzoekers was om een goede combinatie te vinden van overzichtelijkheid, controle en gemak.

3 soorten mensen: paranoïden, pragmatisten en zorgelozen

Mensen willen niet iedere keer 'dit is goed' klikken om een website toegang te geven tot hun data. Maar met een optie 'dit is altijd goed' vergeten ze na verloop van tijd met wie ze welke data delen. De oplossing werd gevonden in een timed consent. Ze geven dan toestemming voor een korte periode. Daarmee bleek de juiste balans gevonden, want bij een gebruikersenquête bleek maar liefst 86% tevreden over dit systeem. Ook de onderwijsinstellingen zijn blij als de eindgebruiker beter zicht houdt op wat er met zijn persoonsgegevens gebeurt.
SURFnet is nu samen met de aangesloten instellingen aan het kijken hoe user controlled privacy kan worden geïmplementeerd in de totale infrastructuur. Lokaal bij de instelling of centraal bij de SURF-federatie?

Identity provider: voordeel en gemak voor TU Delft

De Delftse universiteit was een van de eerste gebruikers van de SURFfederatie en vanaf het begin actief betrokken bij de ontwikkelingen. "We hebben bijvoorbeeld samen met SURFnet gedefinieerd welke kenmerken van studenten en medewerkers je in zo'n federatie wilt kunnen uitwisselen", vertelt Laura Stappershoef. Zij is ICT-architect en functioneel beheerder van het Delftse identitymanagementsysteem. "Voor de hand liggend zijn natuurlijk de naam van de gebruiker en of het een student of medewerker betreft. Maar ook iemands Studielinknummer is heel handig omdat je daarmee studenten kunt identificeren over universiteiten heen." Dat was van extra belang voor de TU Delft, die niet alleen nauw samenwerkt met de twee andere technische universiteiten, maar ook opleidingen deelt met Leiden.
Uit beveiligingsoogpunt is de SURFfederatie voor de beheerders heel eenvoudig. Wanneer iemand vertrekt, kun je meteen de toegang tot alle systemen blokkeren. "Kostenreductie is ook een belangrijk pluspunt", zo benadrukt Stappershoefs collega Wim Penninx. "In plaats van allemaal losse koppelingen met SURFspot.nl, SURFmedia en contentleveranciers als Elsevier Science Direct en Metapress, hoeven we alleen een verbinding te hebben tussen ons identitymanagementsysteem en de SURFfederatie."
Stappershoef voegt toe: "Het is voor ons dus veel gemakkelijker geworden om nieuwe diensten aan te bieden aan studenten en medewerkers. Bovendien hoeven we geen trucs uit te halen om mensen vanaf hun huis toegang te verlenen tot een externe aanbieder. De SURFfederatie is echt anytime anywhere. En het aanbod van diensten die geschikt zijn voor koppeling met de SURFfederatie is groeiende."
Zo bleek het technisch gezien totaal geen moeite te kosten om de koppeling tot stand te brengen met Google Apps. "Op het moment dat je een contract met Google hebt en dat aan SURFnet doorgeeft, kun je je gebruikers meteen Google Apps aanbieden", zegt Penninx. "Vergelijk dat maar eens met het installeren van een tekstverwerker en een mailprogramma op 6.000 werkstations."
Voor zulke SaaS-toepassingen, die alleen gebruikersauthenticatie nodig hebben om iemand toegang te verlenen, is de SURFfederatie dus heel handig.
"De SURFfederatie is een belangrijke infrastructuur voor ons", besluit Penninx. "En een mooi voorbeeld van langetermijndenken waar het hele hoger onderwijs in Nederland de vruchten van plukt."

Digitale persoonscertificaten

Een van de toepassingen die gebruikmaakt van de gemakken van SURFfederatie, zijn digitale persoonscertificaten. Dat zijn een soort paspoorten voor het internet. Je kunt ze gebruiken om bijvoorbeeld te bewijzen dat een e-mailbericht of een PDF echt van jou afkomstig is. Of een instelling kan ze gebruiken om de toegang tot bepaalde systemen steviger af te grendelen. Cruciaal is dat zo'n bewijs wordt uitgegeven door een alom vertrouwde instantie. Voor de Europese academische gemeenschap is dat TERENA, de organisatie van Europese academische netwerken, in Nederland vertegenwoordigd door SURFnet. Goede internationale afspraken garanderen dat een digitaal persoonscertificaat wereldwijd en eeuwig uniek is. Een controle op basis van het tonen van het paspoort garandeert dat zo'n persoonscertificaat daadwerkelijk hoort bij een natuurlijk persoon.
Via de SURFfederatie kan zo'n bewijs eenvoudig en snel online worden uitgegeven, mits de instelling waar de aanvrager bijhoort bepaalde extra attributen voor deze categorie gebruikers heeft vastgelegd. Zo ontstaat een digitale academische wereld die wordt bijeengehouden door de zekerheid dat iedereen is wie hij zegt te zijn. Dat garandeert de SURFfederatie.

www.surffederatie.nl

COLUMN

HOE IK GEDWONGEN WERD TE KIEZEN VOOR VEILIGHEID EN PRIVACY

Eigenlijk zou ik er al rekening mee moeten houden. Althans, het zou me niet moeten verbazen dat het noodzakelijk is. Ik werk immers zelf in de informatiebeveiliging, als jurist weliswaar, maar toch. Dan weet je des te beter dat sommige zaken gevoelig liggen (ik heb al veel Non Disclosure Agreements voorbij zien komen). Zo doe ik, en daar schreef ik al eens eerder over, aan zelfcensuur en zet ik niet klakkeloos alles online. Ik Twitter actief, ook over mijn dochter, die ik daar liefkozend 'kleine diva' noem. De grote, dat ben ik. Ik plaats weleens een foto van haar, vertel wat we doen, waar we zijn, hoeveel plezier we hebben. Maar dat doe ik niet meer zomaar. Daar heb ik, en ik besef me hoe gek dit zal klinken, een Facebookpagina voor. Sinds kort. Sinds dat bericht over mijn dochter.

Niet zo lang geleden kreeg ik dat bericht. Van mijn ex-echtgenoot. Als u opgelet heeft, weet u dat ik getrouwd was, maar dat ik niet zo heel goed ben in dat getrouwd blijven… Enfin, dat bericht dus. Hij doet een leuke klus die ex. Uitdagend, mooi, veel werk te verzetten. Maar diezelfde klus heeft een donkere kant. Die klus ging gepaard met bedreigingen. En dan niet van dat lullige spul, maar de 'real deal'. Ik zal niet uitweiden over die bedreigingen, dat is niet de portee van dit verhaal. Maar dat het wel degelijk erg serieus was (en is) blijkt uit het feit dat ik niet meer zomaar mijn locatie kan onthullen op een publieke online plek. En dan al zeker niet als mijn dochter bij me is. Foto's plaatsen is daardoor ook uit den boze, uit omgevingsmateriaal is immers voor een beetje handige mensen gemakkelijk af te leiden waar ik me bevind. Wie kwaad in de zin heeft, kan dat met een paar muisklikken wel voor elkaar krijgen, ook als ik op Twitter netjes mijn mond dichthoud. Dat besef ik, maar het hele gebeuren zet me wel even met beide benen op de grond. Ik praat regelmatig over dit soort zaken. Heb het over privacy, het niet teveel onthullen over jezelf in de online wereld en het gericht kiezen wat je zelf kenbaar wenst te maken. Ik ben online behoorlijk aanwezig en de manier waarop is misschien niet die van iedereen, maar goed, dat is mijn eigen keuze.

Mijn Twittermond viel er dus ook echt stil van. Risico's komen ineens wel erg dichtbij allemaal. En ik merk dat ik momenteel bij elke tweet wel drie keer nadenk. Staat er niets waaruit je kan afleiden of mijn dochter NU bij me is? Staat er niets waaruit je mijn locatie kunt herleiden? Ik ben nu op een publieke plaats met veel mensen, kan ik daar wel over twitteren of is het toch beter van niet? Foto's laat ik maar echt even zitten, tenzij het een focus is op een kopje koffie of iets dergelijks. Goed. Twitterprotocol. Dat lukt. Het gaat om mijn dochter, dan kan ik alles. Maar wat doe ik nu met mijn vrienden en familie die ik altijd online op de hoogte hou van mijn reilen en zeilen? Diezelfde vrienden en familie die toch wel heel graag willen weten hoe het met me gaat als ik in mijn eentje op surfvakantie naar Bali ga. En 100 sms'jes sturen is ook een beetje veel van het goede (niet iedereen gebruikt WhatsApp). Ja, dan open je dus een Facebookaccount. Die plaats waar het niet echt al te best gesteld is met de privacy als je alle verhalen bij elkaar optelt. Maar tegelijk die plaats waar ik zelf bepaal wie mijn content ziet en ik alles achter slot en grendel kan doen. Ja, je moet er aardig wat vinkjes voor plaatsen. Maar als je er even voor gaat zitten, dan staat alles op 'alleen vrienden'. Nu hoor ik u denken: "Maar je kunt Twitter toch ook privé maken?" Ja, dat kan. Maar dat druist wel in tegen de wijze waarop Twitter gebruikt wordt en hoe het medium sociaal gezien in elkaar zit. Daar voel ik me niet prettig bij om dat op slot te zetten. Twitter is open, snel, delen, leren van elkaar, verspreiden, vragen stellen en antwoorden krijgen. De kracht van Twitter ligt hem nu juist in die openheid en snelheid van het netwerk. De dreiging is gelukkig inmiddels weer iets naar beneden geschaald, maar nog niet geweken. Voorlopig hou ik het dus nog even op Facebook voor de veiligheid en de privacy…

Mr Rachel Marbus
@rachelmarbus op Twitter

IS DE AANDACHT VOOR VEILIG PROGRAMMEREN WEL ZO NIEUW?

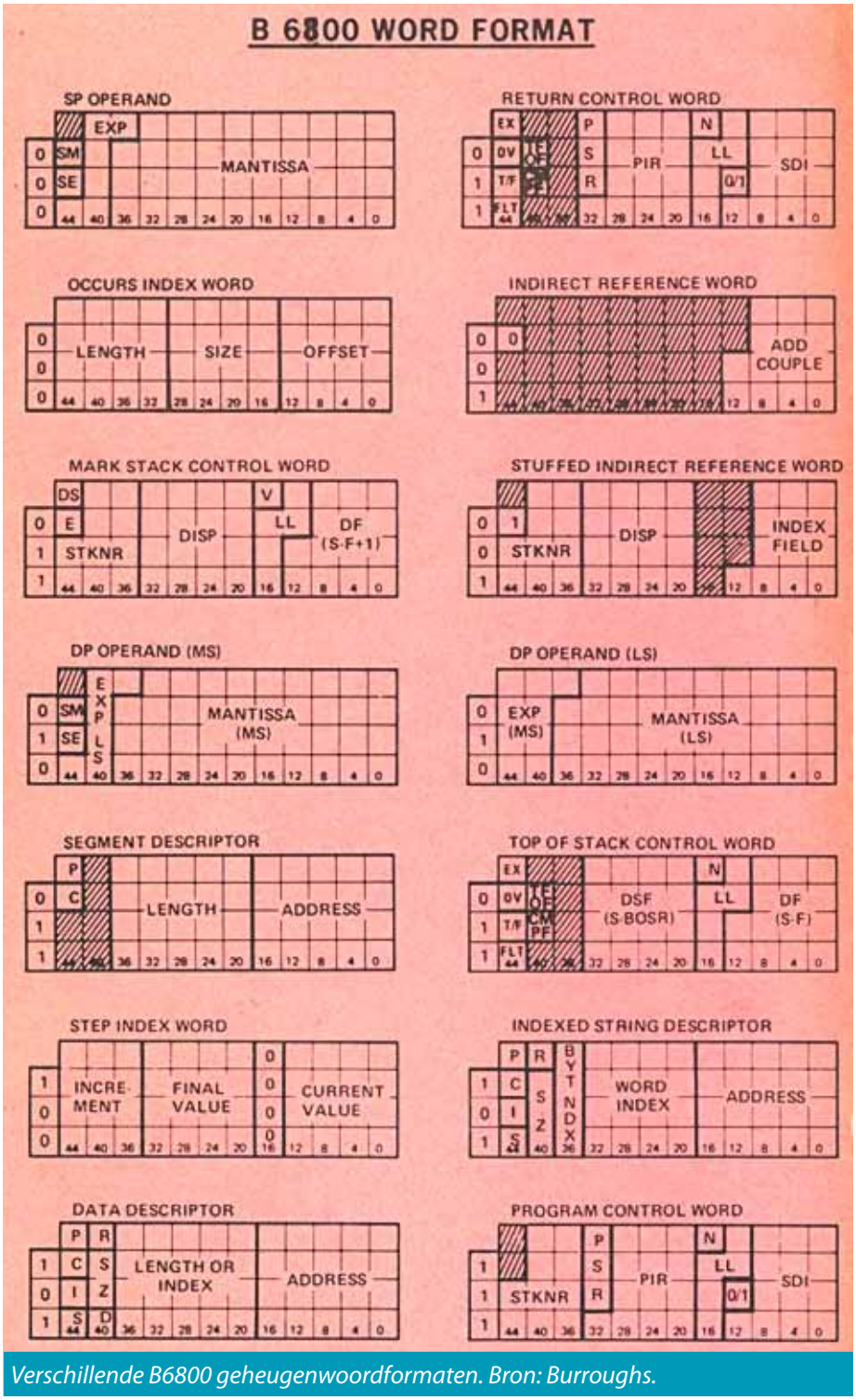
Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via lex.borger@domustechnica.com

Fietsen verleer je niet. Programmeren kennelijk ook niet. Deze gedachte overviel me tijdens mijn bezoek aan de OWASP BeNeLux 2010 in Eindhoven op 2 december. Deze gedachte voegde zich bij een andere mening die ik al een tijdje heb. Ik verbaas me over het soort kwetsbaarheden wat in applicaties gevonden wordt. In besturingssystemen worden nog steeds buffer overflows bij de vleet gevonden.

In webapplicaties is het niet anders, al hebben de kwetsbaarheden een ander karakter. Kijken we naar de huidige OWASP top 10 lijst dan zijn de top twee kwetsbaarheden 'injection' en 'cross-site scripting'. Deze kwetsbaarheden staan al jaren in de top 10. In beide gevallen is de webapplicatie kwetsbaar omdat er data worden gebruikt die vanuit een onbetrouwbare bron zijn binnengekomen. Meestal zal dit gewoon tekst zijn die de gebruiker intikt in een web-form. Als de informatie van de gebruiker afkomt en de gebruiker geen fouten maakt en niet kwaadwillend is, dan gaat dit goed. Dat is wel een hele lijst aannames, maar als beveiliger mag je daar niet vanuit gaan.

Luisterend naar de presentaties hierover, kreeg ik spontaan flashbacks naar mijn programmeercarrière. Ik heb als software engineer nooit het internettijdperk meegemaakt. Sterker nog, ik heb geprogrammeerd voor een mainframe platform. Niet van IBM, maar van Unisys, de A Series systemen.
Nu waren er in die tijd geen webapplicaties, maar de problematiek achter buffer overflows was bekend en ook van injectieproblematiek waren we ons bewust. Cross-site-scripting is wat moeilijker te projecteren op de systemen uit die dagen.

A Series-systemen hebben een andere architectuur dan de PC of UNIX. Een groot verschil is dat ieder geheugenwoord gemarkeerd is met een 'tag' die nadere informatie geeft over de inhoud van het geheugen. Het is vergelijkbaar met Intel's 'Execute Disable Bit', maar is



Verschillende B6800 geheugenwoordformaten. Bron: Burroughs.

veel rijker (drie tot vier bits per woord). Het effect is dat bij elk stuk geheugen gemarkeerd wordt of het code of data bevat en dat betekent dus dat het uitvoeren van data als code niet mogelijk is.

Het gebruik van tags biedt al een aardige bescherming tegen het onbedoeld uitvoeren van data als code. Data heeft als tag altijd een waarde van 0 of 2, code altijd 3. Afwijkingen hiervan leveren alleen maar systeem-interrupts op, wat door het OS afgehandeld wordt als programmafouten. Het programma wordt dan doorgaans geforceerd beëindigd. Buffer overflows zijn hiermee verleden tijd. Dit is veilig, maar niet echt gebruikersvriendelijk. Om het gebruikersvriendelijk te maken is programmeerhulp nodig.

Op A Series programmeerde ik niet in Java of C++, maar in ALGOL. Voor diegenen die ALGOL niet kennen, het lijkt het meest op Pascal, met strikte syntax en typing. Het A Series ALGOL heeft een aantal uitbreidingen ten opzichte van standaard ALGOL 60. Een paar hiervan gebruikte ik om juist buffer overflows en injectieproblematiek buiten het operating system om te voorkomen, zodat het geen programmafouten oplevert.

SCAN statement

Het SCAN statement kan efficiënt de inhoud van een buffer inspecteren. Het statement heeft een aantal invoerparameters, waaronder een pointer naar een locatie in de buffer en de overgebleven lengte van de buffer. Het statement levert ook als uitvoer een pointer naar de bufferlocatie waar de scan gekomen is en de nieuwe resterende lengte in de buffer. Het doel van de functie is zoeken in de buffer tot aan een stopvoorwaarde is voldaan. Zo kun je zoeken naar een specifiek karakter, zoals een spatie of een NULL, maar ook naar specifieke collecties van karakters, zoals een alfanumeriek of een niet-toonbaar karakter. Deze collecties heten TRUTHSETs. Hiermee kan een buffer snel worden geïnspecteerd op een correcte syntax of het wel of niet voorkomen van karakters die worden gebruikt in een injectieaanval.

Voor de lezers met programmeerervaring illustreer ik dit met wat programmaregels in het kader SCAN Statement als voorbeeld. Deze tekst is een voorbeeld van de typische constructie die heel snel externe data in een buffer valideert.

Burroughs B6900 mainframe. Bron: Burroughs.

SCAN Statement

```
...
INTEGER PROCEDURE GETINPUT (PTR);
  VALUE PTR;
  POINTER PTR;
  ... % procedure leest externe input en geeft gelezen buffer-
lengte terug,
    % negatieve lengte is een foutindicatie
ARRAY BUFFER [0:999];
TRUTHSET ESCAPECHAR (48"00" "&' \"); % dit zijn de tekens die
niet in het buffer mogen staan
POINTER BUFPTR;
INTEGER BUFLEN;
...
BUFPTR := POINTER (BUFFER)
BUFLEN := GETINPUT (BUFPTR);
IF BUFLEN < 0 THEN <throw read exception>;
SCAN BUFPTR:BUFPTR FOR BUFLEN:BUFLEN UNTIL IN ESCAPECHAR;
% de constructie BUFPTR:BUFPTR geeft aan dat de pointer mee-
bewogen moet worden met het scannen
IF BUFLEN > 0 THEN <throw invalid char exception>;
...
```

Voorbeeld:

```
...
INTEGER PROCEDURE GETINPUT (PTR);
  VALUE PTR;
  POINTER PTR;
  ...
ARRAY BUFFER [0:999];
REPLACETABLE VALIDCHARS (EBCDIC TO " ";
  ALPHANUMERIC TO ALPHANUMERIC; "-_;" TO "-_;");
% deze tabel vertaalt alle niet-alfanumerieke tekens naar
spaties, behalve "-_;"
POINTER BUFPTR;
INTEGER BUFLEN;
...
BUFPTR := POINTER (BUFFER)
BUFLEN := GETINPUT (BUFPTR);
IF BUFLEN < 0 THEN <throw read exception>;
REPLACE BUFPTR BY BUFPTR FOR BUFLEN WITH VALIDCHARS;
...
```

Detectie van ongewenste tekst is dus heel snel gedaan. In dit voorbeeld is de validatie bewust uit de leesopdracht GETINPUT gehaald, in de praktijk zul je dat juist daar onderbrengen. Of juist een REPLACE statement gebruiken, zoals hierna wordt uitgelegd.

REPLACE statement

Bij het kopiëren van buffers wil je alleen zinnige informatie kopiëren. Het REPLACE statement maakt dit mogelijk. Dit statement gebruikt twee pointers, een bron- en een doelpointer. Ook hier is een bufferlengte als parameter meegenomen en kan een TRUTHSET worden gebruikt. Maar één aspect maakt het REPLACE statement heel krachtig: de TRANSLATETABLE. Een TRANSLATETABLE is in staat om in een klap alle ongewenste karakters uit een buffer te verwijderen bij het kopiëren.

Saillant detail: de bron- en doelpointer mogen gelijk zijn, waardoor het REPLACE statement binnen dezelfde buffer blijkt te werken. Dit is dus veel meer dan een inspectie. Hiermee wordt ook gelijk in een klap de correctie uitgevoerd. Voor de meeste gevallen is dit al snel afdoende. Na een REPLACE bevat de buffer geen ongewenste karakters meer.

Na het uitvoeren van het REPLACE statement bevat de buffer geen ongeldige tekens meer, punt. Zeer krachtig, maar in sommige gevallen ook gebruikersonvriendelijk. Gebruik hangt af van de context.

BOOLEAN 'IN TRUTHSET'-vergelijking

Om het geheel af te maken is het mogelijk om een pointer te testen in een BOOLEAN-expressie tegen een TRUTHSET. Hiermee is snel de tekst waar een pointer naartoe verwijst te toetsen op het bevatten van een uit een reeks karakters. Dit voorbeeld is te zien in het kader TRUTHSET.
Al deze opties zijn beschikbaar op systeemniveau, waardoor ze heel efficiënt zijn in gebruik. Dit zijn slechts eenvoudige voorbeelden, veel complexere tekenmanipulatie is mogelijk.
Met een beetje programmeerdiscipline loop je nooit meer uit een buffer en bevat je buffer nooit meer onverwachte inhoud. De verplichte code-inspectie van je werk zorgde er ook nog eens voor dat je echt op elk invoerveld SCAN en REPLACE gebruikte, zoveel als nodig. Dat deel van de discipline blijft mensenwerk.
Nu bevat lang niet ieder systeem en lang niet elke taal zulke krachtige middelen. Maar in een taal als C, C++ of Java is het zeker mogelijk vergelijkbare functies te introduceren. Ik stel me dan ook voor dat de OWASP code libraries dit soort constructies bevatten. Ik zie daar op het eerste gezicht ook de bewijzen van. Een TRUTHSET is een array van bits, een TRANSLATETABLE een array van karakters, waarbij het invoerkarakter de index in het array is en de gevonden waarde op die positie het uitvoerkarakter is. Dit zijn zaken die ook zo voor een Intel processor eenvoudig gecodeerd kunnen worden. Uiteindelijk komt het neer op programmeerdiscipline, wat niet alleen aan de programmeur zelf moet worden overgelaten.

Het SCAN en het REPLACE statement zijn bij lange na niet het enige securityaspect in een A Series mainframe architectuur. Sterker nog, deze systemen zijn in de jaren 60 en 70 ontworpen met security als een fundamentele pijler. In 1986 hebben de A Series mainframes als eerste lijn van computers een C2-certificatie ontvangen van de NSA tegen het Orange Book, jaren voordat Microsoft Windows dit verkreeg.
Hier is best nog het een en ander over te vertellen, maar dat doe ik dan wel in een volgend artikel.

TRUTHSET

De regel uit het kader SCAN Statement:

```
IF BUFLEN > 0 THEN <throw invalid char exception>;
```

zou vervangen kunnen worden door:

```
TRUTHSET ESCAPECHAR2 ("& \");
...
IF BUFLEN > 0 THEN
  BEGIN
  IF BUFPTR IN ESCAPECHAR2 THEN
    <handle escape> % doe wat extra's bij deze tekens
  ELSE
    <throw invalid char exception>;
  END;
```

Links

Wikipedia: en.wikipedia.org/wiki/Burroughs_large_systems#ALGOL & en.wikipedia.org/wiki/ALGOL_60

OWASP top 10: www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Ponskaarten. Bron: Arnold Rheinhold.

PROFESSIONALS ZIJN ONMISBAAR IN ICT-OPLEIDING

Leo van Koppen is in het dagelijks leven docent aan de opleiding Information Security Management van de Haagse Hogeschool en eenmaal per jaar actief als jurylid voor de verkiezing van het artikel van het jaar van het blad Informatiebeveiliging.

Met de opleiding Information Security Management (ISM) heeft de Academie voor ICT & Media Zoetermeer sinds 2008 een grote troef in handen. De opleiding is uniek in Nederland. Bijzonder binnen deze opleiding is de samenwerking met het bedrijfsleven. Wat levert deze samenwerking op voor studenten, bedrijven en onderwijs? En hoe kijken de studenten nu, twee jaar later, tegen de opleiding ISM aan?

Information Security Management is de enige geaccrediteerde hbo-studie op het gebied van informatiebeveiliging in Nederland. De opleiding loopt nu twee jaar. Studenten leren wat er technisch, organisatorisch en menselijkerwijs nodig is om informatie bij bedrijven te beveiligen. Een niet te onderschatten belang, gezien de opkomst van de informatietechnologie. Studenten krijgen vakken als softwarebeveiliging, risicomanagement, business continuity management, organisatiekunde, ethiek en psychologie. Professionals van drie bedrijven verzorgen een deel van de lessen: Verdonck, Klooster & Associates (VKA) en Vanveen informatica uit Zoetermeer en LBVD Informatiebeveiligers uit Delft.

Maatschappelijke bijdrage

"Lesgeven betekent een maatschappelijke bijdrage leveren. En door het samenspel tussen docent en gemotiveerde student is het ook erg leuk", zegt Dick Leegwater van VKA. "Daarnaast kunnen wij stagiairs alvast beoordelen op hun kwaliteiten om ze na hun stageperiode eventueel in dienst te nemen." Voor Kees Hogewoning van Vanveen informatica is kennis overbrengen de motivatie. "Naast theorie krijgen de studenten nu ook verhalen uit de praktijk."

"Tussen afgestudeerden en professionals zit vaak een grote kloof", vult Rein de Vries van LBVD Informatiebeveiligers aan. "Bovendien stellen organisaties hoge eisen aan toekomstig personeel. Met gastcolleges proberen we die kloof te dichten. En dragen we ook op een andere manier dan commercieel bij aan de maatschappij."

Mystery guest

De studenten beamen dat. "De professionals geven ons een goed beeld van hoe het er in de praktijk aan toegaat en wijzen ons op problemen waaraan wij niet altijd denken", zegt derdejaarsstudent Avinash Kalloe (22). Dat kwam goed naar voren tijdens de opdracht Mystery Guest, waarbij studenten via telefoongesprekken vertrouwelijke informatie lospeuterden bij bedrijven uit het netwerk van VKA, Vanveen informatica en LBVD Informatiebeveiligers. "Bloednerveus was ik", zegt derdejaarsstudent Michel van den Thoorn (23) over de praktijkproef. "Maar met de kennis van de bedrijfscultuur wisten we wie we voor ons hadden en welke tactische vragen we konden stellen."

Social engineering

"Uiteindelijk draait het allemaal om vertrouwen winnen. Heb je eenmaal dat vertrouwen van de receptioniste of wie dan ook, dan komt er interessante en gevoelige informatie naar boven. Denk aan telefoonnummers van medewerkers en de directeur. Zelfs zijn woonadres kreeg ik los", vervolgt Michel. Zo kwam de kwetsbaarheid van een organisatie en de vatbaarheid van medewerkers voor social engineering goed in beeld. Belangrijke input voor de onderzoeksrapportage met conclusies, sterktes/zwaktes en aanbevelingen voor de security awareness van de onderzochte bedrijven.

Onmisbare factoren

Wat de studenten van de gastdocenten hebben geleerd? "Het gaat niet altijd om de techniek. Vaak zorgen juist de menselijke fouten ervoor dat gevoelige informatie letterlijk en figuurlijk op straat komt te liggen. Denk aan een oude computer bij het grofvuil of een memorystick die per ongeluk achterblijft in de trein. Bij het beveiligen van bedrijfsinformatie zijn de ICT, de organisatie en de mens de doorslaggevende factoren. Hoe goed je systemen ook hebt beveiligd, de professionals weten uit de dagelijkse praktijk wel beter en kennen elke valkuil. Zij verbreden onze visie, omdat ze dagelijks met informatiebeveiliging én de valkuilen te maken hebben. Dat maakt ze onmisbaar in de opleiding", concludeert tweedejaars student Marcel van Kleef (23).

Meer dan schoolniveau

Voor tweedejaarsstudent Dennis Buizert (24) was goed presenteren aan de klant de grootste les. "De gastdocenten wensen een scherpe en professionele opbouw van onze rapportage. Ze verwachten immers meer dan 'school-

niveau'. Een dergelijk rapport opstellen leer je echt alleen in de praktijk." Hogewoning zegt daarop: "Je geeft ze een richtlijn mee. Hoe moet je informatie interpreteren? Wat kun je ermee in de praktijk? En welke waarde moet je eraan hechten? Ik wil de studenten in een vroeg stadium meegeven dat ze buiten de kaders moeten denken."

Korte lijnen

Naast de bijdrage van de professionals heeft de academie ook korte lijnen met het Platform voor InformatieBeveiliging, het kenniscentrum op het gebied van informatiebeveiliging in Nederland. Studenten mogen gratis naar thema-avonden waar ze nieuwe kennis opdoen en in contact komen met de beroepsgroep en het bedrijfsleven. Zo hebben de studenten na de opleiding kennis van business continuity management inclusief crisismanagement, risicosignalering, ICT-security en de menselijke factoren die een rol spelen bij informatiebeveiliging. Kennis die voor een information security manager onontbeerlijk is.

Kijkje in de keuken

"De information security manager is een multidisciplinaire deskundige die de organisatie kan beschermen tegen hackers en computerstoringen, maar ook kan voorkomen dat medewerkers vertrouwelijke informatie prijsgeven. Iemand met die kennis staat centraal in de organisatie", vinden alle drie de gastdocenten. De Vries: "Want wat doe je als je al je informatie kwijt bent omdat je bedrijfspand is afgebrand? Waar loop je tegenaan? En hoe pak je calamiteiten op? Dat weten studenten niet altijd. Wij als gastdocenten geven hen met meerdere opdrachten letterlijk een kijkje in de keuken van informatiebeveiliging."

Meerwaarde

In 2012 studeert de eerste lichting ISM-studenten af als information security manager. Inmiddels is al duidelijk geworden dat de samenwerking met het bedrijfsleven een grote meerwaarde heeft voor de studenten én de Academie voor ICT & Media Zoetermeer zelf. Voor de opleiding is de samenwerking een manier om te toetsen of de studie breed en actueel genoeg is. Door het kijkje in de keuken bij de bedrijven blijven de academie en de studenten op de hoogte van bestaande technieken en processen in het bedrijfsleven. De praktijkverhalen van de professionals maken duidelijk waar en wanneer de theorie in de praktijk wordt toegepast, waardoor studenten een goed beeld krijgen van hun toekomstige beroep en de relevantie van de theorie. Dat het intensieve contact met het bedrijfsleven kan resulteren in stage- en afstudeerplaatsen, is een mooie bijkomstigheid.

VOORSTELLEN NIEUW BESTUURSLID CHARLOTTE RUGERS

Tijdens de ALV van 19 april 2011 ben ik als relatief jonge onbekende toegetreden tot het bestuur van deze mooie vakvereniging. Ik stel me graag aan u voor. Mijn naam is Charlotte Rugers en ik ben sinds 2009 werkzaam als security consultant bij Siemens IT Solutions & Services. Al gedurende mijn studie Elektrotechniek was ik geïnteresseerd in security vraagstukken en waterdichte encryptietechnologieën. Na veel theoretisch papierwerk wilde ik na mijn studie meer toegepast aan de slag en koos ik voor de verbreding in het Corporate Traineeship van Siemens. Het bleek echter dat ik mijn grote liefde voor informatiebeveiliging niet kon laten varen en ik besloot om na mijn traineeship weer het pad van informatiebeveiliging te volgen.

De grootste uitdaging in securityland is denk ik, de mens als onzekere factor. Deze mens kiest van nature de weg van de minste weerstand en weet met zijn creatieve geest blokkades te omzeilen. (Informatie) beveiliging wordt door het gros van de mensen gezien als een blokkade of een hindernis. Mijn uitgangspunt is dan ook om beveiliging zo toe te passen dat dit het dagelijkse werk van mensen vergemakkelijkt. Proper security helps the good guys and keeps the bad guys out. Wie de good guys en wie de bad guys zijn, is in onze dynamische wereld altijd een goede basis voor levendige discussies. In mijn vrije tijd wissel ik hierover graag van gedachten net als over andere aspecten die raken aan het totale spectrum van informatiebeveiliging.
Het PvIB is het perfecte podium om van gedachten te wisselen met mensen werkzaam of geïnteresseerd in het vakgebied informatiebeveiliging. Ik draag daarom graag bij aan de volgende professionaliseringsslag van onze vakvereniging. De vereniging heeft mij de portefeuille van de young professionals toevertrouwd en vanuit mijn bestuursfunctie zal ik de commissievoorzitter ondersteunen. Mocht u ideeën hebben of van gedachten willen wisselen, ik begroet u graag tijdens een van onze activiteiten.

DATA QUALITY WITH SOLVENCY II

Karin Küchler is werkzaam als Marketing Manager bij SecondFloor BV, bereikbaar via kuechler@secondfloor.nl, tel: +31 20 6589 700

Karin schrijft over de huidige praktijk van het gebruik van Excel spreadsheets voor bestuurlijke rapportages en de consequenties van deze praktijk bij de invoering van Solvency II voor de verzekeringsbranche in de EU. Het artikel is geschreven in het Engels, maar gezien de actualiteit van het onderwerp willen we het de lezer niet onthouden.

The concept of data quality is as old as data itself and it certainly has gained extra momentum in recent years and months. But while organizations have to put systems in place in order to increase the quality and security of their data, they have to achieve this without neglecting or diminishing the business itself.

Errare humanum est - Automating the process

Generally speaking, human influence is the biggest potential source of mistakes in any operation. The more heavily a process relies on human interaction, the more error-prone it is. One of the most efficient ways to increase the quality of a process is therefore connecting several steps of a process to form a seamless, automated workflow.

Let's look at this concept in more detail: Starting point for a workflow is the input of data. Thanks to developments like ETL (Extract, Transform and Load) and data cleansing, issues like different naming standards can be automatically filtered and addressed, so that all data loaded into the data warehouse adheres to the same rules. Consequentially, a data warehouse offers a simplified view of data, since all information is unified according to an organization's data dictionary. In the next step, this newly formatted data is utilized for modeling and calculations. The resulting report, disclosing management information, is then automatically distributed to managers with the request to approve. Naturally, the extent of a workflow and its degree of automation depends greatly on the nature of the process.

There are two main levels on which such a workflow, and with it the immediate reduction of human input, can be approached:

Firstly, the tools: In any and all business contexts, the use of spreadsheets is considered to be the saving grace regarding data quality. With the correct model or formula, calculations can be done automatically and, provided the input was correct, so will be the results.
All around the world, every single day, thousands of spreadsheets are created, shared and processed, and reports are generated from them. Spreadsheets have become universal tools all over the world; practically everyone uses and relies on them. In the vast majority of cases, Excel is the tool of choice as it is reasonably priced, user-friendly, well established and versatile. But even Excel spreadsheets come with built-in headaches: they're not auditable, anyone with access can tamper with them, and calculations and reporting do not automatically follow a controlled workflow. These crucial deficiencies can cause major errors in calculations – which in return will result in faulty reports. In one famous case in 2003, the reports were US$ 1 billion off target, the deathblow to Fannie Mae, one of the biggest financial institutions in the US.

> Human influence is the biggest potential source of mistakes

Still, abandoning the use of spreadsheets altogether is not unproblematic or often not even feasible, given the associated significant expenses and complications: In addition to the initial purchasing costs of the new software, users need to be trained on the new system, including a long period of extra checks as users are not yet as proficient as they were with the old software. Finally, processes might need to be changed, formulas and models rewritten. All in all, the question of added value versus negative side effects of the innovation is a fundamental one to ask and certainly not an easy one to answer.
At present, Excel's advantages evidently

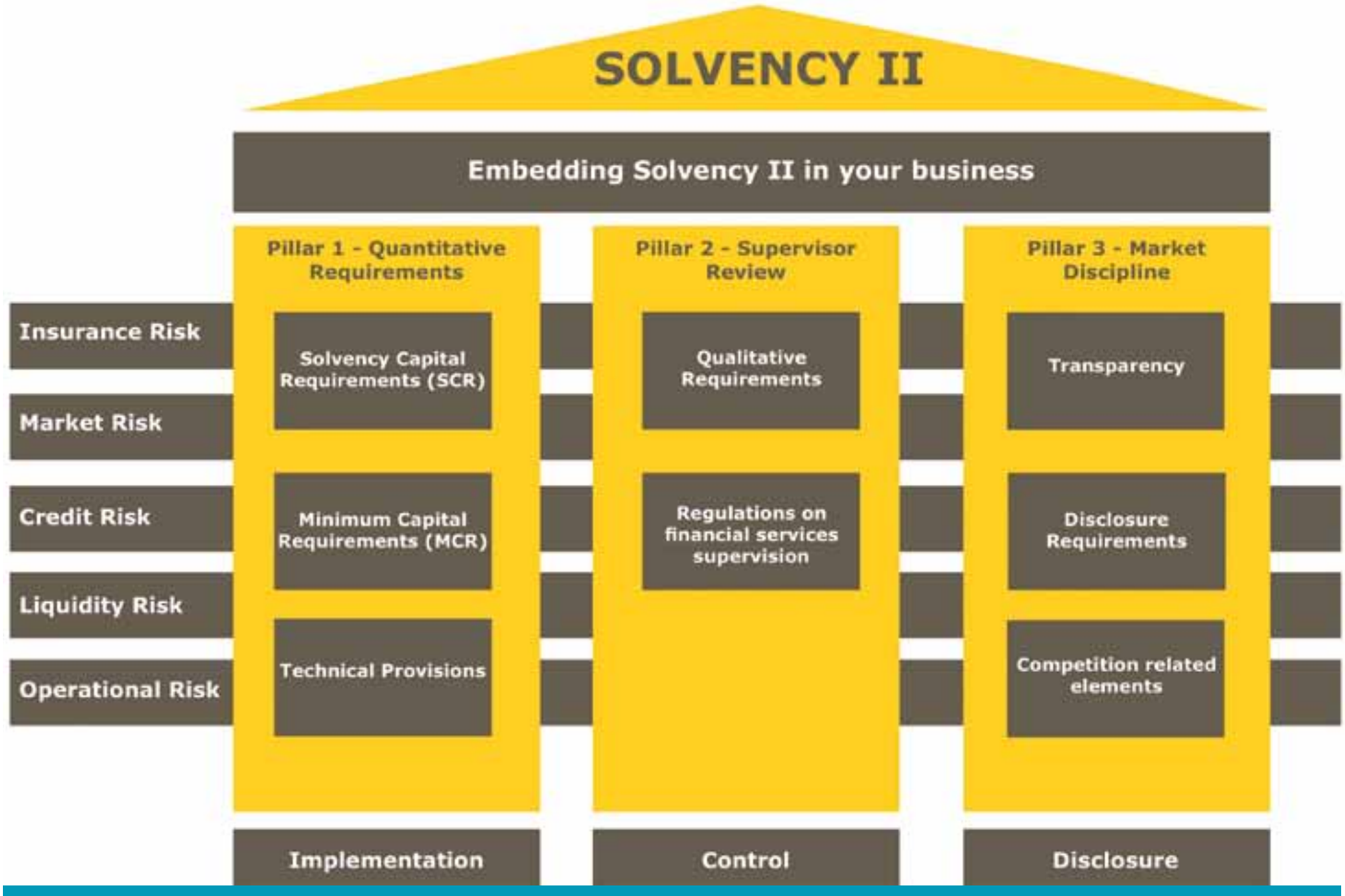
still outweigh its disadvantages, as most organizations are using Microsoft's bestseller rather than competitors' tools more attuned to current regulatory requirements.

Moving on to the other level of workflow automation - the workflow itself. As with any intricate process, the quality of a workflow is largely determined by the way it is configured. Elaborate inside knowledge of the process is mandatory: Who is creating the initial Excel spreadsheet, where do the calculation models come from, who gives input, who needs to check and revise the report and who is eventually going to approve it? Documenting the business processes within an organization is the first step on the road to an end-to-end auditable workflow and facilitates the set-up and execution thereof.
In a nutshell, the challenge of enhanced data quality from the technical side is to take the use of spreadsheets as well as the automation of workflows to a higher level.
Now, for the operational side, let's take a look at the relation of data quality, workflows and Solvency II, an EU directive driving changes in accuracy and completeness in the insurance industry.

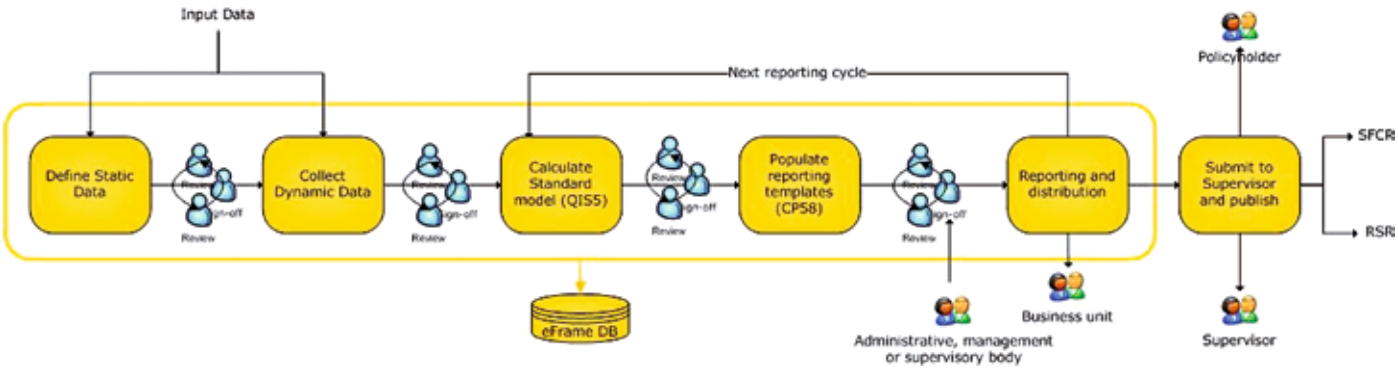
A 101 of Solvency II
No one operating in the insurance industry anywhere within the European Union should be left in any doubt over the far-reaching, mandatory nature of Solvency II. When it is introduced in January 2013, it will completely overhaul the way insurers are assessed for financial soundness.
The four primary aims of Solvency II, the updated set of regulatory requirements for insurance firms in the European Union, are: (1) to provide an early warning system to supervisors so that they can intervene promptly if capital falls below the required level, (2) to reduce the risk that an insurer would be unable to meet claims, (3) to reduce the losses suffered by policyholders in the event that a firm is unable to meet all claims fully and (4) to thereby establish confidence in the financial stability of the insurance sector.
Essentially, Solvency II is forcing the insurance industry to not only measure the risk, but also to go back to the basics – manage the business based on these risks. It forces pockets of control to join together and have a holistic risk view to steer strategic investment decisions - and it relies heavily on data quality.

> Excel spreadsheets come with built-in headaches

The challenge of reporting under Solvency II lies not in the five mandatory reports every year, but more so in the need for senior management and



Embedding Solvency II.



Workflow automation.

the board to really understand how the data in these reports relates to the business. Under the new rules, a regulator can question the meaning of each item in the report, disclosed by the organization.

Moreover, supervisors will ask for evidence and documentation to prove that an insurer is managing data quality. No matter how soundly an organization has set up their data warehouse and workflows, demonstrating the accuracy, completeness and appropriateness of all data will not be an easy task.
In the light of these developments, it is worth taking a closer look at what really constitutes data quality and how it can be ensured.

Data quality revisited
It has become a popular belief that having a centralized data warehouse solution in place is the key to data quality heaven, as all departments feed and draw their information from one single database, which ensures that all data is formatted according to a common naming convention. The fundamental understanding is that everyone working with the same information constitutes data quality… - Unfortunately, it's not all that simple.
Data warehouses are indeed indispensable support pillars for smooth workflows. However, they alone cannot guarantee high quality of all data in a workflow, even when using the most intrinsic data cleansing and ETL tools, as in principle, data quality issues arise as soon as additional information is created from the simplified data in a data warehouse, for example when calculations are performed.
Issues are typically quite stealthy and commonplace. In fact, if you are in the insurance industry, they are happening in your company while you are reading this article.
Consider the following scenario:
A company's CEO is presented with the Profit & Loss report of the previous month. She notices an unusually high amount on a certain item, say, marketing costs. The CEO asks the Financial Director for an explanation – why these costs and are they part of the approved budget? The Financial Director checks the spreadsheet, but ultimately refers to the marketing department, as this is where these costs were generated. The Marketing Manager explains that the item can be traced back to the accumulated paper-based invoices from freelancers who were not using the generally mandatory web-based invoicing system. So these costs were actually spread over several weeks or months, but all come together now that someone has taken the time to retrieve the invoices from the pile of incoming mail.
Sounds familiar? Issues like these arise in small businesses as well as large enterprises, and it is not always easy to get to the bottom of an irregularity. There's much to be said for constant interaction between all parties involved in a reporting process.

Insurance industry has to go back to the basics

Furthermore, the frequency of reporting obviously also plays a part in determining data quality: A higher frequency (e.g. monthly P&L reports) means that potential errors can be caught earlier, but also implies less preparation time and possibly a lower quality of the overall report. Annual reports on the other hand entail that errors can go undetected longer. Having said that, they also implicate more time for governance meetings and more thorough checks of the data.

The essence of data quality is control
Within this article, we have established the fact that it is by no means enough to store all data in one centralized data warehouse. Instead, we have to reach much further: the essence of data quality is to truly gain control of the data.
Important in this context is the concept of a common data dictionary which safeguards that facts and figures will not just be lost in translation. For this, good communication within an organization is needed and data has to be comprehended by its owner.
A popular example for where things can go wrong is the question of the date registration. While Europeans write "day – month – year", in North America, this is reversed into "month – day – year". Imagine the confusion when this difference is not recognized and a deadline set by the American headquarters for 8th January is automatically turned into 1st August at a business unit in France! Similarly, a basic change in terminol-

ogy during the transformation stage, like using the word "price" instead of "rate" or "charge", can bring about misunderstandings, errors and an overall decrease of efficiency.
Whilst diagnostic tools can help, only a workflow including a mandatory sign-off by those who know the data and are aware of the connection to the business (and therefore make or request the necessary corrections) can prevent these errors from happening.

Roles and Responsibilities
When speaking of business processes and workflows, the concept of responsibility is paramount. Responsibilities have to be clearly assigned on all levels of an organization in order to guarantee data quality. In many cases however, this requires a change of culture in an organization. An audit trail, and thereby full transparency on what is done with the data and by whom, necessitates the delegation of responsibility – something not everyone is used to, or will be happy with.

The concept of responsibility is paramount

While clarifying data ownership makes approvers responsible for their actions, it does not provide an enterprise-wide view, as it is required by Solvency II regulations. Therefore, insurance companies require hierarchical overviews. This can be achieved by the introduction of a risk portal, which can cope with the demands of data processing, critical reporting, and the calculation of data flows in a controlled auditable workflow. Embedding a risk portal is a prerequisite for the provision of accurate information, extracted from multiple sources to key parties, analysts, auditors, an organization's board of directors and ultimately external regulators.

In conclusion, data quality is a question of finding the delicate balance between IT and business responsibilities, or in other words, between data security and business efficiency. With the advent of Solvency II, European insurers are faced with the complex task of proving and demonstrating the quality of their data, a task that implicates significant investments both on the technical as well as on the business side of an organization.
The first report under Solvency II is due with the regulators on 14 April 2013, but insurance firms will certainly want to dry run their system prior to this deadline – so there is definitely no time to lose on the winding road to compliancy.

ACHTER HET NIEUWS

In deze rubriek geven enkele van de IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems inzake informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en geeft niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever, of van PvIB. Deze keer heeft de redactie ook een reactie gevraagd aan Ot van Daalen van Bits of Freedom. Vragen en opmerkingen kunt u sturen naar ibmagazine@pvib.nl.

NIETS IS GRATIS.....

EEN PRIVACY KEURMERK OP CLOUD-DIENSTEN, APPS EN SOFTWARE WORDT NOODZAKELIJK

Onder redactie van Ronald van Erven

Er verschijnen steeds vaker diensten en apps die de gebruiker 'iets' gratis geven. Denk hierbij aan Facebook, Twitter en LinkedIn. Maar ondertussen worden via allerlei datamining tools het profiel van personen in kaart gebracht voor allerhande doeleinden. Waaronder niet in de laatste plaats opsporingsdiensten en minder frisse lieden die informatie verzamelen om identiteiten te stelen. Zo is er het voorbeeld van de app WhatsApp waarmee je gratis kan sms'en. Bij de installatie vraagt de app je om een kopie te mogen maken van je gehele adresboek. Natuurlijk krijgen je vrienden een e-mailtje of sms om WhatsApp ook te gebruiken. Maar wat doet WhatsApp nog meer met ieders adresboek? Het is bekend dat de Amerikaanse overheid apps maakt om mensen te profileren. En er is Amerikaanse wetgeving die beslist dat informatie op Amerikaanse bodem toegankelijk moet zijn voor die overheid.
Moeten deze diensten en software worden voorzien van een classificatie naar analogie van kijkwijzer? Of zouden dit soort apps in de itunes- of android-store moeten worden voorzien van een classificatie waarmee de software een aanduiding krijgt dat persoonsgegevens worden verzameld?

Maarten Hartsuijker:
"Wat kan mij dat nou schelen!". Nee, dit is niet hoe ik denk over de stelling van deze Achter het nieuws. Dit is de reactie die ik van een vriend kreeg toen ik hem uitlegde dat zijn smartphone op het punt stond om de gegevens van zijn vrienden automatisch aan derden te verstrekken.
Laten we als beveiligers eerlijk zijn. We maken ons druk over een onderwerp dat het gros van de mensen niet zo heel erg veel kan schelen. Facebook, Twitter, WhatsApp, Gmail en LinkedIn zijn volledig ingeburgerd. En we maken massaal en met liefde gebruik van de adresboeken en de automatische vriendencheckers die de verschillende sites aanbieden. Waarom? 'Makkelijk' is nou eenmaal veel aantrekkelijker dan 'voorzichtig en omslachtig'. En tot nu toe gaat er weinig mis, toch?
Een privacywijzer zal ongetwijfeld helpen om de privacyconsequenties voor de doorsnee gebruiker inzichtelijker te maken. De vraag is echter of we hier op een effectieve wijze voldoende gedragsverandering mee tot stand zullen brengen. Het gemak dat de applicaties bieden blijft ongetwijfeld hoe dan ook gebruikers trekken.
Persoonlijk zou ik het toejuichen als bedrijven verplicht zouden worden gesteld om eigenaren van een e-mailadres of telefoonnummer inzicht te geven in waar dat gegeven aan is gerelateerd. Met hetzelfde gemak als waarmee je een account op een website aanmaakt, zou je door anderen aangeleverde gegevens over jezelf moeten kunnen inzien en verwijderen. Een utopie? Wellicht, maar het is wel een van de weinige oplossingen die de controle daar belegt waar hij hoort namelijk, bij de eigenaar van de gegevens.

Gerrit Post:
Applicaties voor smartphones classificeren naar de mate waarin ze slordig met onze privacy omgaan? Een interessante gedachte? Nou nee, dank u. Waarom niet? Simpel. In dit geval hanteren we namelijk, ben ik bang, niet een wel overwogen risicoanalyse op basis waarvan we een goede conclusie kunnen trekken maar leidt 'harvesten' tot een Pavlov-reactie die het gebruik van een dergelijke app verbiedt. Verklaarbaar, begrijpelijk, maar wat mij betreft nog steeds onterecht. Het ligt een beetje in de sfeer van de EHEC-bacterie in Duitsland. 'Men' hoort

'bacterie', verneemt dat er mensen aan dood gaan en de gehele Nederlandse komkommeroogst van een aantal maanden kan worden weggegooid. Als het aantal doden in het verkeer een dergelijke reactie teweeg zou brengen, reed er niemand meer. Idem voor roken en alcohol.

Is mijn privacy in het geding bij gebruik van WhatsApp? De nietszeggende teksten die ik er over uit en wat ik terug krijg kunnen weinig kwaad. Ligt mijn adresboek nu ergens in de States? Vast wel, maar dat lag het toch al wel, daar maak ik me geen illusies over. En nog zoiets, we 'moeten' met z'n allen aan de Cloud. Dat die Cloud in diezelfde States (en waarschijnlijk elders ook) dus gewoon getapt kan worden door de instanties, daar hoor ik niemand over. Hoezo privacy? Zijn de kroonjuwelen van een gemiddeld bedrijf niet veel belangrijker dan mijn adresboek? Een kwart van dat adresboek bestaat overigens uit contacten die jaarlijks van telefoonnummer wisselen. Desinformatie dus! Dat zal 'ze' leren. Het gebruik van WhatsApp-achtigen is wat mij betreft alleen echt een probleem voor de mensen die hun baan verliezen omdat ik straks geen sms-bundel meer heb. Sorry!

Rachel Marbus: WhatsApp is kewl. Het staat al op m'n iPhone direct nadat de app beschikbaar kwam. Toen gebruikte slechts 1 persoon die ik kende het (2 jaar geleden inmiddels). Nu is de lijst gegroeid naar bijna 60. En nee, dit zijn geen mensen die ik zelf heb toegevoegd. Dit zijn mensen die WhatsApp installeerden en het gingen gebruiken. Die dus zelf akkoord gingen met het gebruiken van hun gegevens. En nee, je hoeft helemaal niemands gegevens door te geven aan WhatsApp. Dat kan wel, maar het hoeft niet. Ik heb dus ook nimmer iemand een sms laten sturen met de vraag of ze samen met me wilden gaan WhatsApp'en. Ik heb ooit een sms-verzoek mogen ontvangen en die persoon heb ik niet toegevoegd. Ongevraagd mijn gegevens delen vind ik namelijk niet kewl. Ik gooi ze liever zelf te grabbel. Overigens zijn de algemene voorwaarden zeer lezenswaardig. Voor vakidioten zoals ik is het smullen. Het is een prachtig voorbeeld van ontzettend Amerikaanse 'wij sluiten overal aansprakelijkheid voor uit'-taal. Alleen al over het zinnetje dat gebruikers kunnen toevoegen als hun statusbericht is een clausule opgenomen met zes (!) paragrafen. 1049 woorden gewijd aan 1 zinnetje. Ik vind het ge-wel-dig! Ik geloof dat dit ook wel een beetje aangeeft wat er mis gaat. Er is, mijns inziens, sprake van een juridische clash tussen twee totaal verschillende werelden, de Amerikaanse en de Europese. Wij gaan anders om met juridische zaken en staan moreel anders in dit soort kwesties. Overigens staat er ook dat 'adult content must be identified as such'. Dat u het even weet als u weer een leuk fotootje WhatsAppt naar uw lief…

Ot van Daalen: Op grond van de wet moeten bedrijven hun gebruikers al duidelijk informeren als ze privégegevens over hun klanten verwerken. In veel gevallen moeten ze ook toestemming van de gebruiker krijgen voor die verwerking. In de praktijk informeren bedrijven gebruikers echter meestal via algemene voorwaarden. In lange zinnen leggen bedrijven precies uit wat ze met je privégegevens doen. Als je dat op je smartphone bekijkt, moet je soms door tientallen pagina's scrollen. Het verbaast me dan ook niet dat weinig mensen die algemene voorwaarden goed lezen. Goed ontworpen icoontjes kunnen in een oogopslag duidelijk maken wat er met jouw gegevens gebeurt. Worden je gegevens opgeslagen in de VS? Worden je gegevens doorverkocht aan derden? Maar het zal nog niet zo eenvoudig zijn om alle mogelijkheden in heldere icoontjes vast teleggen. En daar schuilt ook een belangrijke adder onder het gras. In de praktijk kan een simpel icoontje de complexere privacyreglementen niet goed weergeven. En het mag natuurlijk nooit zo zijn, dat dit soort icoontjes in de praktijk leiden tot misleiding van de gebruiker. Daarom staat of valt zo'n systeem met de manier waarop het wordt ingestoken.

De vervolg vraag is: "Wie zou die icoontjes gaan gebruiken?" Daarin is de wet helder. Het is aan bedrijven die jouw persoonsgegevens verwerken, zoals ontwikkelaars van applicaties voor mobiele telefoons, om te zorgen dat gebruikers goed worden geïnformeerd. De bedrijven die dat nu nog niet goed genoeg doen die overtreden de wet. De beheerders van Appstores zouden daarin een begeleidende rol kunnen spelen, door aan te geven wat een app met jouw gegevens doet. Maar dat kan de verantwoordelijkheid van de app-ontwikkelaars nooit wegnemen. Zij moeten helder uitleggen wat met jouw gegevens gebeurt, en zij moeten toestemming vragen voor verwerking als dat nodig is. Dat betekent dat ze je ook op een /begrijpelijke/ manier moeten informeren. Maar of app-developers jou nou via geluid, tekst of beeld informeren, het gaat er uiteindelijk om dat de gebruiker direct begrijpt wat er met zijn informatie gebeurt. Goede informatie staat voorop.

DE VOLGENDE STAP IN APPLICATIEBEVEILIGINGSONDERZOEKEN

Ing. M. (Michiel) van Veen RE MSc. CISA CISSP is als adviseur bij KPMG IT Advisory werkzaam in de groep Information Protection and Business Resilience. Michiel is specialist op het gebied van IT-beveiligingsadvies, IT auditing, IT-beveiligingsonderzoeken en penetratietesten. Zijn kennisgebied reikt van IT Governance tot technische beveiligingsimplementaties in detail: from board to bit. Hij is te bereiken via vanveen.michiel@kpmg.nl.

De laatste jaren neemt het aantal IT-beveiligingsincidenten sterk toe. Recente berichten over inbraken bij de FBI, CIA, Amerikaanse Senaat en bedrijven als Sony en Nintendo laten de ernst zien van deze dreiging. Dergelijke incidenten bevorderen het bewustzijn dat in vrijwel elk apparaat software zit. Van horloge tot spaceshuttle, alles wordt bepaald door software. Hierdoor ontstaat de behoefte om meer controle te krijgen en te houden op beveiliging in applicaties en het pad naar de data die het ontsluit, om zo te bewaken dat de software precies doet wat het moet doen en niet wat het niet moet doen.

Om meer controle te krijgen over de applicatiebeveiliging is het noodzakelijk inzicht te krijgen in de aanwezige maatregelen en de benodigde maatregelen. Typisch worden applicatiebeveiligingsonderzoeken uitgevoerd om dit in kaart te brengen. In een applicatiebeveiligingsonderzoek staan de IT-controlemaatregelen centraal en daarmee dus de (functie) scheiding tussen verschillende (gebruikers)groepen. Een veel gehanteerde scheiding is die tussen eindgebruikers, beheerders en ontwikkelaars.

- Ontwikkelaars staan aan de basis van de behoeftevoorziening naar de gebruikers. Zij vertalen de wensen en eisen in ondersteunende software. Daarmee dragen zij de verantwoordelijkheid om te zorgen dat de software correct werkt.
- Beheerders zorgen ervoor dat de software in het IT-landschap wordt opgenomen. Daartoe configureren zij de software en eventuele ondersteunende IT-infrastructuur zoals databases, servers en netwerk. Dit wordt zodanig uitgevoerd dat de eindgebruikers op de juiste manier toegang krijgen tot de software.
- De eindgebruikers zetten de software in voor de ondersteuning van de uit te voeren taken en maken zo dus gebruik van de software en de daarin besloten data.

Om de scheiding tussen deze groepen te implementeren is het belangrijk het pad van de gebruiker naar de data onder controle te hebben. Met behulp van bijvoorbeeld authenticatie- en autorisatiemiddelen zoals een gebruikersnaam en wachtwoord, wordt de scheiding technisch afgedwongen. Een applicatiebeveiligingsonderzoek richt zich op de technisch afgedwongen scheidingen. Typisch worden configuratiereviews en penetratietesten gebruikt voor het onderzoek.

Fig. 1. De nadruk van een applicatiebeveiligingsonderzoek ligt meer op IT-beheer in plaats van softwareontwikkeling.

Configuratiereviews hebben tot doel te valideren of alle instellingen de juiste scheidingen technisch afdwingen.Voor veel gebruikte software (zoals Windows besturingssystemen of Oracle databases) worden zogeheten beveiligingsconfiguratiebaselines gebruikt. Deze baselines zijn in feite controlelijsten met configuratie-instellingen zoals die geïmplementeerd moeten zijn. Afwijkingen kunnen soms leiden tot het doorbreken van de scheidingen en daarmee tot ongeautoriseerde toegang tot de software en data. Penetratietesten hebben tot doel inzicht te verschaffen in de aanwezige beveiligingszwakheden. Vaak wordt hiertoe met speciale applicaties en IT-beveiligingspecialisten (ethical hackers) getracht zwakheden te identificeren door de software op zowel gebruikelijke als ongebruikelijke manieren te benaderen. De controles in de software worden omzeild, waardoor ongeautoriseerd toegang wordt verkregen tot de software en data.

Configuratiereviews richten zich vooral op de beheerders. Bevindingen uit dit type onderzoek richten zich op het afdwingen van controle vanuit de software naar de eindgebruiker. Deze worden vervolgens naar beheerders gecommuniceerd die de nodige aanpassingen doorvoeren in de IT-infrastructuur. Verder dragen zij zorg voor de periodieke controle van deze instellingen en waarborgen zo de effectiviteit van de maatregelen over tijd.
Penetratietesten richten zich vooral op de eindgebruikers. Bevindingen uit dit type onderzoek richten zich op de mogelijkheden die de eindgebruiker heeft in de

interactie met de software. Ook deze bevindingen komen uiteindelijk terecht bij beheerders die de nodige maatregelen implementeren of aanscherpen. Daarnaast worden bevindingen die voortkomen uit fouten in de software zelf gecommuniceerd naar de ontwikkelaars. Kortom, de bovenstaande onderzoeksmethodes laten zien dat veel nadruk ligt op het beheren van IT en minder op softwareontwikkeling. Dit is vreemd aangezien juist de softwareontwikkeling bepaalt in welke mate vereiste controlemaatregelen technisch worden afgedwongen in de source-code. Om in de behoefte van meer controle over applicatiebeveiliging te voorzien, dient ook de source-code zelf te worden onderzocht. Fig.1. geeft het onderzoeksgebied duidelijk aan.

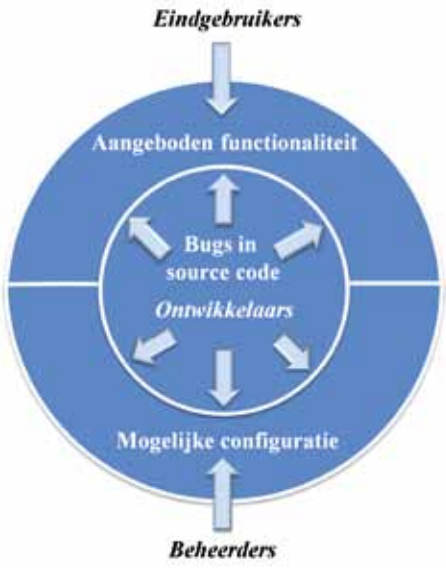


Fig. 2. Bugs in de source-code hebben een grote invloed op de applicatiebeveiliging.

Source-code en haar rol in de applicatiebeveiligingsproblematiek

Applicaties worden geschreven door een softwareontwikkelaar waarbij deze de wensen en eisen van de opdrachtgever in een ontwerp van source-code vertaalt. Die source-code wordt geschreven door ontwikkelaars die daarmee bepalen wat de applicatie wel en niet doet. Het is dus belangrijk vast te stellen dat de applicatie aan de wensen en eisen voldoet. De applicatie moet doen wat zij belooft. Dit lijkt triviaal maar dat is het niet. Immers, een applicatie wordt geschreven door mensen en die maken soms fouten. Deze fouten (bugs) kunnen ervoor zorgen dat de applicatie zich anders gedraagt dan verwacht. Omdat een applicatie al vrij snel complex wordt door de vele commando's in de source-code en hun onderlinge samenhang en afhankelijkheden, is een bug snel geïntroduceerd. Bovendien zijn bugs door de complexiteit moeilijk op te sporen. Een softwareontwikkelaar moet immers beredeneren hoe een computer in een bepaalde situatie omgaat met het opgegeven commando. Ook het vervolgens verhelpen van bugs is geen sinecure. Zeker bij grote applicaties is het vrijwel onmogelijk alle bugs in de software te ontdekken en te verhelpen.

De invloed van bugs op applicatiebeveiliging

Het valideren van de beoogde functionaliteit (eisen en wensen) ten aanzien van de applicatie is nog relatief eenvoudig. Ingewikkelder wordt het om vast te stellen dat de applicatie ook niet doet wat ze niet belooft. Biedt de applicatie meer mogelijkheden aan voor eindgebruikers om data te benaderen dan de bedoeling is? Bijvoorbeeld zonder authenticatie en autorisatie? Of biedt de applicatie, zonder dat het de bedoeling is, toegang tot onderliggende IT-infrastructuur (databases, servers en netwerk)?
In applicaties speelt controle dus een belangrijke rol. Een belangrijk aspect van de controle is het vaststellen of een gevraagde actie wel is toegestaan. Alleen op die manier is het mogelijk preventief te garanderen dat de computer op een juiste manier reageert op een verzoek en zo dus doet wat hij belooft. Daarmee is het authenticeren en autoriseren van gebruikers en hun acties een belangrijke functionaliteit binnen een applicatie. Met authenticatie en autorisatie kan een organisatie controle uitoefenen op bijvoorbeeld het aanpassen van financiële data, het lezen van vertrouwelijke gegevens of het beschikbaar houden van systemen. Vaak maakt een organisatie een vertaalslag van rollen en verantwoordelijkheden en voert deze door in de applicatie.
Het testen van de authenticatie en autorisatiemechanismen in een applicatie is een belangrijk onderdeel van een applicatiebeveiligingstest. Bugs in de authenticatie- en autorisatiemechanismen kunnen het gebruik van de applicatie ondermijnen omdat de scheidingen tussen gebruikers onderling wordt doorbroken. Daarmee wordt feitelijk het model van rollen en verantwoordelijkheden uit de organisatie doorbroken. Dat dit een impact kan hebben op de beveiliging blijkt uit de vele fraude-incidenten, privacyschendingen en recente beschikbaarheidproblemen van websites. Een recent voorbeeld is het stelen van meer dan 130.000.000 creditcardnummers van de betalingsverwerker Hartland door een aanval van buiten het bedrijf. [ITA,2010]
Naast bugs die een functioneel karakter hebben zoals authenticatie- en autorisatiemechanismen, zijn er ook non-functionele bugs. Een bekend voorbeeld is het gebrek aan invoervalidatie. Afhankelijk van het gebruik van deze invoer in de applicatie kan dit grote beveiligingsgevolgen hebben. Wanneer de ongevalideerde invoer bijvoorbeeld wordt gebruikt om een achterliggende database te bevragen, kan de gebruiker zelf extra database-commando's (SQL) toevoegen en zo ongeautoriseerd alle data opvragen, aanpassen of verwijderen. Hierdoor kan een gebruiker alle controles in de applicatie omzeilen. Neem als voorbeeld een salarisadministratie. De software zorgt ervoor dat personeel dat de salarisbetaling uitvoert niet dezelfde medewerkers zijn als diegene die de betaling controleren en autoriseren: functiescheiding. Wanneer een gebruiker de invoervalidatiebug misbruikt kan hij zelf de salarisbetaling direct via de database doorvoeren en omzeilt daarmee alle controles met alle gevolgen van dien.
Een top-10 lijst van veelvoorkomende

Zeker bij grote applicaties is het vrijwel onmogelijk alle bugs in de software te ontdekken en te verhelpen

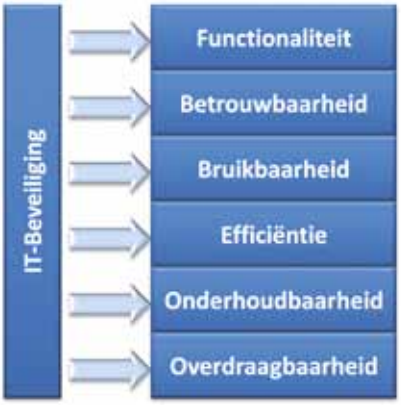


Fig. 3. IT-beveiliging is van toepassing op elk van de zes aspecten van de softwarekwaliteit ISO-norm.

applicatiefouten is terug te vinden in de OWASP top 10 [OWASP,2010].
Kortom, de source-code heeft grote invloed op applicatiebeveiliging. Fig. 2. laat duidelijk zien welke invloed de bugs in source-code hebben op de applicatiebeveiliging. Dit betekent dat het belangrijk is om in een applicatiebeveiligingsonderzoek ook onder de motorkap te kijken van de software om de interne werking vast te stellen, een source-codeonderzoek.

Het uitvoeren van een source-codeonderzoek

De aanpak voor het onderzoeken van source-code is sterk afhankelijk van de vereiste breedte en diepgang.Twee bekende aanpakken zijn het onderzoeken van de kwaliteit van software en source-code reviews.
Een bekende invulling van de kwaliteit van software is gegeven in de ISO-norm 9126. De norm verdeelt de kwaliteit van software op basis van de volgende kenmerken: functionaliteit, betrouwbaarheid, bruikbaarheid, efficiëntie, onderhoudbaarheid en overdraagbaarheid. Door het onderzoeken van deze aspecten ontstaat het beeld of men kan vertrouwen op de software. Daarmee beslaat dit onderzoek meer dan de source-code alleen. De kwaliteit van de software wordt in zijn geheel bekeken. Zo wordt deze aanpak ook vaak gebruikt om de software te koppelen aan de (beheer)kosten daarvan, omdat software met lage kwaliteit veel en moeizaam onderhoud vergt.
In de ISO-norm is applicatiebeveiliging als aspect gehangen onder 'functionaliteit'. Deze classificering staat in contrast met die van functionele en non-functionele eisen. Applicatiebeveiliging kan namelijk zowel functionele als non-functionele eisen hebben. Een functionele eis is bijvoorbeeld als een gebruiker moet zich kunnen authenticeren met behulp van een gebruikersnaam en wachtwoord. Een non-functionele eis is als het wachtwoord opgeslagen dient te worden met behulp van een one-way-hash-functie. Dit betekent dat applicatiebeveiliging niet te plaatsen is onder 'functionaliteit' in de ISO-norm. Wanneer applicatiebeveiliging met de softwarekwaliteittaxonomie wordt vergeleken, blijkt dat applicatiebeveiliging op elk van de zes kenmerken invloed heeft en dus als integraal onderdeel van softwarekwaliteit beschouwd dient te worden. Daarmee heeft de implementatie van de applicatiebeveiliging in software een grote invloed op de kwaliteit van de software en dus op het functioneren van de software in brede zin. In fig.3. is de positie van IT-beveiliging weergegeven in relatie tot de ISO-norm-aspecten.
Source-code reviews richten zich op de diepgang en minder op de breedte. Het reviewen van source-code specifiek voor applicatiebeveiliging is minder bekend dan softwarekwaliteitsonderzoeken. Praktische methodes die zich op applicatiebeveiliging focussen zijn [McGraw,2001] [McGraw,2004] [McGraw,2006]. Bij het reviewen van source-code wordt onderscheid gemaakt tussen kwantitatief en kwalitatief onderzoek. In een kwantitatief onderzoek worden vaak aspecten bekeken zoals complexiteitsmetrieken, codeduplicatie, functiegroottes, overervingen in objectenstructuren enz.

> Het is belangrijk om in een applicatiebeveiligingsonderzoek ook onder de motorkap te kijken: source-codeonderzoek

Met behulp van tools wordt de volledige source-code doorgelicht en worden statistische berekeningen gemaakt. De uitkomst geeft vaak goede handvatten in een onderzoek naar de beheerbaarheid, overdraagbaarheid en uitbreidbaarheid van de software.
Kwalitatieve onderzoeken worden veelal met de hand uitgevoerd waar een specialist de source-code in de diepte onderzoekt. Voor een applicatiebeveiligingsonderzoek betekent dit, dat kwetsbaarheden worden gezocht die de beveiliging kunnen beïnvloeden. Zoals eerder besproken kan applicatiebeveiliging functioneel en non-functioneel worden geïmplementeerd. In een source-code review is het belangrijk om beide benaderingen mee te nemen.

- De eerste stap in het onderzoek is een lexicale analyse. In deze stap wordt onderzocht of de source-code gestructureerd is, alles goed is gedocumenteerd in de code, programmeerstandaarden worden toegepast, variabelendeclaraties consistent zijn en de code goed leesbaar is.
  De lexicale analyse geeft een eerste indruk van de source-codekwaliteit en mogelijke probleemgebieden.
- De tweede stap in het onderzoek is de control flow relation analyse. In

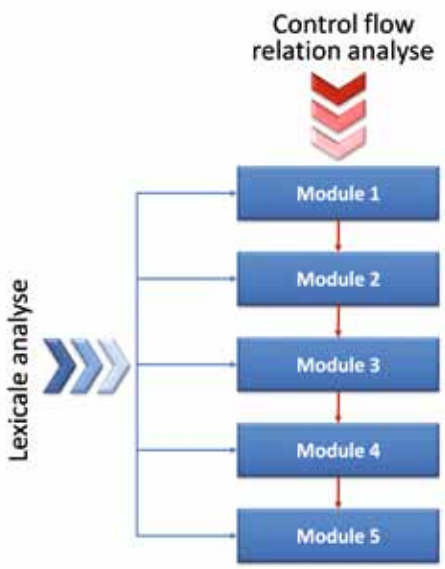


Fig. 4. De relatie tussen lexicale analyse en control flow relation-analyse van de source-code.

deze stap loopt de onderzoeker door de source-code heen op basis van de functieaanroepen in de applicatie. Zo worden de stappen gevolgd die de applicatie zelf doorloopt bij het uitvoeren van acties. De nadruk ligt op aspecten als foutafhandeling, (technische) aannames, design patterns, code hergebruik en logische objectstructuren.

De control flow relation analyse richt zich op de keten als geheel. De lexicale analyse op iedere schakel in die keten. In fig. 4. is deze relatie goed te zien. De resultaten uit beide stappen leveren een goed overzicht op van beveiligingskwetsbaarheden veroorzaakt door de manier van source-code schrijven of door de functionele samenhang van applicatieonderdelen.

Source-codeonderzoek als onderdeel van een applicatiebeveiligingsonderzoek
Zoals besproken bestaat het uitvoeren van een applicatiebeveiligingstest typisch uit een penetratietest, eventueel gecombineerd met een configuratiereview. Een source-codereview is geen vervanging van deze aanpak maar juist een belangrijke aanvulling daarop. Deze aanvulling helpt bij het identificeren van meer en complexe kwetsbaarheden in applicaties binnen een kortere tijd. Dit is duidelijk te zien in fig.5.
Het uitvoeren van een source-codereview in het kader van een applicatiebeveiligingstest kan op twee manieren worden ingezet.

- *Bottom-up-aanpak*
  In een bottom-up-aanpak wordt eerst begonnen met het analyseren van de source-code. Daarmee worden mogelijke zwakheden geïdentificeerd. Deze zwakheden worden vervolgens in een penetratietest gevalideerd. Hierdoor worden 'false-positives' eruit gehaald.

- *Top-down-aanpak*
  In een top-down-aanpak wordt eerst begonnen met een penetratietest. Wanneer vermoedens bestaan van een beveiligingslek, dan wordt de desbetreffende source-code opgezocht. In de source-codeanalyse wordt vervolgens gevalideerd of er sprake is van een beveiligingslek.

De keuze van de aanpak hangt samen met het doel van de applicatiebeveiligingstest. Wanneer het doel van de test is om zoveel mogelijk beveiligingslekken op te sporen en hiervoor aanbevelingen aan te dragen, dan is een bottom-up-aanpak het meest geschikt. Door het integraal analyseren van de source-code worden alle mogelijkheden geïdentificeerd en reële dreigingen zichtbaar gemaakt met een penetratietest.

Top-down en bottom-up: wat kan een anonieme hacker in een realistische situatie doen?

Wanneer het doel is om vast te stellen wat een anonieme aanvaller zou kunnen (ontdekken) is een top-down-aanpak logischer. Immers, de anonieme aanvaller heeft geen beschikking over de source-code (afhankelijk van het open source-karakter) en zal die dus niet als basis gebruiken. Wel kan de source-codeanalyse worden gebruikt om de efficiëntie van de penetratietest te verhogen. Bij een penetratietest is de tijd vaak gelimiteerd, terwijl een echte aanvaller meer tijd en resources tot zijn beschikking heeft.
Het is verstandig om de top-down- en bottom-up-aanpak te combineren. Hierdoor worden zoveel mogelijk beveiligingskwestbaarheden ontdekt en wordt tevens bepaald wat een anonieme hacker in een realistische situatie zou kunnen doen. Samen met een configuratiereview kan de applicatiebeveiligingstest compleet worden gemaakt.

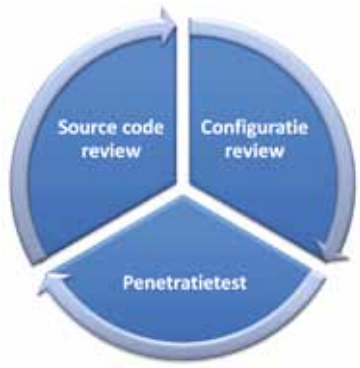


Fig. 5. Het verband tussen een penetratietest, configuratiereview en een source-code review.

Conclusie
Traditionele benaderwijzen van penetratietesten en configuratiereviews voor het testen van applicatiebeveiliging komen onder druk te staan door het toenemend aantal inbraakpogingen op applicaties. Dit stimuleert de vraag naar een aanvulling in de huidige aanpak: source-code-review. Door een source-codereview kan applicatiebeveiliging, als belangrijke invloed van de softwarekwaliteit, verder worden beheerst. Dit voorkomt dat eindgebruikers de software anders laten gedragen (manipulatie) of de software meer laten doen dan de bedoeling is (injectie). Net als de voor de hand liggende functionele en non-functionele eisen, dienen ook applicatiebeveiligingseisen expliciet te worden opgesteld aan het begin van de software-ontwikkelcyclus. Dit waarborgt dat de applicatiebeveiliging al tijdens de software-ontwikkeling wordt getest. Met voldoende aandacht voor applicatiebeveiliging en in juiste balans met gebruikersvriendelijkheid wordt zo veiligere software ontwikkeld en gebruikt. Daarmee kan de samenleving verder steunen en vertrouwen op een juiste ondersteuning door software.

Literatuur

Identity Theft Awareness. 2010 Security Incidents, www.identity-theft-awareness.com/2010-security-incidents.html, 2010

ISO/IEC 9126-1:2001. Software engineering - Product quality - Part 1: Quality model. www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22749, 2011

McGraw et al. Secure Software: How to Avoid Security Problems the Right Way, 2001

McGraw et al. Exploiting Software: How to Break Code, 2004

McGraw et al. Software Security: Building Security In, 2006

OWASP. OWASP top 10,www.owasp.org, 2010

TAGOLOGY, ÉÉN TAAL VOOR ALLES

VOOR PRODUCTLOGO'S, BEWEGWIJZERING, WACHTWOORDEN EN COMMUNICATIE IN NOOD

Christian van 't Hof, chairman tagology

Stel je voor: één taal voor alle mensen en computers. Een taal bovendien waaraan iedereen kan bijdragen en die je leert terwijl je hem gebruikt op een mobieltje of pc. Stichting Tagology streeft een hoge ambitie na: bits gebruiken als pictogrammen, oftewel 'tags'.

Het maken en gebruiken van deze tags is gratis en staat open voor iedereen. Een heel verhaal schrijven is wellicht wat te hoog gegrepen maar de tags zijn goed te gebruiken als bijvoorbeeld productlogo's en bewegwijzering. Tags kunnen ook zeer geschikt zijn als wachtwoorden. Ze zijn gemakkelijk te onthouden en lastig te kraken. En, in het scenario waarbij internet (tijdelijk) uitvalt, hetgeen niet geheel ondenkbaar is met de recente discussie over zogenaamde 'kill switches', kan Tagology een begin vormen voor een alternatieve vorm van communicatie. Ondertussen leren wij veel over hoe mensen communiceren met machines en elkaar.

Hoe werkt het?

Tagology is een lees- en schrijftaal van pictogrammen die zijn opgebouwd als matrix code, oftewel een tag. In de meeste talen kun je redelijk goed communiceren met 10.000 woorden. De tag bestaat uit 30 vakjes. Elk vakje is één bit. Een zwart vlakje is een 1, een witte een nul, net als bij barcodes. Daarmee kun je 230, oftewel 1.073.741.823 mogelijke tags maken. Daarvan zijn de meeste uiteraard niet echt gemakkelijk herkenbaar als beeld, maar al spelenderwijs ontdekken we dat enkele duizenden duidelijke pictogrammen zeker haalbaar zijn. Dat moet genoeg zijn, want een echte roman kun je toch nog steeds beter in het huidige schrift lezen.

Een tag staat voor een woord, letter of teken. Sommige tags zijn vrijwel direct herkenbaar omdat het een bestaand teken of pictogram is. Soms kunnen ook Chinese of Japanse tekens worden gebruikt.

Fig. 1. Voorbeelden van tags.

De meeste tags zijn nieuw voor de gebruiker en moeten daarom worden aangeleerd. Ken je de tag niet, dan kun je die uitlezen met een scanner, de digitale camera op een telefoon of een webcam. Heb je een tag een paar keer gescand, dan herken je hem waarschijnlijk de volgende keer. Tagology leer je dus terwijl je het gebruikt.

Wat kan je ermee?

Tagology is vooral bedoeld voor praktische, korte berichten. Omdat het alleen een lees- en schrijftaal is, zal het echter nooit bestaande talen kunnen vervangen. Maar, onder omstandigheden waarin (elektronische) communicatie wordt bemoeilijkt of waar een wildgroei aan concurrerende betekenissystemen heerst, kan het op een basale wijze een alternatieve methode van communiceren bieden. Hieronder enkele praktische voorbeelden.

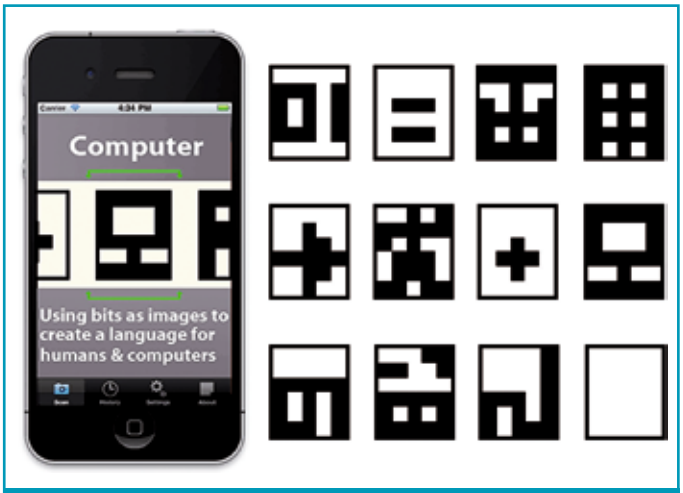


Fig. 2. De Tagology App leest: 'bits = plaatje gebruik → mens + computer van taal ontwikkelen.' Oftewel, we gebruiken bits als plaatje om een taal te ontwikkelen voor mens en computer.

Logistiek

Stel, een bedrijf uit Shanghai verstuurt regelmatig pakketjes naar Bangelore, Osaka, Bangkok en weer terug. Vier steden met elk een ander schrift en mensen die niet altijd bereid zijn elkaars taal te leren. Scanners bij de in en uitgaande post lezen de tags, automatiseren de verhandeling en vertalen de nodige boodschappen over de inhoud, bestemming en instructies over de inhoud. De veelgebruikte tags worden

op een gegeven moment vanzelf door de werknemers herkend.

Wachtwoorden

We hebben steeds meer wachtwoorden nodig en de eisen aan de complexiteit van wachtwoorden worden ook steeds strenger. Een redelijk standaard wachtwoordbeleid vereist vaak de opname van een vreemd teken, een cijfer en het gebruik van kapitalen. Dit alles dan ook nog liefst met een minimum van 6 tekens in totaal (liever 8) en elke vier maanden gewijzigd. Hoe goed het wachtwoordbeleid van een organisatie ook is, mensen blijken over het geheel genomen moeite te hebben met het onthouden van lange wachtwoorden. Tagology leent zich er goed voor om hieraan tegemoet te komen. Een plaatje is immers gemakkelijker te onthouden dan een heel woord en is tegelijkertijd een ingewikkelde code. Typ het plaatje in op een touchscreen of op een Tagology toetsenbord (5x6 knoppen en een enter toets) om een deur of account te openen. Eén tag geeft al 230 mogelijkheden. Drie plaatjes 290. Dat is een erg lang wachtwoord! Is dat niet moeilijk genoeg, dan kan ook nog de volgorde waarin de knoppen worden ingedrukt opgenomen worden in het wachtwoord.

Productenlabels

De verpakkingsindustrie lijkt de wanhoop nabij met de wildgroei van allerlei voedsellabels en teksten. Verschillende bedrijven bedenken hun eigen logo's voor glutenallergieën, Fair Trade, Eco, schadelijke stoffen, enz. Teksten over de ingrediënten moeten in veel verschillende talen op de verpakking worden gezet. Die zouden vervangen kunnen worden door meer eenduidige tags. Klanten scannen de tag met hun mobieltje en zullen de logo's die belangrijk zijn steeds sneller herkennen. Supermarkten zijn sowieso omgevingen waar scanners staan opgesteld langs de hele logistieke keten. Dus ook die kunnen worden gebruikt om de producten uit te lezen.

> Tagology is wellicht een alternatieve vorm van elektronische communicatie

Signalering

Verkeersborden, waarschuwingen of bewegwijzering op plaatsen waar veel mensen uit verschillende culturen samenkomen kunnen uit enkele tags bestaan. Niet alleen de mensen, maar bijvoorbeeld ook de voertuigen (met optische lezers) of robots kunnen de borden lezen. In Nederland hebben we weliswaar een redelijk consistente verkeersbordentaal, maar dat is bijvoorbeeld niet het geval in China waar momenteel veel analfabeten achter het stuur kruipen. Die kunnen worden bijgestaan door een scanner op de auto.

Een alternatieve communicatievorm in tijden van nood

We gaan wellicht nog meemaken dat internet het niet meer doet. De gewone man wil hier natuurlijk niet over nadenken, maar in de dagelijkse praktijk van de informatiebeveiliging is dit steeds vaker een scenario waarover wordt nagedacht. Tijdens het recent gehouden Kooy Symposium over Cyberoperations schetste TNO een fictief scenario waarin onze dagelijkse communicatiemethodes ernstig worden ondermijnd en aan het einde van een dag cyberattacks niet alleen de communicatie, maar ook verschillende delen van onze vitale infrastructuren uitvallen. De diverse aspecten waaruit dit scenario was opgebouwd zijn allen voorgevallen, echter nog niet gelijktijdig. Het was wel een fictief, maar niet een geheel ondenkbaar scenario.

> Tags kunnen ook zeer geschikt zijn als wachtwoorden

Tagology zou wellicht een begin kunnen zijn om na te denken over alternatieve vormen van elektronische communicatie. De huidige protocollen bestaan vooral uit verschillende vertaallagen, om de enen en nullen om te zetten in begrijpelijke tekens of beelden. Dat maakt communicatie kwetsbaar en complex. Die lagen zijn er bij Tagology niet. Elke reeks van 30 bits is meteen een teken. Het meest basale alternatief is een soort morselijn. De zender gebruikt een toetsenbord van dertig knoppen. Een 'nul' is bijvoorbeeld 1,5 Volt (default) en een 'één' is 4,5 Volt. De ontvangers krijgen reeksen van 30 bits binnen, die op een scherm tags vormen, zonder dat daar enige software tussen hoeft te zitten. (Vooruit, laten we het afronden op 32 bits, zodat elke tag ook een begin- en eindbit heeft.) Virussen of andere malware krijgen zo geen kans om stiekem mee te reizen en de communicatie te ontwrichten. Benodigde bandbreedte is minimaal omdat het om zeer kleine datapakketjes gaat. Afluisteren zou mogelijk zijn maar is tegen te gaan met encryptiesleutels aan beide kanten.

Taalexperiment

Tagology is vooral een experiment omdat het een heel andere manier is van omgaan met taal. Zo is bij gewone talen bijvoorbeeld sprake van een zekere fuzzyness. Woorden betekenen vaak net iets anders in een andere context, worden telkens anders uitgesproken en veranderen continu. Dat maakt talen levendig. Grammatica is vooral achteraf bedacht om er enige orde in aan te brengen. Omdat in Tagology één tag maar één

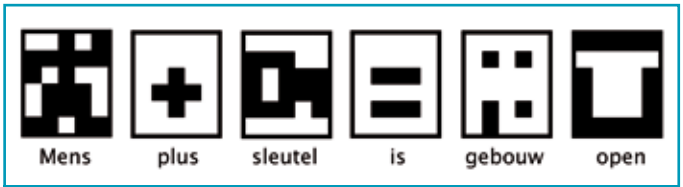


Fig. 3. Vergeet wachtwoorden, log in met een plaatje.

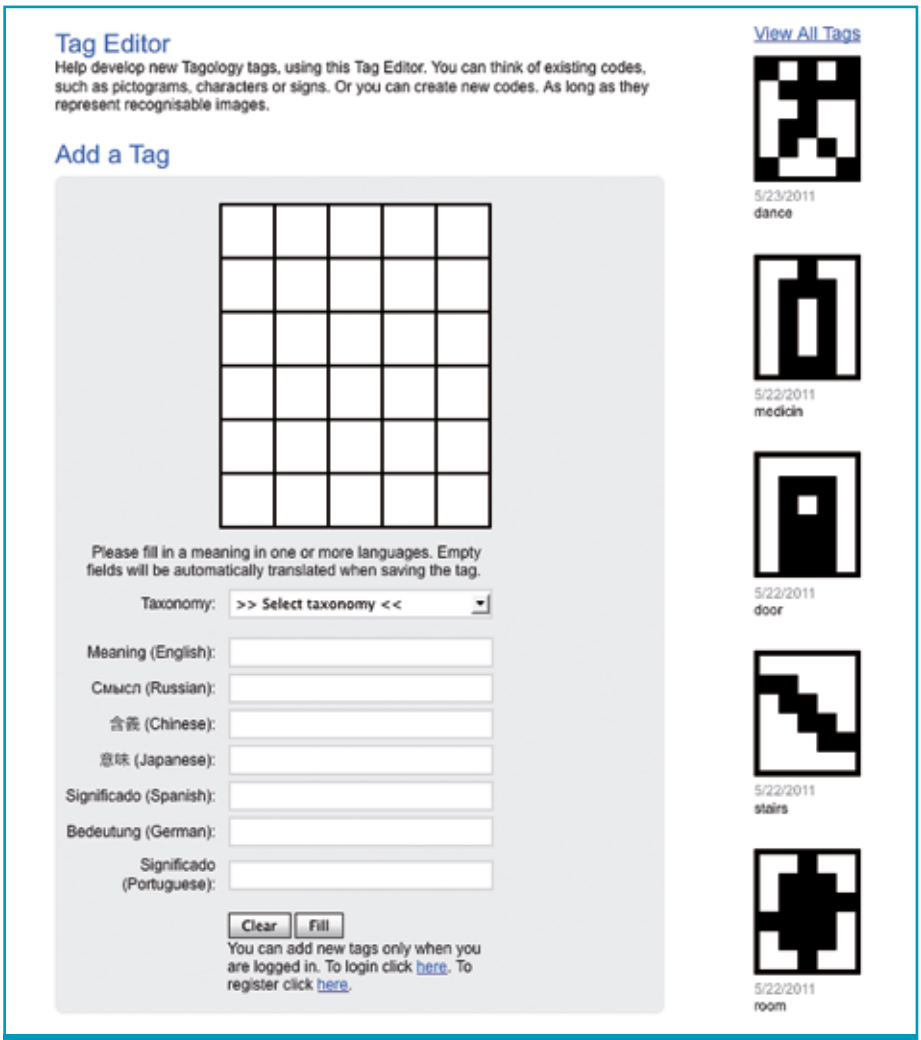


Fig. 4. De online Tag editor op www.tagology.net in zeven talen.

betekenis kan hebben en centraal wordt uitgewisseld verdwijnt deze fuzzyness. Grammatica kan vooraf in plaats van achteraf geconstrueerd worden. Kun je dan beter communiceren of juist minder goed? En hoe zullen verschillende culturen dit gebruiken?

Wie maakt dit?

De organisatie achter Tagology lijkt nog het meeste op een open source community. We zijn begonnen met wat vrijwilligers die een online platform hebben gebouwd dat wordt beheerd door een stichting. Iedereen kan online tags maken en gebruiken, zonder dat daarvoor wordt betaald. Bedrijven kunnen nieuwe diensten en producten ontwikkelen die zijn gebaseerd op Tagology. Zo biedt Mobiubiq de iPhone App om tags te lezen momenteel gratis aan, maar wellicht komen er later uitgebreidere betaalde versies. Bij de toepassing van Tagology in een bepaalde logistieke keten, zou bijvoorbeeld verdiend worden aan arbeidsuren, net als bij Linux.

Het idee achter de Tag Editor is dat een taal niet door een klein groepje mensen kan worden gemaakt. Mensen verschillen nu eenmaal nogal in hoe ze een betekenis in een beeld omzetten en andersom. Op de site kunnen de tags daarom worden gemaakt en gelezen in het Chinees, Engels, Japans, Russisch, Spaans, Portugees en Duits. Met een vrije concurrentie van beelden en toepassingen wordt het misschien wel wat rommelig, maar wie weet gaat het ooit lukken: één taal voor alle mensen en computers. En in de tussentijd hebben we er vooral veel plezier mee.

Links:

Tagology website en Tag Editor: www.tagology.net

De gratis Tagology App om tags te lezen: http://itunes.apple.com/us/app/tagology/id401887574

COLOFON

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

Redactie
Lex Borger (hoofdredactie, werkzaam bij Domus Technica),
e-mail: lex.borger@domustechnica.com
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (Univé-VGZ-IZA-Trias)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
Van de Ridder Druk & Print, Nijkerk
www.vanderidder.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
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

WIE KAN IK NOG VERTROUWEN?

Wind en regen slaan tegen mijn zolderraam terwijl ik begin met mijn bijdrage aan dit onvolprezen blad. Ik heb vanmorgen al even mijn camping via Google Earth bezocht en ik hoop deze over twee weken in het echt te gaan bezoeken. Mijn gedachten dwalen af naar de lange reis die ons te wachten staat en het gedrang bij de tolpoortjes. Bij de tolpoortjes ben ik iedere keer weer verbaasd over de enorme hoeveelheid auto's die zich een weg banen door de poortjes. Het tolbiljet wordt gegeven, de creditcard wordt gegeven en na een paar seconden kun je weer verder. Ik geef mijn creditcard niet, ik heb altijd voldoende euro's bij me om contant te betalen. 'Wellicht een beetje last van beroepsdeformatie'. Ik ben altijd bang dat de creditcard gedupliceerd wordt en dat ik getroffen wordt door allerlei ongewenste afschrijvingen van mijn rekening. Ook dat oude grijze mannetje van dat leuke tankstation midden in de bergen die vroeger altijd mijn creditcard meenam naar het kantoortje in zijn tankstation zal het nu ook met contant geld moeten doen. Nee, de creditcard blijft gewoon in mijn zicht.

Ik prijs mij gelukkig dat ik geen gamer ben. Niet alleen om de enorme hoeveelheid tijd die daarin gaat zitten, maar ook omdat je je creditcardgegevens moet achterlaten om gebruik te kunnen maken van de diensten van de leverancier van de gameconsole. Je gaat ervan uit dat jouw gegevens daar natuurlijk zeer vertrouwd en veilig liggen opgeborgen omdat niemand wil dat er mee gefraudeerd wordt. Sony ontkent in eerste instantie in alle toonaarden dat er problemen zijn met het zogenaamde PlayStation-netwerk. Dat het netwerk is gestopt zou te wijten zijn aan 'technische' problemen. Om een lang verhaal kort te maken; de gegevens van 77 miljoen klanten zijn weg evenals de gegevens van tien miljoen creditcards. Tien miljoen creditcards is bijzonder veel. Alle schade wordt uiteraard door Sony vergoed en het bedrijf denkt dat het met 120 miljoen euro wel afgerond kan worden. 'Afronden' is een lastige zaak want wie wil nu nog gegevens bij hen achterlaten? Waarom was Sony niet voldoende beveiligd? Is het omdat ze dat allemaal niet zo nodig vonden? Waarom worden dit soort sites niet door toezichthouders onderzocht op robuustheid? Vragen, vragen en vragen waar jammer genoeg nooit antwoorden op komen. Sony heeft de aandacht weten te verschuiven naar de gevolgen voor de productie door de natuurramp in Japan. Ook in Nederland kunnen dit soort hacks natuurlijk voorkomen. Zoek op Google of Webwereld eens 'problemen bij internetbankieren' en de schermen en ogen schieten vol. Phishing-aanvallen, gebroken TAN algoritmes, Joomla-lekken enzovoort.

DUO (de voormalige IB-Groep) was kortgeleden ook in het nieuws omdat zijn website zwakheden bevatte die op de televisie even werden gedemonstreerd. OV-chipkaarten die, zelfs met mijn beperkte technische kennis, thuis achter de pc even weer geladen kunnen worden zonder dat je rekening daarmee wordt belast.

Wanneer gaan we met zijn allen weer terug in de tijd en gooien we de oude sokken niet meer weg maar gebruiken we deze om ons spaargeld in op te bergen? Zó ver zal het niet komen. Eén oververhitte frituurpan en je pensioen gaat in rook op.

Nee gelukkig hebben we bedrijven die gespecialiseerd zijn op beveiligingsvraagstukken. Multinationals die gelukkig tooling hebben uitgevonden waarmee authenticatie aan de toegangspoort van de website op een veilige en zekere manier kan worden uitgevoerd. Neem bijvoorbeeld het ouderwetse maar nog steeds goed functionerende token. Iedere minuut wordt er een unieke passcode gegenereerd waarmee toegang kan worden verkregen. Helaas zijn deze algoritmen gestolen van de website van RSA en daarmee is een stuk van de beveiliging onderuit gehaald. Ook mijn bedrijf gebruikt deze toegangsmethode maar gelukkig hebben wij ervoor gekozen om een pincode toe te voegen, een user-id in combinatie met een wachtwoord waarmee de diefstal van de algoritmen niet direct een beveiligingslek heeft veroorzaakt.

Als de beveiliger al kan worden gehackt dan wordt het lastig om je veilig te voelen. Dan wordt het lastig om te geloven dat die bedrijven waar ik mijn creditcardgegevens aan heb verstrekt, de beveiliging wel op orde hebben.

Buiten is het inmiddels droog geworden en een waterig zonnetje lijkt zich door de wolken heen te branden. Misschien dat het weer ervoor heeft gezorgd dat mijn column vandaag toch wel erg somber overkomt. Ik beloof dat ik deze column nog eens zal doorlezen als het buiten prachtig weer is zodat ik misschien een iets positievere inhoud kan laten afdrukken.

Berry

Real-time Malware beveiliging

Uw organisatie heeft toegang tot het internet nodig om te kunnen functioneren, klanten goed te kunnen ondersteunen en marketing activiteiten te ontplooien. Zorg dat Web 2.0 geen bedreiging wordt voor uw organisatie. Geef toegang tot het internet zonder risico's te nemen.

De M86 Secure Web Gateway met Real-time Code Analyse geeft u de mogelijkheid om de organisatie op een veilige manier gebruik te laten maken van de mogelijkheden die Web 2.0 biedt. De M86 Secure Web Gateway ontdoet webpagina's van kwaadaardige code in plaats van het blokkeren van de gehele pagina. Zo kunnen werknemers veilig en ongestoord toegang tot het internet blijven hebben en kunt u erop vertrouwen dat dat veilig gebeurt!

Bel nu CRYPSYS Data Security, distributeur van de M86 Secure Web Gateway, op 0183 62 44 44 of mail naar sales@crypsys.nl voor meer informatie.

M86™ SECURITY
Real-Time Security for the Borderless Network

CRYPSYS
data security