**MANAGEMENT-SUMMARY**
**Waarom faalt cyber security steeds? Waarom verkiezen burgers en bedrijven functionaliteit boven cyber-veiligheid? Oftewel: waarom houden we zo van cyber-onveiligheid? Een artikel dat een pleidooi is voor een andere aanpak van cyber security en het maken en gebruiken van veiliger ICT-producten en -diensten.**

# VERLIEFD OP ONVEILIGHEID

Bij ontwikkelaars en gebruikers in de ICT-wereld staat veiligheid zelden bovenaan als het gaat om de belangrijkste producteigenschappen. Op de eerste plaats moet het gewoon werken. Vervolgens moet het zoveel mogelijk kunnen. En het mag natuurlijk niet te ingewikkeld zijn. Of het ook veilig is? Dat zal toch wel? Nu tegenwoordig zo ongeveer alles en iedereen deel uitmaakt van de ICT-wereld, kan het geen kwaad om eens met een andere bril naar cyber security te kijken.

Tijdens mijn studie, nu ruim veertig jaar geleden, kluste ik bij als programmeur. Zodra het programma geschreven was en in een stapel ponskaarten was omgezet, volgde het functionele testen. Werkte alles naar behoren, dan wilde je graag aan de volgende uitdagende programmeerklus beginnen. De systeemontwerper en -verantwoordelijke dacht daar anders over. Hij haalde een paar honderd ponskaarten uit de afvalbak naast de ponsmachine die je vervolgens moest laten verwerken door je programma. O wee als er ook maar één ponskaart door je programma geaccepteerd werd, dan had je heel wat uit te leggen. Het programma moest zichzelf en daarmee het totale systeem beschermen tegen iedere mogelijke vorm van foutieve invoer.

## Crashes

In 1978 crashten mainframes iedere dag wel een paar keer. De kunst was de oorzaak van de meest voorkomende crashes weg te nemen. Er bleek echter een diepliggender oorzaak te zijn. Veel systeemprogramma's controleerden de invoerparameters niet. Vaak werd door een programmeerfout een ellenlange stroom gegevens (bytes) in plaats van een enkel getal aangeboden. Resultaat was een crash van het gehele mainframe door een zogenaamde 'buffer overflow'. Systematisch hebben een collega en ik meer dan honderd van dergelijke systeemprogramma's voorzien van betere invoercontrole en dergelijke fouten uit het besturingssysteem gehaald.

## Wachtwoorden

Inloggen op een mainframe was in de jaren 70 eenvoudig. Je ging naar een terminal, verzon een gebruikersnaam en ging aan de gang. Geen wachtwoord was nodig. Pas veel later werden gebruikersnamen en initiële wachtwoorden uitgegeven. Sterke wachtwoorden werden geëist die na korte tijd verversing behoeven. Iedere ICT-innovatie na die tijd zoals midicomputers, minicomputers, PCs, genetwerkte PCs, tablets en smart phones vereiste geen vorm van authenticatie: het waren toch persoonlijke middelen nietwaar? Kort nadat deze systemen grootschalig ingezet werden, bleken er toch veel gevoeliger acties op de systemen uitgevoerd te worden dan eerder gedacht. Bijvoorbeeld opslag van medische gegevens, elektronisch bankieren en een het onderhouden van een verborgen tweede leven. Wachtwoorden met sterkere eisen werden achteraf alsnog toegevoegd.

## Onveiligheden

Bij iedere nieuwe ICT-innovatie blijken we echter niet geleerd te hebben van de opgeloste onveiligheden tijdens de vorige ICT-innovatiegolven. Eind jaren tachtig kwamen bijvoorbeeld Unix- en netwerkomgevingen opzetten. In eerste instantie opgezet voor groepsgebruik in een besloten omgeving waren de beveiligingsmaatregelen niet bestaand of ronduit zwak te noemen. Wachtwoorden als klare tekst over het netwerk en geen invoercontrole door communicatieprotocollen waardoor systemen crashten als je er ook maar een byte meer of minder dan verwacht naar toe stuurde. Veel van dergelijke fouten werden achteraf met patches opgelost toen hackers dit type systemen en netwerken gingen openbreken of lieten crashen met bijvoorbeeld de ping-of-death. Pas recent komen de makers van procescontrolesystemen er achter dat ze dezelfde problemen hebben. Raffinaderijen zijn door dergelijke zwakheden plat gegaan omdat een ICT-beheerder per ongeluk een test losliet op het proces¬controle¬netwerk. Inmiddels weten hackers bijna iedere week nieuwe mogelijkheden open te leggen om op dergelijke systemen in te breken.

## Vooruitgang

Waarom houden we van onveilige systemen? Ten eerste houden we van vooruitgang. We kunnen we niet snel genoeg nieuwe functionaliteit krijgen die de informatie- en communicatietechnologie (ICT) ons biedt. De verwarming van uw bedrijf vanaf thuis regelen? De bewakingscamera of het hek op afstand via internet besturen? Doen we! Daarnaast willen we gebruikersgemak, geen moeilijk authenticatieproces. We houden ook van de nieuwe gadgets. Het slimme horloge, de slimme bril, bedrijfsgegevens op de eigen slimme telefoon. Informatiebeveiliging? Is dat niet een vage afdeling op het hoofdkantoor?

## Briljante ideeën

Ten tweede denken ontwikkelaars van de volgende generatie ICT-innovatie geheel niet aan informatiebeveiliging. Het betreft steeds vaker jonge talenten die al vroeg gescout worden met briljante ideeën om ons geluk, gemak en genot te brengen. Als je bezig bent met het ontwikkelen van apps voor de volgende generatie smartphones, smartwatches, pacemakers [1] of energiezuinige gebouwen, kijk je met een Google Glass op alleen vooruit. Dan kijk je niet terug naar de oude meuk als desktops of, erger nog, mainframes. De eerder lessen van oude beveiligingsfouten in die systemen en hun oplossingen worden daarom niet meegenomen in de ontwikkeling van de volgende generatie ICT-producten. Daarom vinden we in nieuwe producten bijvoorbeeld wederom standaard fabriekswachtwoorden en achterdeuren voor het testen, kunnen hackers opnieuw de code manipuleren door een buffer of stack overflow te creëren en kun je opnieuw cryptografische sleutels onttrekken aan het geheugen. Het is ons onvermogen om te leren van in eerdere generaties ICT geconstateerde beveiligingsfouten waardoor we hier na zo'n vijftig jaar nog steeds last van hebben.

## Gebouwbewakingssystemen

Ten derde komt ICT haast ongemerkt steeds vaker in handen van medewerkers van bedrijven die alleen de functionaliteit zien en niet dat ze een te beveiligen ICT-systeem gebruiken. De noodzaak om daarmee veilig om te gaan wordt niet duidelijk uit de installatie-

instructies, de werkinstructies en de context van het gebruik. Denk bijvoorbeeld aan moderne ontruimingsinstallaties, de telefooncentrale, IP-camera's en gebouwbewakingssystemen. Maar bovenal, als dergelijke systemen niet veilig uit de doos komen, gaat het zeker fout. Producenten en systeemintegratoren hebben hier een grote taak.

## Lessen

Willen we cyber security aanpakken, dan moeten we eerdere lessen nu eens echt tot ons nemen en daarvan leren. We moeten zorgen dat die lessen ook in de volgende generatie ICT-producten en -diensten terechtkomen. Vooral nu we steeds vaker ketens aan ICT-diensten ontwikkelen, zullen we in de jaren 70 uitgedachte en reeds toegepaste beveiligingsprincipes ter 'zelfbescherming' nu eens echt moeten gaan toepassen. Bijvoorbeeld: controleer alle binnenkomende, maar ook uitgaande informatie op validiteit.

## Vitale functies

Nieuwe ICT-toepassingen verstoppen zich steeds vaker diep weg in gebruikersfunctionaliteit. Het aan- of uitzetten van pompen, verlichting, airconditioning en zelf vitale functies voor onze samenleving kan vanaf een tablet gedaan worden. De vraag wordt niet gesteld of dat ook altijd vanaf de keukentafel via internet moet kunnen. Het Shine-project identificeerde in de afgelopen paar jaar al 29.349 procescontrolesystemen in Nederland die rechtstreeks aan het internet gekoppeld zijn… [2].

## Glazen bol

Maar we kunnen ook vooruit kijken. Dat doen de hackers en cybercriminelen ook. Ze zien een gouden toekomst tegemoet. Uw wagenpark gaat bijvoorbeeld eerdaags met andere auto's en de weg communiceren. Aan de informatiebeveiligingskant van dergelijke communicatie is er nog weinig ontwikkeling geweest. Hackers hebben allerlei elektronische systemen in auto's al opengebroken [3]. Staan auto's uit uw wagenpark ook op de lijst van onderzochte autotypen? [4] Maar ook bij u thuis hangen spoedig de slimme thermostaat en de slimme meter en rollen de slimme koelkast en de slimme wasmachine eerdaags binnen. Recent kwam naar buiten dat er negen serieuze beveiligingslekken zitten in een bepaald type draadloze thermostaten [5]. Shodan, een 'Google' om bepaalde typen systemen met bepaalde softwaretypen en -versies te vinden, liet zien dat 7000 van dergelijke thermostaten direct op afstand manipuleerbaar zijn. De standaard toegang is user=admin, password=admin, de pincode 1234, geen bescherming tegen het proberen van alle 9999 cijfercombinaties, niet-versleutelde informatie over de Wi-Fi-toegangen tot het privénetwerk, enzovoorts. Zijn uw gebouwbeheer en –bewakingssystemen veiliger? Hoe zeker bent u daarvan?

## Dweilen

Hoe is het gesteld met de beveiligingssystemen die u maakt of koopt, installeert, samenstelt of reeds in gebruik heeft? Levert u de volgende reeks producten en –diensten veilig(er) af? Blijft u onveilige producten kopen of stelt u minimale eisen aan de producten die u eerdaags gaat kopen of laat installeren? Blijft u liever houden van onveiligheid gepaard gaande met veel gebruikersgemak en ongekende functionaliteit (ook voor de hacker)? Dweilen we verder met de kraan open? Is uw strategie die van een Internet of Insecure Things [6, 7]? Dan kan ik nu al voorspellen dat we in 2050 de verjaardag van honderd jaar buffer overflows en standaard¬wachtwoorden gaan vieren.

**Links:**

[1] http://fusion.net/story/20228/first-cyber-murder-will-happen-in-next-three-months-experts-claim/
[2] http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014
[3] I. Rouf et al, Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study, USENIX Security'10 Proceedings of the 19th USENIX conference on Security, http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf
[4] https://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces
[5] http://cybergibbons.com/security-2/heatmiser-wifi-thermostat-vulnerabilities/
[6] http://www.channelweb.co.uk/crn-uk/news/2371839/iot-vendors-accused-of-taking-security-back-to-1990s
[7] http://www.networkworld.com/article/2687169/security0/bot-herders-can-launch-ddos-attacks-from-dryers-refrigerators-other-internet-of-things-devices.html

*Dit artikel is deels ontleend aan een eerder artikel van de auteur 'Are we in love with cyber insecurity?' in het International Journal of Critical Infrastructure Protection (2014), V7(3), pp. 165–166, september 2014*

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