iB
INFORMATIEBEVEILIGING
jaargang 16 - 2016
#5

NIEUWE BEDREIGINGEN

Apple vs FBI: de feiten op een rijtje

Security voor Internet of Things

Bedreigingen vitale infrastructuur Europa

Black Hat Sessions XIV

KWETSBAAR OP DE MARKT

Actoren, acties, bedreigingen, kwetsbaarheden. Allemaal aspecten die bijdragen aan een operationeel bedrijfsrisico. Het IT-systeem is het kind van de rekening. En als je de vraag stelt "Wat zijn de nieuwe bedreigingen?", dan kun je dit eigenlijk niet los zien van de andere aspecten. Zo zie ik drie factoren die bijdragen aan nieuwe bedreigingen:

De eerste factor is de market push achter nieuwe technologie. We rollen nieuwe technologie uit omdat het nieuwe mogelijkheden blootlegt, maar met die nieuwe mogelijkheden komen ook nieuwe bedreigingen mee. We zijn nog steeds bezig met meer en meer gevoelige 'big data' te verzamelen, zonder dat we eigenlijk weten hoe die data veilig opgeslagen kan worden. Het aggregatierisico is enorm en wordt alleen maar groter als het volume aan data toeneemt.

Verder halen we steeds vaker de factor mens uit het geautomatiseerde proces. We laten systemen door andere systemen bedienen en controleren. Informatie-uitwisselingen gaan automatisch, transacties gaan automatisch. En dat wat automatisch gaat, gaat automatisch fout. Mensen hebben een ongelofelijk vermogen om abnormale gevallen te kunnen herkennen. Systemen niet. We weten al dat 'kleine' problemen in de bediening van bruggen of de besturing van auto's dodelijke gevolgen kunnen hebben.

En dan is er IoT: het internet der dingen. 'Dingen' in deze context bevatten meestal volledige Linux computers. Dat zijn bij uitstek de nieuwe schaapjes voor de herders: de thingsbotnet, samengesteld uit thingbots. De focus ligt hier nog zó bij functionaliteit en zo weinig bij veiligheid dat het gewoon eng is. We hebben heel hard beveiligingsstandaarden nodig voor allerlei gebruiksscenario's, waarbij gebruiksgemak ook nog eens overeind blijft.

De trek van de zwarte markt is de tweede factor. Malware was al vercriminaliseerd met ransomware, en dit is en blijft voorlopig nog een lucratieve bezigheid. Het is fijn voor de criminelen dat ze gemakkelijk grenzeloos te werk kunnen gaan, een eigen munt hebben en een eigen netwerk. En we horen ook regelmatig dat leveranciers het ze gemakkelijk maken, omdat ze blijven vinden dat ze backdoors moeten inbouwen in hun producten. Zo worden kwetsbaarheden regelrecht bedreigingen... Wel hebben we skimming eindelijk onder controle gekregen. Dus wat zie je nu? De criminaliteit focust zich nu op de online betaling. Daar wordt geen chip bij gebruikt.

Spionageactiviteiten zijn afgenomen, meldde onder andere het nieuwe Verizon DBR. Is dat werkelijk zo, of hebben ze zich succesvol onder de radar kunnen houden?

En de laatste factor is het falen van de 'witte' markt. We zijn nog aan het kibbelen wie beter is in cloud-hosting: de ISP of wijzelf. Ondertussen proberen we cloud te reguleren door kunstmatige grenzen aan te leggen, 'als de data maar in Europa blijft'. En we bespioneren elkaar liever dan dat we met elkaar samenwerken. Als we al het cyberfalen eens als wijze lessen zouden zien die we compleet met elkaar zouden moeten delen.

In dit nummer een aantal verhalen uit of over bovenstaand speelveld.

Veel leesplezier.
Lex Borger, Hoofdredacteur

In dit nummer

Interview met Stefan de Wit - **4**
Arbeidsveiligheid bedreigd vanuit cyberspace - **8**
Ronald Prins - Alumnus van het Jaar 2016 - **12**
Column Privacy - Het vergeten kind - **13**
Apple vs FBI: de feiten op een rijtje - **14**
Security voor Internet of Things - **21**
Niet gekeken altijd mis! - **24**
Column Attributer - Exit-Ready - **27**
Verslag - Black Hat Sessions XIV - **28**
Verslag CISO 11 - **30**
Achter het Nieuws - **32**
Column Berry - Grijze haren - 35

OUDE WIJN IN NIEUWE ZAKKEN

De 'tegenstanders' waar je als security-professional anno 2016 mee te maken hebt, zijn vooral veel professioneler dan enkele jaren geleden. Over 'echt' nieuwe security-dreigingen heeft Stefan de Wit, Security Consultant bij SecureLabs, onderdeel van SecureLink, het dan ook bewust niet wanneer we hem hiernaar vragen. Hij ziet in de praktijk vooral dat bekende fenomenen als phishing en ransom- of cryptoware steeds volwassener en daarmee professioneler worden. 'Professionele' oude wijn in nieuwe zakken, zo beaamt hij.

"Cybercrime is een volwassen businessmodel en de kans van slagen is groot. Cybercriminelen ontpoppen zich tot professionele aanbieders van cybercrime-as-a-service binnen allerlei darknet-achtige marktplaatsen. Plekken waar ze kwaadwillenden de mogelijkheid bieden om het beste aanvalsmechanisme in te kopen voor hun specifieke doel", legt De Wit uit.
"Een volwassen markt van vraag en aanbod waarbij net als voor aanbieders van legale producten en diensten reputatie van doorslaggevende betekenis is. Een inkoper koppelt diensten van de beste malware-ontwikkelaar en datahandelaar aan die van een malware-distributeur, in combinatie met de partij die de payment-delivery het best kan afhandelen. Zo ontstaat een keten van best of breed in cybercrime-as-a-service."

Stefan de Wit, Security Consultant bij SecureLabs, onderdeel van SecureLink

'Cybercrime is maatwerk geworden'

Deze professionele ketens van cybercriminelen gaan aan de slag voor de hoogste bieder. "Het zijn effectief opererende ondernemers die het geld volgen", vat de security-specialist samen. Wat naast deze professionalisering volgens De Wit opvalt, is dat aanvallen steeds persoonlijker worden.
"Voordat aanvallers toeslaan, wordt uitgebreid gerechercheerd via social media. Cybercrime is hiermee maatwerk geworden. Jij als persoon of als medewerker van een organisatie bent het specifieke slachtoffer."

Dit geldt zeker wanneer cybercriminelen uit zijn op cruciale bedrijfsinformatie. Wat dit betreft zijn met name innovatieve bedrijven een belangrijk doelwit. Bedrijven waarbinnen intellectueel eigendom, patenten en octrooien een factor van belang zijn. Zij zijn immers bezig met ontwikkelingen die voor bijvoorbeeld regeringen van bepaalde landen, maar ook voor concurrenten erg interessant zijn. Het moeilijke hierbij is volgens De Wit dat de budgetten van de opdrachtgevers voor dit soort e-spionageactiviteiten vaak oneindig zijn.

Om je tegen deze professionele vorm van criminaliteit te wapenen, moet je je volgens De Wit allereerst bewust zijn van de gevaren. De opmerking 'bij ons valt toch niks te halen' is wat hem betreft anno 2016 eigenlijk op geen enkele organisatie meer van toepassing. "Elk bedrijf en elke organisatie beschikt over gegevens, assets of diensten die voor een ander van belang of waarde kunnen zijn. Je moet je daarom steeds weer afvragen welke risico's je loopt en hier je niveau van beveiliging op afstemmen. Een continu proces."

Impact steeds groter

Maar welke bedrijven lopen nu het meeste risico? Als het gaat om afpersing middels ransom- en cryptoware is eigenlijk elke organisatie in de ogen van De Wit een mogelijk doelwit. Door de toenemende professionaliteit van cybercriminelen wordt de impact van hun acties volgens hem bovendien steeds groter.
"Neem de nieuwste methode van ransom- en cryptoware. Hierbij zie je een combinatie van een persoonlijk, op de gebruiker gerichte actie, in combinatie met nieuwe of bestaande kwetsbaarheden in Office- en Adobe-toepassingen. De ransom- en cryptoware versleutelt documenten, maar nestelt zich ook op het netwerk van de organisatie", legt hij uit. "Het openen van een bestand in een bijlage start een serie acties die niet alleen de bestanden van het slachtoffer encrypt, maar die ook software downloadt op het systeem van de gebruiker. De bijlage zelf lijkt een corrupt bestand, echter op de achtergrond worden diverse taken uitgevoerd. Zo wordt bijvoorbeeld de Windows VSS (Volume Snapshot Service)

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

Hoe beperk je gevolgen ransomware?
Welke maatregelen zou je als bedrijf sowieso moeten nemen om de gevolgen van ransomware zoveel mogelijk te minimaliseren?

- **Software up-to-date houden**
- **Rechten van gebruikers minimaliseren**
- **Netwerk segmentatie doorvoeren**
- **Vulnerability- en patchmanagement**
- **IDS en anti-malware maatregelen**
- **Logging en Monitoring**
- **Maken en testen van back-up**
- **Bewustwording van gebruiker verbeteren**
- **Incident response processen inrichten en testen**

De opmerking 'bij ons valt toch niks te halen' is anno 2016 eigenlijk op geen enkele organisatie meer van toepassing.

verwijderd zodat gecodeerde bestanden niet kunnen worden hersteld. De ransomware is zo ingesteld dat deze elke keer actief wordt wanneer de gebruiker opstart."

Een voorbeeld van deze ransomware die zich gedraagt als worm is RAA-ransomware binnen Java ZCryptor. Een gevaar waarvoor onder meer Micosoft onlangs nog waarschuwde. De worm zou zich via USB-sticks en netwerkmappen kunnen verspreiden waardoor snel meerdere systemen besmet raken.

Gebruiker blijft minst sterke schakel

De impact van de nieuwste vormen van ransom- en cryptoware neemt dus toe. Een stabiele factor blijft volgens De Wit dat de gebruiker de minst sterke schakel is in het geheel. "In de meeste gevallen komt ransomware immers op systemen/netwerken terecht via interactie met de gebruiker", legt hij uit. Awareness kweken onder medewerkers blijft wat hem betreft dan ook essentieel. "Je kunt in deze niet vertrouwen op technische oplossingen alleen", benadrukt hij.

Aan het begrip awareness zit wat deze security-specialist betreft echter ook weer 'een bovengrens'. "Je kunt mensen op de vloer niet eindeloos belasten met nieuwe protocollen. De dreiging van een protocollen-overload ligt altijd op de loer", waarschuwt hij. "Het beste wat je als security-specialist kunt doen, is er vanuit gaan dat een gebruiker in de fout gaat. En je hierop voorbereiden door je steeds weer de vraag te stellen wat het betekent voor jouw organisatie wanneer dit gebeurt."
Betalen om op die manier gegijzelde bestanden 'los' te krijgen, adviseert De Wit eigenlijk nooit. "Op die manier houd je het lucratieve businessmodel in stand. Hoe meer bedrijven en organisaties betalen, hoe meer tijd cybercriminelen bereid zijn erin te steken om dit soort malware steeds verder te ontwikkelen. Het is kiezen tussen twee kwaden. Toegeven aan criminelen of afscheid nemen van gegijzelde bestanden en verdergaan op basis van een back-up."
De Wit geeft echter toe dat vanuit business perspectief betalen de meest effectieve manier kan zijn om de schade voor een organisatie te beperken.

Ransomware moet als je het aan De Wit vraagt anno 2016 dus nog steeds bij elke security-specialist hoog op zijn agenda staan. Het is volgens hem voor de meeste bedrijven namelijk niet de vraag of ze er last van krijgen, maar wanneer. Waarbij hij tot slot nog opmerkt dat de beste bewustwording in deze 'helaas nog altijd een incident is'. "Bij veel bedrijven ontstaat pas dan de behoefte om daadwerkelijk stappen te nemen", geeft hij aan.

Gevaar van het Internet of Things

Een heel andere security-dreiging die De Wit signaleert, staat waarschijnlijk nog wat minder op ieders netvlies. Die van het

Top 5 bedreigingen komende tijd:

- Social engineering via social media
- Persoonlijke of bedrijfsnabootsing (zich voordoen als..)
- Ransom/cryptoware op basis van in het artikel genoemde componenten
- Firmware-aanvallen op IoT-toepassingen
- De onbewust en onbekwame gebruiker

Alle apparaten verbonden aan het internet vormen in feite een nieuwe ingang voor criminelen.

Internet of Things (IoT). Een ontwikkeling die eraan bijdraagt dat onze fysieke en digitale wereld steeds meer samensmelten. Daarnaast groeit de afhankelijkheid voor gebruikers van digitale informatie en toepassingen hierdoor nog sterker dan voorheen. Waardoor ook de mogelijkheden voor misbruik volgens hem toenemen.
"Alle apparaten verbonden aan het internet vormen in feite een nieuwe ingang voor criminelen. Denk aan auto's, systemen voor klimaatbeheersing, ijskasten, rookmelders, maar ook medische apparaten voor de monitoring van de gezondheid. Wanneer deze apparaten niet goed zijn beveiligd, kan iedereen ze binnendringen", geeft hij aan.

Vraag is nu volgens De Wit wiens verantwoordelijkheid dit is. "Moeten bijvoorbeeld al dit soort apparaten getest worden op hackbaarheid? En zo ja, wie moet dit doen? Fabrikanten, branche-organisaties, de Consumentenbond?"
Beveiliging heeft tot op heden als het gaat om IoT volgens De Wit zeer beperkte prioriteit. Functionaliteit staat voorop. Dat biedt criminelen dus de mogelijkheid van een soort oneindige speeltuin. Wat hem betreft ligt hier een gezamenlijke verantwoordelijkheid van ontwikkelaars, fabrikanten, toezichthouders en wetgevers.

Security-professionals raadt hij vooral aan zich bewust te zijn van deze nieuwe dreiging. Je af te vragen wat voor jouw organisatie de belangrijkste dreigingen in deze zijn. En - zoals je ook doet in het geval van meer traditionele risico's als het gaat om security - een plan maken om adequaat te kunnen reageren, mochten deze dreigingen werkelijkheid worden.

Beste antwoord: Security Defense

'Security Defense' is hierbij volgens De Wit het sleutelwoord. Waarbij het wat hem betreft zaak is dat organisaties van preventief naar proactief gaan. Circa tachtig procent van de budgetten van IT-security worden besteed aan preventieve (IT-security) middelen. Inzicht in en kunnen reageren op dreigingen zijn onderbelicht.
"Weten wanneer een aanval plaatsvindt, weten waar de dreigingen zitten, weten waar een mogelijke aanval plaats gaat vinden", vat hij samen. "Ben je zover dan heb je inzicht in je eigen kwetsbaarheid en weet je bovendien hoe je kunt voorkomen dat die kwetsbaarheden te exploiteren zijn. Het beste antwoord op de steeds professioneler wordende cybercrimineel."

ARBEIDSVEILIGHEID BEDREIGD VANUIT CYBERSPACE

Nieuwe dreigingen voor de werkomgeving

Een werkgever is conform de Arbowet integraal verantwoordelijk voor een veilige werkomgeving en heeft daartoe een risico-inventarisatie en -evaluatie uitgevoerd. Er zijn de nodige risicobeperkende maatregelen getroffen zodat de medewerkers een veilige werkomgeving hebben. Maar is er ook gekeken naar het risico voor de arbeidsveiligheid door onvoldoende informatiebeveiliging van digitaal gestuurde processen, machinerieën en robots? Grote kans dat dit over het hoofd gezien is!

De Arbeidsomstandighedenwet 1998 legt werkgevers en werknemers een aantal eisen en verplichtingen op inzake de veiligheid van het werk en de gezondheid van de medewerkers [1]. Maar is er wel rekening gehouden met onbevoegden of malware die digitaal gestuurde processen kunnen overnemen of verstoren? Hier kan de veiligheid van de werknemers in uw bedrijf door in het geding komen. Hieronder laten we zien dat de Europese machinerichtlijn en de Arbowet nog weinig handvatten geven die bedrijven helpen om dit risico te beperken. Niets doen is echter geen optie daar ICT zich steeds meer innestelt in de arbeidsomgeving van uw naaste collega's. Bijvoorbeeld in de besturing van machinerieën of in autonoom voortbewegende voertuigen en robots.

Artikel 3 stelt "De werkgever zorgt voor de veiligheid en de gezondheid van de werknemers inzake alle met de arbeid verbonden aspecten en voert daartoe een beleid dat is gericht op zo goed mogelijke arbeidsomstandigheden, waarbij hij, gelet op de stand van de wetenschap en professionele dienstverlening, het volgende in acht neemt:

(a) tenzij dit redelijkerwijs niet kan worden gevergd, organiseert de werkgever de arbeid zodanig dat daarvan geen nadelige invloed uitgaat op de veiligheid en de gezondheid van de werknemer;

(b) tenzij dit redelijkerwijs niet kan worden gevergd, worden de gevaren en risico's voor de veiligheid of de gezondheid van de werknemer zoveel mogelijk in eerste aanleg bij de bron daarvan voorkomen of beperkt; naar de mate waarin dergelijke gevaren en risico's niet bij de bron kunnen worden voorkomen of beperkt, worden daartoe andere doeltreffende maatregelen getroffen waarbij maatregelen gericht op collectieve bescherming voorrang hebben boven maatregelen gericht op individuele bescherming; slechts indien redelijkerwijs niet kan worden gevergd dat maatregelen worden getroffen die zijn gericht op individuele bescherming, worden doeltreffende en passende persoonlijke beschermingsmiddelen aan de werknemer ter beschikking gesteld; {…}

(f) elke werknemer moet bij ernstig en onmiddellijk gevaar voor zijn eigen veiligheid of die van anderen, rekening houdend met zijn technische kennis en middelen, de nodige passende maatregelen kunnen nemen om de gevolgen van een dergelijk gevaar te voorkomen {…}."

De werkgever is daarom wettelijk verplicht om een risico-inventarisatie en –evaluatie uit te (laten) voeren. Op basis daarvan moeten de nodige risicobeperkende maatregelen getroffen worden. Hierbij beginnend, zoals hierboven in lid b is geschetst, bij het voorkomen van risico bij de bron en als laatste door het treffen van beschermingsmaatregelen voor de individuele werknemer.

Inmiddels zijn de werkgevers en ook de door hen ingehuurde Arbodiensten goed ingevoerd om fysische, chemische en fysieke risicoaspecten op de werkvloer in kaart te brengen en te beheersen. Maar wordt daarbij niet een nieuw soort dreigingen over het hoofd gezien? Dreigingen die komen vanuit cyberspace: malware, hacking en menselijke fouten in het cyberdomein (zie ook het kader)?

Eric Luijf is principal consultant Bescherming Vitale Infrastructuur bij TNO. Eric is bereikbaar via eric.luijf@tno.nl.

Wouter Steijn is Junior Scientist Innovator bij TNO. Wouter is bereikbaar via wouter.steijn@tno.nl.

Cyberfysische systemen

Informatie- en communicatietechnologie (ICT) en daarmee "cyberspace" dringt steeds verder door in allerlei functies die wij dagelijks gebruiken. Veelal verstopt ICT zich daarbij achter een simpel aanraakschermpje of worden functies op afstand gecontroleerd en aangestuurd. Apparatuur en machines, oftewel cyberfysische systemen, lijken daardoor nog steeds op hun klassieke mechanische voorgangers (bijv. draaibanken) maar zijn ineens veel flexibeler, efficiënter en 'slimmer'. Denk hierbij bijvoorbeeld aan computergestuurde machinerieën op de werkvloer en aan computergestuurde processen die chemische processen controleren. De ouderwetse draaibank is inmiddels vervangen door een CNC-draaibank, de heftruck door een automatisch bewegend voertuig met een hefinrichting en het verwerken van gevaarlijke chemische stoffen is een volledig computergestuurd proces. Het is waarschijnlijk dat kranen eerdaags met een tablet op afstand bestuurd worden. Robots bewegen zich al op sommige werkvloeren voort tussen de medewerkers en zullen steeds nauwer gaan samenwerken met de mens (cobots).
De ingebouwde ICT-component reageert daarbij op inputs van sensoren en bestuurt het apparaat of machine. Qua efficiëntie maar ook qua veiligheid en ergonomische belasting voor de werknemers vormen deze ontwikkelingen veelal een grote verbetering. Er is echter één maar: de sensoren, programmatuur, apparatuur en het communicatie¬netwerk moeten betrouwbaar functioneren.
Als er geen aandacht wordt besteed aan de informatie- en communicatiebeveiligingsaspecten van deze componenten wordt er een groot risico gelopen. Malware, hackers, of een eenvoudige configuratiefout kunnen een machine of een proces onverwacht anders laten reageren. De programmatuur kan daarbij een motor van de machine onverwacht laten starten en de machine een onverwachte beweging laten uitvoeren waarbij werknemers gevaar lopen.
Helaas is dit onderwerp nog sterk onderbelicht bij veel bedrijven en organisaties, zoals onder andere beschreven is in eerdere artikelen [2] [3]. Het onbewust binnendringen van ICT in functionaliteiten in bedrijven en organisaties zorgt ervoor dat de 'op papier' verantwoordelijken zich niet bewust zijn van dit nieuwe arbeidsrisico voor werknemers.

De Arbowet

De Arbowet vereist het regelmatig uitvoeren van een risico-inventarisatie en –evaluatie door de werkgever. Veel werkgevers zullen de mechanische en bedienaspecten van risicovolle apparatuur en processen ten volle hebben meegenomen in hun analyses. Maar is er ook nagedacht over dat netwerkkabeltje dat onder de vloer doorloopt? Aan de USB-stick voor het laden van een ander programma? Onderhoud op afstand door derde partijen? Dat zijn slechts enkele aanvalsfactoren waardoor cyberfysische systemen onbetrouwbaar kunnen worden en er een groot risico op de werkvloer voor uw collega's ontstaat.
Omdat de wet uitgaat van een integrale risicobenadering voor de arbeidsomstandigheden, is de werkgever ook nu al wettelijk aansprakelijk indien er onvoldoende aandacht is geweest voor cyberfysische risicoaspecten. Onvoldoende aandacht voor informatiebeveiliging waardoor letsel of dood is opgetreden of op andere wijze de veiligheid van personen negatief is beïnvloed, is dus verwijtbaar. Het is dus verstandig om aandacht in de risico-inventarisaties en –evaluaties te geven aan het risico van arbeidsonveilige situaties door cyberverstoring, hacking, malware of signaalverstoring, dan wel op andere wijze via "cyberspace" geïnitieerde procesverstoringen.
Dit risico is niet denkbeeldig. Malware dringt al regelmatig zonder mededogen cyberfysische systemen binnen en een deel van de hackersgemeenschap 'speelt' met cyberfysische systemen zonder zich daarbij rekenschap te geven dat dit een veiligheidsrisico voor mensen op kan leveren. Gezien de snelle technologische ontwikkelingen en de toenemende verbondenheid van systemen en processen, worden de dreigingen alsmaar groter.
De Arbowet gaat uit van een integrale benadering van de veiligheid van het werk en de zorg voor de gezondheid van de medewerkers. Voorkomen aan de bron is beter dan genezen. U als informatiebeveiliger en uw bedrijf zijn dus aan zet, maar hoe?

Gebrek aan steun

Volgens de Arbowet mag een bedrijf een Arbodienst inschakelen om te helpen bij de Arbo-veiligheid. Helaas hebben Arbodiensten (nog) weinig kennis van cyberfysische risicoaspecten. Sterker nog, er zal met de intentie van de Arbowet zelf een interpretatie gemaakt moeten worden over wat de juiste veilige aanpak is. Soms betekent dat zelfs dat een werkgever en zijn werknemers net niet moeten doen wat de Arbowet stelt! Een voorbeeld hiervan is artikel 11 lid c, dat een werknemer verplicht om "de op arbeidsmiddelen of anderszins aangebrachte beveiligingen niet te veranderen of buiten noodzaak weg te halen en deze op de juiste wijze te gebruiken". Logisch voor fysieke beveiligingsmaatregelen als een beschermkap. Maar hoe ga je hiermee om als het bedrijfsbeleid is dat iedere twee maanden of bij vertrek van een medewerker alle wachtwoorden oftewel een aangebrachte

(informatie)beveiliging veranderd moeten worden? Wijziging van een wachtwoord van een machine of robot staat daarmee haaks op de wet maar volgt wel de intentie van de wet.
Ook de Europese machinerichtlijn [4] en bijbehorende CE-markering geven nauwelijks tot geen handvatten om het informatiebeveiligingsrisico en de cyberfysische invalshoek die een risico kan vormen voor werknemers te beteugelen.
Conform de 2006/42/EG-richtlijn hoeven de makers en systeemintegratoren van apparatuur en machinerieën in hun risicoafwegingen nog geen rekening te houden met informatiebeveiligingsaspecten (Annex I - principes). Ze hoeven dan ook geen informatiebeveiligings¬ ¬handleiding op te leveren (artikelen 5 en 13) of speciale informatiebeveiligingsmaatregelen te nemen (artikel 9).
Ook bevat de machinerichtlijn, net zoals de eerder aangehaalde Arbowet, zelfs veiligheid¬verlagende verplichtingen als we de artikelen strikt beschouwen vanuit een informatiebeveiligingsoptiek. De artikelen van de richtlijn kennen weliswaar een aantal ontsnappingsclausules, maar een duidelijker handreiking voor de informatiebeveiliging van machinebesturingen zou aan de bron kunnen helpen bij het veilig houden van de werkvloer. Denk bijvoorbeeld aan een verbod tot het gebruik van 'fabrieksdefault' wachtwoorden en de noodzaak tot het opleveren van een handleiding informatie¬veiligheid bij een apparaat of machine.

Uw aanpak?

Er wordt op het moment gewerkt aan de vernieuwing van de Europese machinerichtlijn. Verwacht mag worden dat cyberfysische systemen in de toekomst ook explicieter in de Arbowet en bijbehorende Arborichtlijnen een plaats krijgen. Tot dat moment kan een maker, leverancier of systeemintegrator in de tussentijd kiezen voor het bieden van integrale veiligheid bij de bron waarbij het informatiebeveiligingsrisico in het hele ontwerp-, constructie- en onderhoudsproces meegenomen wordt. Het bieden van een integrale informatiebeveiligingsbenadering in producten kan enerzijds dergelijke bedrijven een concurrentievoordeel opleveren en u anderzijds meer zekerheid.

In ieder geval dient u als informatiebeveiliger als expert uw werkgever te wijzen op dit risico en hem te ondersteunen in de Arbo-risicoanalyse en –evaluatie. Zoals gezegd, de werkgever blijft integraal verantwoordelijk voor een veilige werkomgeving en de gezondheid van de werknemers. Het is daarom zaak om ook in de dagelijkse operatie aandacht te besteden aan de informatiebeveiliging van arbeidsmiddelen. Anders zullen ontwikkelingen als computergestuurde machinerieën, autonome voertuigen, robots en andere Internet-of-(Every)Things ineens voor ongedacht risico op de werkvloer zorgen. Let hierbij sterk op de directe en indirecte (bijvoorbeeld USB-)koppelingen tussen arbeidsmiddelen en interne en publieke netwerken, waaronder het internet. Een handreiking voor uw analyse is de veiligheidskaart welke eerdaags op het Arboportaal [5] zal verschijnen en die tezamen met een uitgebreider rapport te vinden is op [6].

In risicoanalyses wordt er vaak van de juiste intentie van handelen uitgegaan bij medewerkers. Echter veel informatiebeveiligingslekken ontstaan door onbewust onbekwame handelingen. Denk hierbij aan een medewerker die het ene moment een internetgame op de bedrijfslaptop speelt en het volgende moment op diezelfde laptop bij een grote klant inbelt om een procesverstoring te verhelpen; een operator die zijn mobiel oplaadt via een usb-aansluiting op een bedrijfssysteem, of een medewerker die met een USB de 'air gap' van een gesloten systeem verbreekt. Elk van deze handelingen kan een mogelijk informatiebeveiligingsrisico opleveren die resulteert in een onveilige werkomgeving met risico voor lijf en ledematen van werknemers.

Links

[1] Arbeidsomstandighedenwet 1998, http://wetten.overheid.nl/BWBR0010346

[2] Verliefd op Onveiligheid, Eric Luijf, InformatieBeveiliging, (15) #3, 2015, pp 10-12.

[3] Onbewust Onveilig, H.A.M. Luijf, Informatiebeveiliging, nr. 4, 2012, pp 4 - 7.

[4] RICHTLIJN 2006/42/EG VAN HET EUROPEES PARLEMENT EN DE RAAD van 17 mei 2006 betreffende machines en tot wijziging van Richtlijn 95/16/EG (herschikking), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:nl:PDF

[5] Veilige Arbeidsmiddelen en Cybersecurity, Arboportaal, 2016. Online: http://www.arboportaal.nl/

[6] Opkomende risico's voor arbeidsveiligheid als gevolg van IT-koppelingen van en tussen arbeidsmiddelen, TNO-rapport 2016 R10096 en de veiligheidskaart. Online: https://www.tno.nl/nl/aandachtsgebieden/gezond-leven/prevention-work-health/gezond-veilig-en-productief-werken/veilig-werken/

PERSBERICHT

RONALD PRINS 'ALUMNUS VAN HET JAAR 2016'

Ronald Prins, CTO en medeoprichter van Fox-IT is Alumnus van het jaar 2016 van de TU Delft. Sinds 2011 reikt het Universiteitsfonds Delft de prijs 'Alumnus van het Jaar' uit. De prijs is voor bijzondere alumni die hun sporen hebben verdiend in de wereld van innovatie en onderzoek, maar ook om studenten te inspireren bij hun studie- en carrièrekeuzes. Op donderdag 2 juni heeft Anka Mulder, lid van het College van Bestuur, de 'Alumnus van het Jaar 2016' award uitgereikt aan Ronald Prins.

Prins ontvangt de award voor zijn baanbrekende werk in het bestrijden van cybercriminaliteit. Anka Mulder namens de jury: "Door als expert op te treden in de media geeft Prins techniek een gezicht bij het grote publiek. Hij is een schoolvoorbeeld van een man die van zijn hobby zijn werk heeft gemaakt, zijn hart volgde en hiermee groot succes behaalde. Dit maakt hem niet alleen een topondernemer en ambassadeur van de TU Delft, maar ook een grote inspiratiebron voor de huidige en toekomstige studenten. Hier zijn we als TU Delft trots op. Daarom maken we boegbeelden zoals Ronald Prins graag zichtbaar met de 'Alumnus van het Jaar' award en de 'Alumni Walk of Fame'". Ronald Prins studeerde in 1994 af aan de TU Delft, Technische Wiskunde. In 1999 richtte Prins samen met mede-TU-Delft-alumnus Menno van der Marel Fox-IT op. Sinds de oprichting is Fox-IT uitgegroeid tot een van de meest toonaangevende bedrijven in internetbeveiliging. Het bedrijf werd vorig jaar overgenomen door de Britse NCC Group.

Over Fox-IT

Fox-IT voorkomt, onderzoekt en beperkt de meest serieuze dreigingen door cyberaanvallen, datalekken of fraude met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. In haar aanpak combineert het bedrijf slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. Fox-IT ontwikkelt producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

Kijk voor meer informatie op https://www.fox-it.com/nl/

Mr. Rachel Marbus
@rachelmarbus op Twitter

HET VERGETEN KIND

1. *Geen enkel kind mag worden onderworpen aan willekeurige of onrechtmatige inmenging in zijn privéleven, in zijn gezinsleven, zijn huis of zijn briefwisseling, noch aan enige onrechtmatige aantasting van zijn eer en goede naam.*
2. *Het kind heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.*

- VN Kinderrechtenverdrag, artikel 16

Pedagogen en psychologen luiden de alarmbel. Het is waarlijk slecht gesteld met de privacy van het (hulpbehoevende) schoolgaande kind. Het NVO (Nederlandse Vereniging van pedagogen en onderwijskundigen) en NIP (Nederlands Instituut van Psychologen) hielden een enquête onder hun leden. In de praktijk zien zij een gebrekkige beveiliging, ongebreidelde toegang tot gegevens en verstrekkingen zonder toestemming. Maar liefst 73% van de ondervraagden maakt zich ernstig zorgen over de privacy van het kind.

"Pedagogen en psychologen voelen zich vaak alleen staan in hun pleidooi binnen scholen om (meer) aandacht aan privacy te besteden", meldt het bericht op de website van NVO. Het bericht van halverwege juni haalde het landelijke nieuws niet. Bij mijn weten werd het zelfs niet door privacypromotende nieuwsplatformen opgepakt. En dat terwijl de constateringen toch behoorlijk ernstig zijn. Resultaten van psychodiagnostisch onderzoek zijn vaak voor alle werknemers van de school toegankelijk, gegevens van leerlingen worden zonder toestemming gedeeld met bijvoorbeeld jeugdhulp of wijkteams en soms weten zelfs de ouders van het kind niet eens dat het kind wordt onderzocht.

Er bestaan vele prachtige digitaal en privacy georiënteerde leerprogramma's en initiatieven. We leren kinderen hoe zij hun eigen privacy moeten beschermen in de online wereld en leren hen aldaar veilig navigeren. We leren hen dat ze om de privacy van andere kinderen moeten denken en dat ze die naaktfoto's van Elsje niet naar de hele klas moeten appen. We leren hen een goed wachtwoord te kiezen wat voor een ander moeilijk te raden is en dat ze dat wachtwoord niet moeten delen.

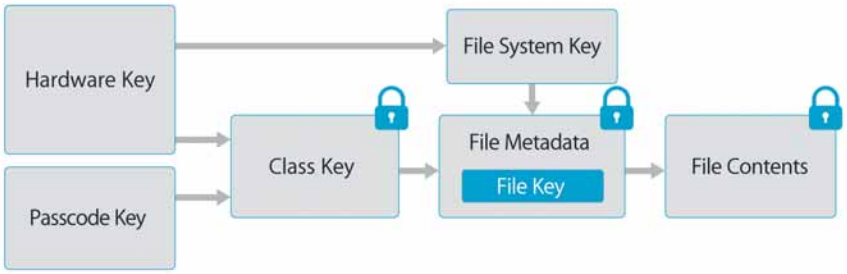
We zijn wat vergeten

We zijn vergeten de leraren te leren dat ze de privacy van het kind dienen te respecteren en te beschermen. Het zal waarschijnlijk geen onwil zijn, maar veel eerder onwetendheid. En privacy is groter dan alleen maar digitale privacy. We moeten terug naar de tekentafel en leraren leren dat privacy een grondrecht is en hoe zij het recht op privacy van "hun" kinderen kunnen beschermen.

En, eerlijk is eerlijk, tot op de dag van vandaag had ik eigenlijk ook nog niet gekeken naar het privacybeleid van de school van mijn dochter. Ik weet dat ze prudent met foto's van kinderen op de website omspringen indien daarom gevraagd wordt. Maar dat is eigenlijk alles wat ik weet. Op de website vind ik niets over privacy. In de schoolgids ook niet. Gelukkig staat er wel een emailadres van de directrice in. Toch maar even gemaild en voorzichtig gevraagd of ik misschien gewoon niet goed gekeken had…

APPLE VS FBI:
DE FEITEN OP EEN RIJTJE

In februari 2016 beval de FBI Apple mee te werken aan het doorzoeken van de iPhone van één van de (omgekomen) daders van de schietpartij in San Bernardino. Apple weigerde dat. De FBI ondernam juridische stappen, maar maakte vlak voor de eerste hoorzitting bekend de telefoon te kunnen ontgrendelen via een (vooralsnog) onbekende methode die tegen betaling is verworven van een (vooralsnog) onbekende derde. Hoe zat het precies met het FBI-bevel aan Apple? In dit artikel de zaken nog eens op een rijtje, met aandacht voor een aantal technische details van iOS.



Figuur 1 - Diagram van sleutels en versleuteling op iOS. Bron: [1]

Versleuteling: de UID en passcode

De telefoon van de dader betreft een iPhone 5c met iOS 9. Sinds iOS 8 is de 'Data Protection'-functie, opslagversleuteling, standaard ingeschakeld. Op iOS 9 werkt dat op hoofdlijnen als volgt [1]:

Er is sprake van twee geheime codes. De eerste geheime code is de 'Passcode Key', kortweg 'passcode': dat is de code die de gebruiker instelt bij ingebruikname van het iOS-device. iOS 9 vraagt de gebruiker een 6-cijferige code in te stellen, maar de gebruiker kan ook een veel langere alfanumerieke code opgeven.

De tweede geheime code is de 'Hardware Key', ook wel 'Unique Identifier' of kortweg 'UID': dat is een 256-bits AES-sleutel die tijdens het fabrikageproces van de CPU-chipset (A6, A7, A8, enz.) wordt gegenereerd en in de hardware zit ingebakken. Op iOS-devices met een A7-chipset of nieuwer, zoals de iPhone 5s en de iPhone 6, bevindt de UID zich in de 'Secure Enclave', een co-processor met een door Apple geminimaliseerde versie van ARM TrustZone. De iPhone 5c, het model waar het bij San Bernardino om gaat, heeft geen Secure Enclave. Om dit artikel ook relevant te houden voor gebruikers van nieuwere iOS-devices, wordt toch enkele malen gerefereerd aan de Secure Enclave.

Figuur 1, afkomstig uit Apple's documentatie, geeft weer welke sleutels worden gebruikt. Op iOS vindt de versleuteling plaats op bestandsniveau, afhankelijk van de 'Protection Class' die aan een bestand is toegewezen. Voor elk bestand wordt een random sleutel gegenereerd, de 'File Key'. Daarmee worden de gegevens in het bestand feitelijk versleuteld. Er zijn vier klassen: 'Complete Protection', 'Protected Unless Open', 'Protected Until First User Authentication' en 'No Protection'. Elke klasse heeft een eigen sleutel, de 'Class Key', die wordt gebruikt om de 'File Key' te versleutelen. De versleutelde 'File Key' wordt opgeslagen in de metadata van het bestand. Die metadata zelf is versleuteld met een 'File System Key', die wordt gegenereerd tijdens de installatie van iOS en wordt opgeslagen in een snel wisbaar gedeelte van het flashgeheugen. De 'File System Key' dient louter als schakel in het mechanisme voor remote wipe en auto-erase. Wanneer de gebruiker de passcode wijzigt, wijzigt alleen de versleuteling van de 'Class Keys'. Die werkwijze voorkomt dat bij elke wijziging van de passcode alle bestanden volledig opnieuw moeten worden versleuteld. De 'File Key' wijzigt dus niet. Het is niet bekend hoe iOS de random sleutels genereert en hoe random deze precies zijn.

Van de passcode en de UID wordt via PBKDF2 een sleutel afgeleid. Het aantal PBKDF2-iteraties is volgens Apple zo afgestemd dat 80ms (hardwarematige) vertraging per inlogpoging wordt geïntroduceerd.
Bestanden met de klasse 'Complete Protection' maken gebruik van een 'Class Key' die is versleuteld met een sleutel die wordt afgeleid van de passcode en UID. Dat geldt ook voor bestanden met de klassen 'Protected Unless Open' en 'Protected Until First User Authentication'. Alleen bij bestanden met de klasse 'No Protection' is dat anders: de 'Class Key' van deze bestanden is versleuteld met alleen de UID. Dat is bijvoorbeeld nodig voor om het besturingssysteem te kunnen

Matthijs Koot is senior security consultant bij Madison Gurkha. Hij is bereikbaar via koot@cyberwar.nl en actief op Twitter: @mrkoot. Dit artikel is geschreven op persoonlijke titel.

Hoe achterhaal je de passcode? Hoe random de passcode is, en of iets of iemand meegluurde toen de gebruiker deze instelde en sindsdien invoerde, is op voorhand niet te zeggen

laten booten tot aan het passcode-scherm. De 'File Key' en 'Class Key' worden vanaf A7-chipsets nimmer in het normale geheugen verwerkt; de 'key wrapping' (conform RFC 3394) vindt daar plaats binnen de Secure Enclave, en de Secure Enclave spreekt met minder vertrouwde delen van de hardware tijdelijke sleutels af als 'toegangscontrole' voor het versleutelen en ontsleutelen.

Hoe kom je achter de UID en passcode?

Hoe achterhaal je de passcode? Hoe random de passcode is, en of iets of iemand meegluurde toen de gebruiker deze instelde en sindsdien invoerde, is op voorhand niet te zeggen. Als de passcode alleen bij de (in dit geval overleden) dader bekend is, dan zal in beginsel moeten worden gedacht aan brute-force proberen. Het brute-forcen van een alfanumerieke passcode van 6 cijfers en kleine letters zou volgens Apple vanwege de 80ms (hardwarematige) vertraging maximaal 5.5 jaar duren. Gemiddeld zal het in de helft van die tijd lukken. Natuurlijk kunnen voor de hand liggende combinaties eerst worden geprobeerd: '000000', '123456', '654321', betekenisvolle datums, postcodes, enz.; met een beetje geluk is het dan veel eerder raak. Heel soms zal keyspace-reductie mogelijk zijn op basis van vetvlekken op het schermpje, daar waar zich toetsen van het on-screen toetsenbord bevinden.

Een eerste probleem bij het brute-forcen is dat iOS na 5 passcode-pogingen een minuut blokkering oplegt voordat een volgende poging kan worden gedaan; na 6 pogingen een blokkering van vijf minuten, etc.; en na 9 pogingen een blokkering van een uur. Na 10 foute pogingen moet het device op iTunes worden aangesloten om een restore uit te voeren. Daarbij gaan gegevens die op het device zijn toegevoegd sinds de laatste backup verloren, net als bijvoorbeeld de cache van on-screen toetsaanslagen (die, voor zover mij bekend, niet in de backup staat). Daarna zijn opnieuw 10 pogingen mogelijk. Op die manier kan een passcode in principe brute-force worden achterhaald, maar erg praktisch is dat niet.

Een tweede probleem is de auto-erase-functie: indien deze is ingeschakeld (standaard uitgeschakeld), dan wordt na 10 foute passcode-pogingen de 'File System Key' gewist. Op dat moment kunnen de bestandsmetadata en bestanden met de klasse 'No Protection' niet meer worden ontsleuteld, en het besturingssysteem daarom niet meer booten. De documentatie van Apple vermeldt overigens niet wat bij de auto-erase gebeurt met de versleutelde bestanden en metadata, waaronder dus ook gebruikersgegevens; vermoedelijk blijven deze, versleuteld, in het flashgeheugen aanwezig.

Dan de UID. Hoe achterhaal je die? Hoe random de UID is, en of iets of iemand meegluurde bij het fabricageproces, is niet bekend. Volgens Apple wordt de UID niet vastgelegd bij Apple of Apple's leveranciers [1]. Op iOS-devices met de A6-chipset, zoals de iPhone 5c van de dader, is de UID volgens Snowden te achterhalen via 'chip decapping' ([4]). Het is denkbaar dat de UID ook kan worden gevonden door deze uit het werkgeheugen van de A6-chipset te dumpen, mits de relevante pin-outs kunnen worden geïdentificeerd en de signalen op die pins goed kunnen worden geinterpreteerd. Op devices met een Secure Enclave wordt de UID volgens Apple nooit in het werkgeheugen verwerkt, en zou dan (nog) veel moeilijker te achterhalen zijn.

Als de UID niet bekend is, dan zou ook die moeten worden geraden, wil men kunnen brute-forcen via het rechtstreeks aanspreken van het flashgeheugen in plaats van de normale kanalen. Aangezien de UID 256 bits lang is, is dat onwerkbaar. Vanaf de A7-chipset zou het vanwege de Secure Enclave bovendien niet mogelijk zijn om op deze wijze een brute-force-aanval uit te voeren, omdat de extra vertraging per inlogpoging dan niet door de iOS-software, maar door de Secure Enclave wordt afgedwongen. Om die vertraging te omzeilen zou aangepaste Secure Enclave-firmware nodig zijn.

Ten overvloede: bestanden met de klasse 'No Protection' zijn toegankelijk voor een ieder met fysieke toegang tot het device, zonder de passcode te kennen. De FBI kan dus reeds bij de gegevens in die bestanden; maar zal daar weinig spannends vinden. Ontwikkelaars van iOS-apps beslissen trouwens zelf welke klasse ze toepassen voor opslag van gebruikergegevens, en

zouden dus ook 'No Protection' kunnen kiezen; in dat geval zijn de gegevens niet beschermd bij diefstal of verlies van het device.

Het FBI-bevel

De FBI eiste van Apple een methode die 1) "will bypass or disable the auto-erase function whether or not it has been enabled", en 2) "will enable the FBI to submit passcodes to [the device] for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol available on [the device]" (want de passcode kan normaal alleen via het on-screen toetsenbord worden ingevoerd), en 3) "will ensure that when the FBI submits passcodes to [the device], software running on the device will not purposefully introduce any additional delay between passcode attempts (...)". De FBI wil dus ongelimiteerd en zonder softwarematig geïntroduceerde vertraging tussen passcode-pogingen geautomatiseerd passcodes kunnen uitproberen via een kabeltje, Bluetooth of Wi-Fi, zonder te riskeren dat de auto-erase-functie wordt getriggerd.

Technisch gezien kan Apple aan de eis van de FBI voldoen door een aangepaste versie van iOS beschikbaar te stellen. Een Apple-executive sprak in die context over "GovtOS", anderen trokken "FBI" en "iOS" samen tot "FBiOS". Het iOS-beveiligingsmodel maakt dat nieuwe iOS-firmware door een iOS-device alleen wordt geaccepteerd indien deze digitaal is ondertekend onder Apple's eigen root CA, waarvan het certificaat op iOS-devices is opgeslagen (in de BootROM). Zonder zo'n ondertekening weigert een iOS-device de firmware. Een door Apple ondertekende variant van iOS zou via de Device Firmware Upgrade-functie (DFU) als ramdisk in het werkgeheugen van een inbeslaggenomen device moeten worden geladen en uitgevoerd. Dat kan zonder passcode. Indien de gebruiker de Find My iPhone-functie heeft ingeschakeld, zijn Apple ID-credentials nodig, maar daarvoor zou Apple eventueel een bypass kunnen maken voor de FBI.

Op devices met een A7-chipset of nieuwer worden de extra vertraging en auto-erase afgedwongen door de Secure Enclave. Maar naar verluidt zou de L4-firmware die in de Secure Enclave draait door Apple zelf te updaten zou zijn, zónder dat gebruikersdata wordt gewist [2, 3]. Als dat klopt, wat toch enigszins saillant zou zijn omdat via die weg de bescherming van het sleutelmateriaal kan worden afgezwakt, dan kan Apple technisch gezien ook voor devices met een A7-chipset of nieuwer voldoen aan dit FBI-bevel.

De FBI stelt in haar bevel dat de aangepaste iOS-firmware alléén moet kunnen worden uitgevoerd op het device waarop het bevel betrekking heeft, gebaseerd op unieke identifiers: "serial numbers, ECID, IMEI, etc.". Door de aangepaste firmware te binden aan unieke identifiers wordt het risico op misbruik teruggebracht, aangenomen dat de gebruikte identifiers op een vergrendeld device niet zomaar te vervalsen zijn. Maar de FBI heeft dus niet gevraagd om generieke firmware die tegen om het even welk iOS-device kan worden ingezet.

Het uitlekken van zo'n GovtOS-image heeft, op 't eerste oog, alleen gevolgen voor de veiligheid van één device. Het manipuleren van dat image om het geschikt te maken voor een ander device, of generiek te maken, eist ten minste dat een aanvaller het image zo weet te manipuleren dat een collision optreedt in het hashalgoritme dat wordt gebruikt bij het genereren van de ondertekening (de 'SHSH-blob'). De kans dat zo'n aanval kan worden uitgevoerd vóórdat de hele wereld alweer op de volgende versie van iOS draait, en de uitgelekte GovtOS-image z'n waarde heeft verloren, is waarschijnlijk klein, maar ook niet uit te sluiten. De FBI stelt in haar bevel (daarom?) dat de firmware on-site bij Apple zelf, dus op de Apple-campus in Cupertino, op het device mag worden geladen. Als de firmware de fysieke grenzen van de Apple-campus nimmer verlaat, is er minder gelegenheid voor ongewenste distributie en resteert slechts de insider threat.

Het werken met een device-specifiek GovtOS-image betekent dat voor elk toekomstig te onderzoeken device een nieuw image moet worden gemaakt. Tenzij de FBI toegang heeft tot de iOS-broncode en de private key die Apple gebruikt voor ondertekening, moet Apple dat doen. Het is best mogelijk een voldoende veilige interface op te zetten tussen de FBI en Apple.

De FBI zou de relevante versie-informatie en unieke identifiers aan Apple kunnen toezenden, en Apple vervolgens, eventueel na een out-of-band-controle, een nieuw GovtOS-image genereren.

Als de FBI de rechtszaak had voortgezet en Apple was blijven weigeren, zou de FBI volgens mediaberichten van plan zijn bruutweg toegang te eisen tot de iOS-broncode en Apple's private key. Volgens weer andere mediaberichten zou dat bij andere bedrijven reeds zijn gebeurd, op grond van de Amerikaanse FISA-wetgeving.

Backdoor-light

Het feit dat Apple in staat is een iOS-variant te maken die via DFU kan worden geladen, kan in zekere zin al worden opgevat als backdoor. Zij het eentje waarbij nog steeds de passcode moet worden geraden; een backdoor-light, zeg maar.

Het is niet uitgesloten dat andere methoden bestaan om gegevens te achterhalen of de passcode te brute-forcen; voor de iPhone 5c bleek dat laatste het geval. Indien een gebruiker iCloud-backups heeft ingeschakeld, dan staat een gedeelte van de gegevens op servers van Apple, versleuteld met een sleutel die bekend is bij Apple (dus zonder passcode of UID). En indien een device binnen 48 uur sinds de laatste ontgrendeling niet is uitgeschakeld of gereboot, en wordt gekoppeld met een computer die door het device reeds wordt vertrouwd, is het eveneens mogelijk om toegang tot sommige gegevens te krijgen: dan start de synchronisatie namelijk zonder dat de passcode opnieuw hoeft te worden ingevoerd. Maar dat zijn toevalstreffers die zich in de opsporingspraktijk vermoedelijk zelden voordoen, en waarbij bovendien onbekend blijft of er belangrijke gegevens op het device staan die niet in de backup staan. Bij San Bernardino bleek dat trouwens niet het geval.

Techbedrijven en overheden

Bij San Bernardino staat buiten kijf dat het gaat om een dader van de moord op 14 personen, is de betrokkene dood, en heeft de eigenaar van de telefoon, de werkgever van de dader, toestemming gegeven voor ontgrendeling. Tóch weigert Apple. 'Apple vs FBI' gaat dus niet over de (on)mogelijkheid om toegang te krijgen tot gegevens op deze ene iPhone, maar om de vraag in hoeverre van techbedrijven mag worden verlangd dat zij inspanningen leveren ter ondersteuning van opsporings- en inlichtingenwerk. Ook de (legitieme) vijand gebruikt moderne technologie en kan beschikken over een niveau van beveiliging dat, kijkend naar bijvoorbeeld iOS-devices met de Secure Enclave, toch behoorlijk hoog begint te worden. Dat is niet goed of fout; het is gewoon een realiteit.

Dat Apple zegt zes tot tien engineers twee tot vier weken te moeten inzetten om de gevraagde software te maken, is van ondergeschikt belang in de discussie; dat argument gaat over kosten en beschikbaarheid van personeel. Er zijn belangrijkere vragen: als Apple dit verzoek inwilligt, kunnen dan ook andere techbedrijven dit soort verzoeken tegemoet zien? Moet een medewerkingsplicht zich kunnen uitstrekken tot het op afstand laten inschakelen van een microfoon of camera? En tot toegang tot broncode en geheime sleutels? Moeten verzoeken van andere landen worden ingewilligd? Wie beslist daarover, en hoe?

Betogen dat techbedrijven per definitie geen medewerking moeten verlenen aan opsporingsdiensten en inlichtingen- en veiligheidsdiensten, staat gelijk aan het ontkennen van de

Had Apple moeten meewerken aan het verzoek van de FBI? Er zijn op z'n minst heldere voorwaarden, waarborgen en effectief toezicht nodig

rechtsstaat. In een rechtsstaat worden belangen immers altijd tegen elkaar afgewogen, en zijn er geen belangen die te allen tijde als troefkaart kunnen worden gespeeld. In verschillende rechtsstaten, waaronder Nederland, is reeds sprake van bepaalde medewerkingsplichten: bijvoorbeeld de plicht voor aanbieders van openbare communicatienetwerken om aftapbaar te zijn. Discussie over medewerkingsplichten ging en gaat, ook in het debat over de vernieuwing van de wet op de inlichtingen- en veiligheidsdiensten (wetsvoorstel Wiv20xx), niet of nauwelijks om een principieel 'voor' of 'tegen', maar vooral over voorwaarden (kosten, verantwoordelijkheden, beveiliging, schade), toezicht, en wettelijke waarborgen (bescherming van grondrechten, noodzaak/proportionaliteit/subsidiariteit).

Dat misbruik niet is uit te sluiten, is al eens gebleken bij tapvoorzieningen. Zo werd de mobiele telefoon van de premier van Griekenland aldaar illegaal afgeluisterd via (zeer verfijnde) spyware op een tapvoorziening bij de betrokken telecomaanbieder [5]. Zo'n incident is echter geen bewijs dat tapvoorzieningen massaal onveilig zijn en worden misbruikt door onbevoegden (of bevoegden). Gezonde scepsis over opsporings- en inlichtingenbevoegdheden is een deugd, maar vooralsnog moet worden vastgesteld dat er weinig voorbeelden bekend zijn van (overtuigende) casussen van misbruik. Als het klopt dat bij de NSA in een decennium tijd een dozijn LOVEINT-incidenten hebben gespeeld, en er niet óók tientallen of honderden niet-opgemerkte of geheimgehouden gevallen van oneigenlijk gebruik zijn, is dat toch niet heel slecht voor zo'n enorme organisatie. Zonder daarmee de ernst van die incidenten te ontkennen of te concluderen dat de status quo helemaal jofel is. Het blijft tandenknarsen.

Afsluiting

Had Apple moeten meewerken aan het verzoek van de FBI? Er zijn op z'n minst heldere voorwaarden, waarborgen en effectief toezicht nodig. De huidige situatie, waarin de FBI vertrouwt op een geheime methode die (volgens de FBI) niet aan Apple bekend is gemaakt, is in elk geval ook niet florissant: immers, met die methode kan de FBI --of elke ander die de methode kent-- zelfstandig élke (gelijksoortige) iPhone ontgrendelen (generiek), terwijl de FBI van Apple 'slechts' vroeg één apparaat te ontgrendelen (specifiek). Het is denkbaar dat de FBI de derde partij al langer voor handen had en simpelweg hoopte dat Apple onder druk zou buigen voor het bevel, om zo over meer dan één methode te beschikken zonder daadwerkelijk een juridisch precedent te veroorzaken. Want ook voor de FBI is de uitkomst van zo'n rechtszaak onzeker, zoals hen duidelijk zal zijn geworden uit de massale bijval die Apple vanuit de (advocaten van de) Amerikaanse techsector en burgerrechtenbewegingen wist aan te wakkeren.

Links

[1] Versie september 2015, bezocht 2 april 2016 https://www.apple.com/business/docs/iOS_Security_Guide.pdf
[2] https://blog.trailofbits.com/2016/02/17/apple-can-comply-with-the-fbi-court-order/
[3] https://twitter.com/JohnHedge/status/699882614212075520
[4] http://www.ibtimes.co.uk/apple-vs-fbi-snowden-says-decapping-can-crack-iphone-used-by-san-bernardino-attacker-syed-farook-1545397
[5] http://spectrum.ieee.org/telecom/security/the-athens-affair

SECURITY VOOR INTERNET OF THINGS

Er wordt veel over gesproken maar wat het precies is blijft vaak in het midden. Vaak zijn IoT-apparaten kleine sensoren die een bepaalde waarde uit de fysieke wereld kunnen halen en die (in)direct delen met andere apparaten, bijvoorbeeld een temperatuursensor. Een andere mogelijkheid is een IoT-apparaat dat informatie ontvangt uit het netwerk en op basis daarvan acties kan ondernemen die effect hebben op de fysieke wereld, bijvoorbeeld een thermostaat. Uiteraard zijn combinaties van bovenstaande ook mogelijk.

De bovenstaande beschrijving geeft wel een richting maar evenals de verschillende definities, die helpen u waarschijnlijk niet om onderscheid te maken tussen al veel langer bestaande op internettechnologie gebaseerde toepassingen en IoT-specifieke toepassingen. Om hier toch enige handvatten aan te reiken hanteren we voor dit artikel een aantal criteria die u in staat stellen te beoordelen of iets behoort tot het IoT-domein of niet.

Het doel van deze criteria is niet om te komen tot een nieuwe definitie maar om beter te kunnen bepalen of iets wel of niet IoT is. Dit helpt om vervolgens scherper te krijgen welke eisen er aanvullend zouden kunnen gelden bovenop reguliere eisen en maatregelen die nu al gemeengoed zijn. Uiteindelijk zullen we in dit artikel een aantal handvatten geven om na te denken over de beveiligingsaspecten van deze apparaten. Op basis van de criteria laten we zien welke specifieke aspecten voor IoT van toepassing zijn. Dit laat ook zien waarom IoT toch anders is dan andere op internet aangesloten apparaten en biedt u richting voor het treffen van passende maatregelen. Hieronder vind u en voorzet voor deze criteria:

a) **IoT heeft een directe relatie met de fysieke wereld**
b) **IoT is verbonden (draadloos of bekabeld)**
c) **Primaire functies van IoT zijn gericht op meten en/of beïnvloeden van de fysieke wereld**
d) **Optioneel: Secundaire functies van IoT zijn gericht op het analyseren van informatie om te redeneren over de fysieke wereld of voorbereiden op het beïnvloeden van de fysieke wereld**

In de onderstaande tabel staan een aantal voorbeelden met daarbij aan welke criteria dat voorbeeld voldoet.

Omschrijving	Voldoet aan criteria	Wel of niet IoT	Mogelijk aanvullende eisen ivm IoT
Een op internet aangesloten koelkast met een ingebouwd scherm, waarop via een webwinkel boodschappen besteld kunnen worden. We gaan er vanuit dat vanuit de webwinkel niet direct een fysiek systeem aangestuurd wordt. Mocht dat wel het geval zijn dan, dan zou dat deel nog onder criterium D kunnen vallen.	B C (D)	Nee	
Een op internet aangesloten koelkast, die met behulp van sensoren kan bepalen welke producten niet meer vers zijn, of waar te weinig voorraad van is. D is van toepassing als de benodigde informatie voor het bepalen van versheid over producten uit een backoffice-systeem komt.	A B C (D)	Ja	Omdat er gekeken naar de fysieke staat van het in de koelkast aanwezige voedsel, zou kunnen betekenen dat er voor deze specifieke toepassing voldaan moet worden aan eisen met betrekking tot de voedselveiligheid.
Een app op een smartphone die bijhoudt hoe vaak een oefening is uitgevoerd. Op basis van hoe vaak een app of activiteit in een app gestart is.	B	Nee	
Een app die gebruik kan maken van de microfoon van telefoon om knallen waar te nemen. In de backoffice wordt dan op basis van meerdere telefoons bepaald waar vuurwerk in een wijk explodeert.	ABCD	Ja	
Televisie verbonden met internet waarmee on-demand-video te kijken is.	B	Nee	
TV die op basis van omgevingsgeluid van zender wisselt of volume regelt. Eventueel kan de analyse van de geluiden in een backoffice uitgevoerd worden.	ABC (D)	Ja	Door het opnemen van omgevingsgeluid, kan dit voor de persoonlijke levensfeer een zeer hoge impact hebben.

Als uitgangspunt kan genomen worden dat de lifecycle van een IoT-apparaat relatief laag is en moet ook op die manier behandeld worden

Aantal voor security relevante kenmerken van IoT

Apparaten voor Internet of Things zijn de afgelopen jaren ontzettend populair geworden. Bedrijven zien hier een kans en proberen zo snel mogelijk hiervan gebruik te maken. Dit doen ze door nieuwe kleine apparaten te maken, dan wel door bestaande producten aan te passen door verbindings-functionaliteit erbij te doen.

Door de snelle ontwikkeling wordt er vaak niet direct gekeken naar de veiligheid van deze apparaten. Door de grote potentie en lage kosten voor het toevoegen van netwerkfunctionaliteit, komen in een rap tempo nieuwe diensten en producten op de markt, die een alternatief vormen voor bestaande diensten en producten. Deze introductie kan soms een zeer disruptief karakter hebben, waarbij rekening gehouden moet worden dat naast de voordelen die hiermee op korte termijn voorhanden zijn, ook nieuwe security-uitdagingen zich voordoen. Het inzetten van IoT-sensoren en apparaten zorgen ervoor dat data uit de sensoren maken dingen zichtbaar voor een groter publiek die eerder niet zichtbaar waren. Als dit eenmaal zichtbaar is kan dit leiden tot een scope creep of zelfs een verschuiving van belangen.

Naast de security-vraagstukken die samenhangen met de technologie, kunnen er ook specifieke aandachtspunten voortkomen uit het toepassingsgebied van IoT. Daartoe kijken we naar een aantal voorbeelden van IoT en de specifieke randvoorwaarden die daarmee gepaard gaan.

De goedkope apparaten zorgen ervoor dat ze snel ingezet en uitgerold kunnen worden. Doordat de ontwikkeling nog in volle gang is, volgen generaties van apparaten elkaar snel op. Ondersteuning van oudere generaties houdt vaak snel op, als het al mogelijk is om de apparaten te kunnen updaten. Hier moet duidelijk rekening mee gehouden worden bij het uitrollen van IoT-apparaten. Als uitgangspunt kan genomen worden dat de lifecycle van een IoT-apparaat relatief laag is en moet ook op die manier behandeld worden.

Conclusie

Beveiliging van IoT-apparaten is in zekere zin niet anders dan beveiliging voor algemene IT. Echter, de nauwe verwevenheid met de fysieke wereld maakt dat onvoldoende beveiliging van IoT een ander type impact kan hebben dan reguliere op internet tecnologie gebaseerde systemen.

Als de trend van een relatief korte economische levensduur en continue ontwikkeling van IoT-technieken zich doorzet, kan dat ervoor zorgen dat de levensduur van IoT voor wat betreft security-ondersteuning ernstig beperkt wordt.

Voor organisaties die IoT toe (gaan) passen is het van belang om hiermee rekening te gaan houden, bijvoorbeeld door dit soort aspecten expliciet op te nemen in hun risicomanagementstrategie voor zover ze dat nog niet gedaan hebben.

In aanvulling zou het goed zijn om in de breedte een kritische houding aan te nemen in het kader van wat wel en wat vooral ook niet IoT is. Door het nu nog diffuse karakter van de terminologie blijven specifieke security-randvoorwaarden en aandachtspunten die IoT zo specifiek maakt onder het maaiveld.

Andre Smulders is senior business consultant security bij TNO. Andre is te bereiken via andre.smulders@tno.nl en te volgen via Twitter @ldr404.

Jeroen van der Ham is security-onderzoeker bij het NCSC, waar hij zich bezighoudt met IoT, en ook onderzoek naar Vulnerability Disclosure en andere ethische aspecten van security-onderzoek. Jeroen is te bereiken via jeroen.vanderham@ncsc.nl, en op Twitter onder @1sand0s.

ONDERZOEK: 4 MOBIELE SPOOFTRUCS DIE JE GEGEVENS STELEN

Mobiele malware wordt heimelijk toegevoegd aan legitieme apps

Er is onlangs onderzoek gedaan naar malware die zakelijke apps nabootsen. Het is de klassieke wolf in schaapskleren, die ervoor zorgt dat malware niet wordt opgemerkt. Onderstaand vier voorbeelden:

1. Shuanet

Wat doet het? Shuanet root een apparaat en installeert vervolgens zelf verschillende applicaties. Wat is het risico voor bedrijven? Een threat die een device kan rooten en applicaties kan installeren is zorgwekkend om een aantal redenen. Ten eerste tast het de staat van beveiliging van het apparaat aan, terwijl reguliere software-updates vaak niet meer worden ontvangen. Ten tweede root Shuanet niet alleen het apparaat, maar installeert het zichzelf op de systeempartitie, waardoor het bijna niet te verwijderen is. Zelfs resetten naar fabrieksinstellingen lost het probleem niet op. En als laatste kan malware die applicaties installeert ook ongemerkt gevaarlijke apps installeren en daarmee het apparaat en persoonlijke- alsook zakelijke data in gevaar brengen. Voorbeelden van apps die het nabootst: ADP Mobile Solutions, CamCard Free, Cisco Business Class Email (BCE), Duo Mobile, Google Authenticator, VMWare Horizon Client, Zendesk, Okta Verify.

2. AndroRAT

Wat doet het? AndroRAT is oorspronkelijk een legitiem remote administration tool die een derde partij toegang geeft tot contactinformatie, telefoon-logs, tekstberichten, locatie van het apparaat en audio. Tegenwoordig wordt het echter vooral door kwaadwillenden gebruikt. Wat is het risico voor bedrijven? Verborgen remote access-software stelt een aanvaller in staat om vanaf een mobiel apparaat toegang te krijgen tot zowel persoonlijke als zakelijke data! Voorbeelden van apps die het nabootst: Dropbox, Skype, Business Calendar.

3. UnsafeControl

Wat doet het? UnsafeControl kan contactinformatie verzamelen en naar een server van een derde partij sturen. Vervolgens kan het de contactenlijst spammen of SMS-berichten sturen naar telefoonnummers die door de zogenoemde command-and-control-servers worden doorgegeven. Wat is het risico voor bedrijven? Malware als UnsafeControl steelt contactinformatie, die voor veel bedrijven als zeer gevoelig kan worden beschouwd. Bijvoorbeeld de contactgegevens op het apparaat van een directeur of hoofd sales kunnen andere bedrijven competitief voordeel verschaffen. Voorbeelden van apps die het nabootst: FedEx Mobile, Google Keep, Remote VNC Pro, Sky Drive, PocketCloud, Skype.

4. Ooqqxx

Wat doet het? Deze applicatie bevat een advertentie-netwerk dat reclames naar je notificatiebalk pusht, pop-ups stuurt, snelkoppelingen op je homescreen plaatst en grote bestanden downloadt zonder toestemming. Het is vaak niet duidelijk dat de reclames door deze app worden veroorzaakt. Wat is het risico voor een bedrijf? Simpeler dan je denkt: als het apparaat waarop een werknemer werkt plots reclames toont en zo het werk verstoort, zal de werknemer helpdesktickets gaan indienen bij de IT-afdeling. En tijd is geld. Voorbeelden van apps die het nabootst: Mobile Learn from Blackboard, Evernote, PocketCloud, Remote Desktop, Adobe Reader, aCalendar.

Is MDM de oplossing?

Helaas is Mobile Device Management (MDM) geen 'silver bullet'. Dit type management-oplossing stelt bedrijven in staat om apps te black- en white-listen. MDM doet dit op basis van de pakketnaam van een app. Als een bedrijf bijvoorbeeld FedEx gebruikt, en de app van deze pakketdienst als geschikt voor gebruik markeert, glipt malware met dezelfde pakket-naam er moeiteloos door. Het idee dat mobiele apparaten waar MDM op draait onaantastbaar zijn voor malware is onjuist: ongeveer 33 van de 1000 apparaten waar MDM op draait hebben last van malware, blijkt uit onderzoek van Lookout. Dit is net zo vaak als bij apparaten waar geen MDM op draait. Dat betekent dat bedrijven die MDM gebruiken nog steeds in contact komen met malware, en erop moeten vertrouwen dat de beveiligingssoftware de malware zal detecteren en de problemen zal oplossen.

Lookout

Jeroen Wijdogen, werkzaam als Senior Mobile Security consultant bij Lookout en bereikbaar via jeroen.wijdogen@lookout.com

Nationale overheden maken zich zorgen over de cyberveiligheid van vitale infrastructuren. Met specifieke wet- en regelgeving probeert de Europese Unie en ook de Nederlandse overheid het risico voor de samenleving te verminderen en een adequate respons op ernstige cyberaanvallen te bieden. De vraag is of dit voldoende is om als land voorbereid te zijn op Internet Of Everything als grootschalig cyberaanvalsmedium en het risico van maatschappelijke ontwrichting. Zijn beleidsontwikkeling en responsorganisaties wel voldoende voorbereid op wat er op ons afkomt?

NIET GEKEKEN, ALTIJD MIS!

Wat zijn de nieuwe cyberdreigingen?

Nationale overheden maken zich zorgen over de cyberveiligheid van vitale infrastructuren [1]. Met specifieke wet- en regelgeving proberen de Verenigde Staten, de Europese Unie en ook de Nederlandse overheid het risico voor de samenleving te verminderen en een adequate respons op ernstige cyberaanvallen te bieden. De meeste aandacht van overheden gaat daarbij uit naar de telecommunicatiebedrijven met eigen infrastructuur en de in een land belangrijkste Internet Service Providers (ISP). Als voorbereiding op een besloten workshop van Europese ICT-regelgevers en -toezichthouders in Sankt Gallen in 2014 hebben de auteurs van dit artikel zich de vraag gesteld of er geen blinde vlekken zijn dan wel aan het ontstaan zijn, bijvoorbeeld door de Internet-of-Everything ontwikkelingen. De presentatie tijdens de workshop en de discussies hebben geleid tot een artikel in het European Journal of Risk Regulation [2]. Dit artikel gaat in op de behandelde problematiek vanuit de optiek van verantwoordelijken voor een informatieveilig Nederland en België.

Achtergrond: Vitale informatie-infrastructuur

Vitale infrastructuur en hun bescherming is van alle tijden, denk bijvoorbeeld aan de militaire wegen van de Romeinen en hun strategisch gepositioneerde legerplaatsen. In de recente historie, was de Verenigde Staten de eerste die in 1996 op presidentieel niveau aandacht ging besteden aan de bescherming van vitale infrastructuur. Het millenniumprobleem maakte duidelijk dat de samenleving aan nieuw risico blootstaat door de verwevenheid en afhankelijkheden van vitale infrastructuren. ICT-ontwikkelingen versterken dit risico.

Nederland ontwikkelde in de jaren 2003-2005 het eerste overheidsbeleid rond de bescherming van de nationale vitale infrastructuren; de Europese Commissie volgde kort daarna met een Green Paper en de zogenaamde CIP Directive [3]. Voor de vitale ICT-sector werden door Nederland de volgende vitale producten en diensten onderscheiden: vaste telecommunicatievoorziening, mobiele telecommunicatie-voorziening, internettoegang, radiocommunicatie en –navigatie, omroep en satelliet¬communicatie en –navigatie. Sinds mei 2015 onderkent Nederland de volgende vitale ICT-diensten: internettoegang en dataverkeer, spraakdiensten (mobiel en vast), satellietcommunicatie en tijd- en plaatsbepaling (GPS/Galileo). België heeft elektronische communicatie als vitale sector benoemd, maar kent nog geen indeling in vitale diensten. Andere Europese landen onderscheiden een diversiteit aan ICT-diensten als vitaal, al voeren de klassieke telecommunicatievoorzieningen, omroep en internettoegang hierin de boventoon.

De ICT-sector viel buiten de initiële uitwerking van de CIP Directive voor de Europese vitale infrastructuur. Wel is er Europese wet- en regelgeving (Regulation en Directives) voor de telecommunicatiesector waarin informatiebeveiliging een rol speelt, zoals de verplichting om ernstige ICT-beveiligingsincidenten aan ENISA te melden via de nationale toezichthouder. Deze wet- en regelgeving is door de lidstaten geïmplementeerd in de nationale telecommunicatiewetgevingen. Ook is de nationale uitwerking van de Network Information Security Directive in wording.

Is dit voldoende?

Is dit voldoende om eventuele maatschappelijke ontwrichting te voorkomen of te beperken? Onze analyse bracht een aantal blinde vlekken aan het licht welke we hieronder bespreken:

1. De categorie "top ICT-leveranciers". Op dit moment gebruiken vitale infrastructuren, organisaties, het MKB en burgers dezelfde computers, netwerkelementen en programmatuur van een kleine hoeveelheid leveranciers. Indien bijvoorbeeld een ernstige zwakte uitgebuit wordt in bijvoorbeeld een router waarvan er honderdduizenden exemplaren geïnstalleerd zijn, kan dat tot ernstige uitval van (inter)nationale dienstverlening leiden waaronder die van vitale infrastructuur. Er is al een aantal incidenten geweest waarbij maar net grote gevolgen zijn voorkomen. Denk bijvoorbeeld aan de ASN.1- en Heartbleed-kwetsbaarheden. Desondanks vallen deze leveranciers niet onder de noemer "vitaal" en ontbreken governance-afspraken.
2. De categorie "telecommunicatie- en internetdiensten". Zoals hierboven besproken kijken overheden en hun toezichthouders vooral naar de vitale grootschalige netwerken en de dienstverlening van telecommunicatiepartijen en ISP's. De rest van het internet is toch redundant met meer concurrerende aanbieders. De categorie "internetkerndiensten" wordt daarbij veelal over het hoofd gezien. Dat internet alleen werkt doordat een beperkt aantal partijen cruciale, zo niet vitale, diensten leveren ontgaat veel toezichthouders en wet- en regelgevers. Denk aan de bedrijven die de internetrouteringstabellen en de domain name server (DNS)-infrastructuur onderhouden. Ook binnen deze categorie hebben zich narrow escapes voorgedaan.
3. De categorie "overige vitale infrastructuren". Vitale processen in de vitale sectoren energie, drinkwater, watermanagement, transport en financiën zijn steeds meer ICT-afhankelijk. Ze zijn sterk afhankelijk van hierboven onder (1) genoemde leveranciers. Toezichthouders en de bestaande wet- en regelgeving voor de meeste vitale sectoren richten zich voornamelijk op de continuïteit van de dienstverlening en de fysieke veiligheid, niet op de noodzaak van cybersecurity. Dit ondanks voorbeelden van het risico voor deze sectoren zoals Stuxnet (2010), de stroomuitval in Brazilië (2005) en recent de Oekraïne (2015). Daarnaast ontbreekt het aan toezicht op de veiligheid van vitale middelen met ingebedde ICT in deze sectoren. Denk bijvoorbeeld aan het gebrek voor aandacht voor de cybersecurity van pacemakers, insulinepompen, infuuspompen en hartbewakingsapparatuur. Een ernstige cyberinbreuk op dergelijke apparatuur kan leiden tot duizenden doden in Europa. Alleen de Food en Drug Administration in de VS lijkt op dit gebied enige richtlijnen af te geven. Het toezicht in de EU en de Europese landen blijft achter.
4. De categorie "third party diensten". Bijna onzichtbaar zijn er een aantal partijen actief die als vitaal aan te merken ICT-diensten leveren waarmee hele stelsel aan dienstverlening opgehangen zijn. Sinds minister Donner om 01:00 uur 's ochtends een persconferentie gaf over DigiNotar is duidelijk dat certificaatleveranciers een sleutelrol

Eric Luijf en Marieke Klaver zijn als onderzoekers Bescherming Vitale Infrastructuur en Bescherming Vitale Informatie-infrastructuur werkzaam bij TNO. Eric en Marieke zijn bereikbaar via e-mail: eric.luijf@tno.nl en marieke.klaver@tno.nl

spelen in de e-overheidsdienstverlening en de zakelijke dienstverlening. Ook de .nl en .be top-level-domein-registrars vallen in deze categorie. Toch staan dergelijke dienstverleners niet op de vitaal-lijst van de meeste landen; de VS vormen een uitzondering daarop.

5. De categorie "consumentendiensten". Indien grote groepen burgers en MKBers het vertrouwen verliezen in ICT doordat zij gedurende meer dagen hun sociale netwerken niet kunnen bereiken, niet elektronisch kunnen winkelen of gebruik maken van overheidsdiensten en dergelijke (bijvoorbeeld door langdurige onbereikbaarheid van clouddiensten) kan de sociaalpsychologische impact de impactcriteria van de overheid voor 'wat is vitaal' benaderen. Zelfs bij een korte storing van Facebook wordt in de VS 911 al gebeld door verontruste burgers! Cybersecurity binnen deze categorie primair een taak van de dienstverlener. Toch zal de overheid er wellicht niet aan ontkomen om plannen te maken om bij grootschalige verstoring in te grijpen en hulp te bieden om mogelijke maatschappelijke onrust te voorkomen.
6. De categorie "massamarktfunctionaliteiten met ingebedde ICT". In toenemende mate zit ICT diep ingebed in consumenten- en professionele producten. Die producten communiceren via Bluetooth, Wi-Fi, Zigbee, GSM (3G, 4G, 5G) met elkaar en de wijde wereld; binnenkort komt Lora daar nog als nieuwe communicatiemogelijkheid bij. De aanstormende Internet of Everything ontwikkelingen komen vooral uit de koker van niet-traditionele ICT-bedrijven: veel van de komende grote spelers zijn nu nog startups in een schuur, of bekende bedrijven die embedded ICT in de vorm van slimme functies gaan toevoegen aan hun apparatuur. Enkele voorbeelden hiervan zijn digitale TV's, thermostaten en koolmonoxidemelders (bijv. Google Nest), slimme lampen, domotica, robots en slim witgoed als koelkasten en (vaat)wasmachines. Voor de leveranciers is de functionaliteit de eerste prioriteit. Cybersecurity komt als laatste. We spreken echter al gauw over miljoenen apparaten die bij een ernstige kwetsbaarheid een perfect aanvalsmedium vormen op vitale en belangrijke diensten. Kwetsbaarheden die een groot risico vormen voor de privacy van burgers en ook een onbewaakte achterdeur van de thuisnetwerken, maar ook –in geval van slimme elektrische apparatuur- kunnen leiden tot instabiliteit van lokale elektriciteitsnetwerken.

Duidelijk is dat bij een ernstig gebrek met grote maatschappelijke gevolgen door overheid en consument gekeken wordt naar de tussenhandelaar en de fabrikant. Maar noch de bekende fabrikanten van digitale TV's en witgoed, noch nieuwe startups met "cool gadgets" en bekende grote winkelketens, autodealers en vergelijkbare partijen zijn voorbereid op het massaal distribueren en installeren van patches voor dergelijke apparatuur. Voorbeelden hiervan zijn een recente kwetsbaarheid in de ICT van barbecues, problemen die autofabrikanten hebben bij het updaten van (sjoemel)software in vele honderdduizenden auto's en de noodzaak om de software van 230.000 zonnepanelen in Duitsland te upgraden om elektriciteitsstoringen te voorkomen.
Recent stelde de Rijksdienst voor het Wegverkeer dat zo'n 120.000 auto's die de afgelopen jaren werden teruggeroepen voor het verhelpen van een gevaarlijk gebrek dat niet gedaan hebben en nog steeds gevaarlijk rondrijden. De afgelopen jaren kwamen er steeds meer programmatuurgebreken met veiligheidsrisico aan het licht. De vraag is hoe vaak een eigenaar gaat reageren op een terugroepactie voor aanpassen van de programmatuur.

Eén ding is duidelijk: de onduidelijkheid hoe de wet- en regelgever hier enige vorm van governance over gaat voeren en of toezichthouders zich op dit risicodomein gaan richten. Maar wat als de elektriciteit in delen van Nederland en België staat te klapperen door een cybersecurity¬probleem in slimme wasmachines? Als auto's onverwachts botsneigingen krijgen? Is 'preventief ruimen' door de overheid dan de enige optie? Of moeten autodealers en winkelketens als de Mediamarkt en Intratuin de cybersecurityproblemen dan gaan oplossen? De cybersecurityuitdagingen door "Internet of Everything" voor de vitale functies van landen zijn dus groot.

Een stapje

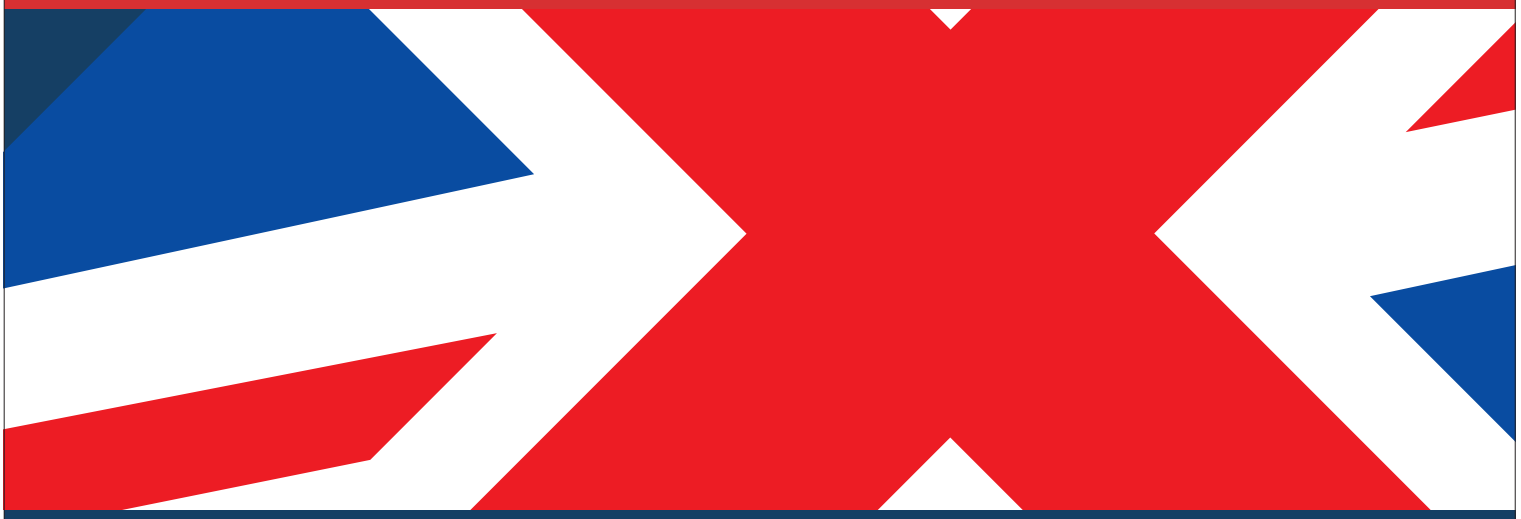
Op dit moment buigt het Nederlandse Parlement zich over een nieuw wetsvoorstel "Wet gegevensverwerking en meldplicht cybersecurity". Daarin wordt onder andere geregeld dat aangewezen vitale aanbieders iedere "inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken" aan de overheid moeten melden. Daarnaast krijgt het Nationaal Cyber Security Centrum (NCSC) de formele taak om vitale aanbieders te ondersteunen in geval van cyberdreigingen en incidenten. Sinds de herijking vitale infrastructuur in 2015 is het aantal in Nederland onderkende vitale diensten echter verschraald. Daarnaast is de uitwerking voor de ICT-sector en een aantal andere ICT-diensten nog gaande.
Maar,... zelfs met een optimistische benadering zal uit het bovenstaande duidelijk zijn dat er bij alle genoemde categorieën sprake is van blinde vlekken in de governance, waarbij de snelle Internet of Everything ontwikkelingen het risico nog eens extra versterken. Blinde vlekken die de nodige aandacht van wet- en regelgevers, toezichthouders, fabrikanten en leveranciers behoeven. Anders komen we er, waarschijnlijk veel sneller dan verwacht, in een crisis achter dat we qua wet- en regelgeving, toezicht en plannen maken niet naar voren hebben gekeken en dat geïdentificeerde lessen uit het verleden niet zijn geleerd.

Links

[1] Een groot aantal nationale definities voor vitale infrastructuur en nationale lijsten met vitale sectoren zijn te vinden op www.cipedia.eu

[2] Luiijf, E., & Klaver, M. Symposium on Critical Infrastructures: Risk, Responsibility and Liability - Governing Critical ICT: Elements that Require Attention, European Journal of Risk Regulation, Vol. 6, Issue 2 (2015). pp. 263 – 270

[3] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32008L0114&from=RO



EXIT-READY

Sometimes an enterprise has to get out of some business arrangement for some reason. It may be something the business has been considering for some time and finally comes to a decision after some trigger event, or it may occasionally be a totally unexpected requirement to find a way out, triggered by an event totally unexpected or at least uncertain. Currently, at the time of writing, the world is digesting the news that the UK has voted to leave the European Union. This was not totally unexpected but was uncertain until a few days ago.

What is clear now is that many important institutions such as the UK Government and The Bank of England have been developing two parallel plans for a long time in the run-up to the referendum. One plan for Remain and one plan for Leave. This is called 'contingency exit planning' and is an essential strategic activity for any serious business enterprise. Is your business 'exit-ready' for this or any other similar outcome? Let's hope it is.

What concerns the Attributer is the frequently reported fact that so many business enterprises have no business continuity or contingency plans at all. Because this event was anticipated, maybe those affected will have been doing some work on double scenario planning too, but what about facing exit events that are totally unexpected and unplanned?

Some years ago the Attributer was attending a conference on information security and at lunchtime had popped outside for some fresh air and a bit of a walk. Also on the pavement outside the building was another attendee pacing furiously up and down, having a conversation on his mobile phone. After the call had ended a conversation was struck up and it transpired that the gentleman had some serious trouble back at the office in another country. He was the Information Security Manager for a large Scandinavian corporation and right now he was in London, away from the office.

He explained that his company had an outsourcing arrangement for managed security services and that they were happily having such things as malware protection, firewall management and email filtering provided by a service provider with whom they had a good working relationship. He had just been informed by phone that the service provider had been acquired by a much larger service providing company, and that this new owner was not intending to offer services of this type. Without notice, they were informed that the contract was ended. Phow!

Here it is then – the unexpected, unplanned exit, not of their making, but all the more surprising and shocking for that, a Black Swan. Could they have planned for this event? The answer (perhaps with hindsight) is yes they could. One thing that could have been done would have been to ensure that the contract had clauses in it giving them some protection against this type of outcome. It is not uncommon in the service provider industry for mergers and acquisitions to occur, so this could have been foreseen as a possible scenario. Wise after the fact eh?

However, that's what contingency planning is all about. Being wise before the fact by dreaming up business discontinuity scenarios and stress testing the organisation's ability to survive those events. Not all Black Swans are unforeseeable – some are decidedly grey in colour. Brexit has been becoming a paler colour by the month for some time.

So, The Attributer concludes that contingency planning is an essential activity, and that within that activity, scenario planning is the main tool by which an enterprise can protect itself by foreseeing generic event types such as 'forced exit'. SABSA uses business attributes to ensure that each and every business requirement is captured and risk assessed, and that controls such as contingency plans are put in place to meet the risk appetite of the company. Is your enterprise 'exit-ready'?

The Attributer

VERSLAG

BLACK HAT SESSIONS XIV

Twee kettingzagen, een Barbie, een kitten en een ring "to rule them all"

De reden om te komen maakt hem niet uit, hij noemt als mogelijke redenen: driften met de auto op de A28 en een mogelijke baan bij Madison Gurkha. Black Hat Sessions [1] dagvoorzitter Walter Belgers wenst iedereen een fijne dag. Na het bedanken van de sponsoren valt op dat er ook mensen van AVROTROS van het programma "Opgelicht" aanwezig zijn gedurende de dag. Walter wijst er wel op dat het verstandig is om de hulp die deze mensen willen bij het maken van hun nieuwe serie op legale wijze te geven.

De eerste keynote is van Aral Balkan en gaat over "wolken" en technologie. Hij laat een patentaanvraag van Google zien voor een teddybeer. Niet een standaard teddybeer maar één met sensoren en draadloos netwerk. Eén die luistert, ziet en praat. Hij stelt de vraag: "Wat is het product hier?" Daarna vraagt hij aan de zaal of ze de getoonde Barbie kennen. Vanwege het uitblijven van reactie zegt hij: "Praat ik tegen een zaal vol met mannen? Reken maar dat jullie dochters tegen Barbie praten tijdens het spelen. Dat gaat over zaken die ze niet delen met volwassenen. Deze data wordt verzameld en ToyTalk Inc. luistert."

Later komt de quote van de FBI: "We kill people based on metadata" voorbij. Deze quote komt in een latere presentatie ook terug. Aral betoogt dat open source voor niet-ingewijden als een kettingzaag is. Een kettingzaag waarmee het voor hen best moeilijk is om een boterham te smeren. De zaal lacht.

Al met al is het geen mooi beeld dat Aral van de "wolken" schetst. Het is een inktzwart beeld waarin de wereld(burgers) onder volledige surveillance staan en data in serverfarms wordt opgeslagen. Privacy is alleen iets voor de allerrijksten (of ingewijden). Een selfie van Mark Zuckerberg waarin deze van zijn werklaptop zowel de audio als de camera fysiek heeft afgeplakt, wordt getoond.

Er zitten heel veel boodschappen in de presentatie van Aral en hij weet het publiek heel goed te boeien met als gevolg het luidste applaus van de dag.

Zijn belangrijkste boodschap is dat wij een wereld moeten maken waarin op basis van ethisch design, technologie wordt ingezet. Vanaf de basis juist en dat betekent onder andere geen venture capitalists betrekken. Hierdoor worden de mensen niet het product maar is er vanaf de basis respect voor mensenrechten.

Aan het einde laat hij als voorbeeld een product zien. Better, een content-blocker. Deze zou ik graag op mijn iPhone willen, ware het niet dat dat waarschijnlijk niet kan omdat mijn mobiel te oud is daarvoor.

De tweede keynote spreker, Daniel Bernstein, heeft in zijn presentatie een plaatje van de volgende kettingzaag. Hij heeft het over drie crypto horror-stories. De eerste over RC4 dat door Ron Rivest in 1987 is bedacht. De jongere mensen in de zaal vinden het moeilijk om Daniel te volgen. Als professor vooronderstelt hij veel (historische) kennis. In sneltreinvaart worden zaken genoemd zoals de exportbeperking op crypto, ingesteld door de USA in de vorige eeuw, de NIST-competitie voor de opvolger van DES, WEP en aircrack. Het meest ontluisterend is dat in 2016 we nog steeds niet van RC4 af zijn. Daniel schetst historisch hoe dit zo gelopen is.

De tweede horror-story gaat over timing-attacks. De eerste werd al in de zeventiger jaren van de vorige eeuw uitgevoerd op het systeem TENEX. In 1996 werd een theoretische mogelijkheid beschreven van een timing attack die in 2008 nog als "a small thing" werd afgedaan. In 2013 was het raak en werden TLS-implementaties als niet langer veilig aangemerkt.

Spreker Rob van der Veer.

De derde horror-story gaat over de aanvallers. In 2012 werd een lezing van Daniel weggezet als cryptography for the paranoid. Iets later onthulde Snowden het één en ander en werd paranoid ingeruild voor nieuws.

Eén van de te leren lessen die Daniel deelt is dat we performance niet moeten inruilen voor security-maatregelen. En de meest treurige is, dat in 2016 de NSA nog steeds via ISO-normeringen slechte security-ciphers promoot. Daniel laat de ring uit Lord of de Rings zien als hij het over de NSA heeft.

In het volgende deel van het programma moet een keuze worden gemaakt tussen een technische en een niet-technische track. Zoals Madison Gurkha aan haar stand verplicht is, is de niet-technische track toch technisch genoeg.

Rob van der Veer deelt zijn bevindingen met betrekking tot mobile apps. Aan de hand van zeven zonden schetst hij veel gemaakte fouten. Zoals bijvoorbeeld het niet testen, of niet helemaal of alleen achteraf testen van softwaresystemen. Om de dialoog tussen bouwer en opdrachtgever beter vorm te geven geeft Rob als tip om gebruik te maken van Grip op SSD. Deze methode en normenset is te vinden op de pagina's van het CIP [2]. Nieuw is de Engelse vertaling hiervan en de set specifiek voor mobiele apps.

In de niet-technische track is het daarna de beurt aan Ralph Moonen van ITSX. Het motto van zijn presentatie is: 'Alles van waarde is draadloos'. Hij refereert nog even naar de vorige spreker die het heeft gehad over de auto waarbij je de besturing en controle kon overnemen omdat het entertainmentsysteem toch gekoppeld bleek te zijn via een en hetzelfde netwerk. Waarom worden er wel kamervragen gesteld over slimme meters, maar niet over connected vehicles? Die slimme meter weet eigenlijk alleen of je thuis bent (en je verbruik) maar die auto levert veel meer data en risico's op. In een verwijzing naar de keynote van Aral toont Ralph een plaatje van een kitten aan de zaal. Vier redelijk nieuwe draadloze technologieën, NFC, LoraWAN, Zwave en Zigbee, elk met eigen risico's, worden behandeld. De in de samenvatting genoemde fouten zijn niet anders voor deze draadloze technologieën als voor andere technologieën. De zaal is niet verbaasd. Ralph komt nog even terug op zijn eigen gestolen auto. Hiervan had hij, vanwege zijn achtergrond en de wens van privacy, het GPS-systeem dat met de fabrikant communiceert uitgezet. Toen het vervoersmiddel gestolen was, was hij erg blij dat hij het weer aangezet kreeg doordat zijn draadloze softwareupdate uitgevoerd werd door de auto. De politie kon met de GPS-gegevens van de auto het vehikel terugbrengen.

In het technische track maakte Raul Siles nog indruk met zijn technische opsomming van mogelijkheden om iOS aan te vallen. In de verwijzingen stond een verwijzing naar 2016 het jaar van de malware op iOS. Hopelijk luistert Apple heel goed naar deze onderzoeker en lost de problemen, of vulnerabilities, gewoon op.

De afsluitende keynote is voor Kevin McPeake. Ooit in 2000 op DefCON sprak hij over kwetsbaarheden in Lotus Notes. Het vreemdst vond hij toen dat de fabrikant iemand van productmarketing had gestuurd. Iemand die vooraf al een conflict of interest had vanuit zijn positie. Want het oplossen van security kwetsbaarheden in het product waarop hij alleen op de verkoopcijfers wordt afgerekend levert hem geen voordelen en alleen kosten op. Een aantal wijze lessen passeren de revue. Zoals dat opzetten van riskmanagement in een enterprise-organisatie niet in silo's gedaan moet worden en het onderbrengen van een security-afdeling bij IT. Nog een voorbeeld, het (schijnbaar oneindig) investeren in beveiligingsmaatregelen, zonder duidelijk te maken wat dat moet opleveren, is een slecht idee. Een verwijzing naar Lord of the Rings blijft in deze presentatie achterwege maar een WOPR (War Operation Plan Response) komt wel in beeld.

Al met al een interessant programma op een warme dag.

Nog een afsluitende observatie: op een totaal van twaalf sprekers zijn er twee vrouwen. Enkele vrouwen hadden de organisatie op het lage aantal gewezen. Maar een te halen quotum op vrouwelijke sprekers bij een securitycongres lijkt mij niet de juiste oplossing. Wel wil ik meewerken aan het proberen meer vrouwelijke sprekers op de volgende BHS te krijgen.

Links

[1] Black Hat Sessions: https://www.blackhatsessions.com
[2] CIP: https://www.cip-overheid.nl

VERSLAG CISO 11

DE JAARLIJKSE ESMERALDA-LEZING OP 8 JUNI 2016

Tijdens de jaarlijkse Esmeralda lezing leidde Ronald Paans ons langs de elementen die de essentie vormen van de risico's rond communicerende dingen. IoT, weten wij voldoende om een oordeel te hebben over de risico's die daarmee verbonden zijn? Deze vraag bleef over na CISO 8 in december 2015. In zijn introductie toonde Bart van Staveren zich erg tevreden over het feit dat Ronald bereid was gebleken de uitdaging op te pakken om over dit onderwerp met ons in gesprek te gaan.

Internet of Things, van belang tot beveiligen

Onder deze vlag voerde Ronald Paans (www.noordbeek.com), ons mee langs een groot aantal sheets. Een methodische gang langs de velden van risicomanagement doortrokken van discussievragen, praktijkvoorbeelden en dilemma's, alles vanuit de blik van informatiebeveiliging en privacybescherming. Uitgangspunt daarbij was de NCSC-indeling die de dreigingen op de belangen van organisaties en maatschappij ziet in relatie tot de weerbaarheid daarvan.

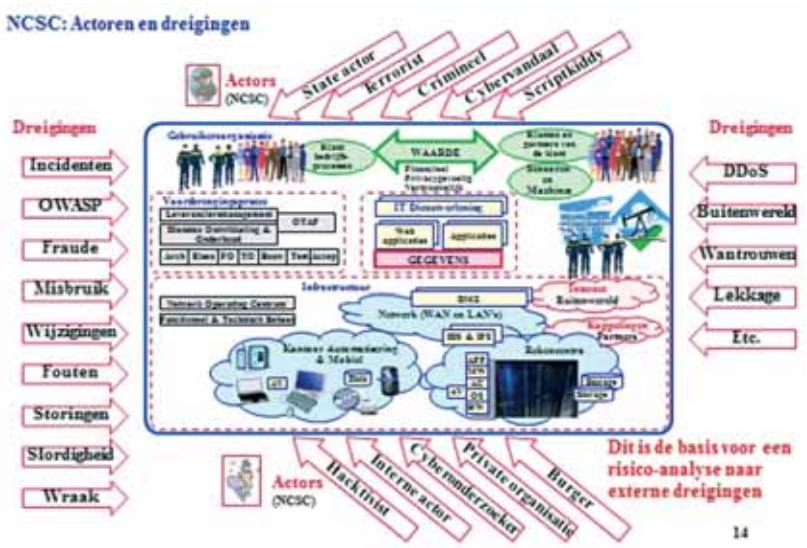
Ronald wees op de blik van de IT-auditor die steeds op IT gericht is geweest. Nu wordt het tijd ons te richten op de 'echte wereld' want daar speelt de informatieverwerking zich nu af met al die communicerende dingen. Daar zit tevens de uitdaging. In de omvangrijke en diverse wereld van mensen, belangen, IT-diensten en -infrastructuur, wordt het voor de IT-auditor steeds moeilijker een oordeel te geven. Maar dat wordt nog steeds van hem/haar gevraagd.

De definitie van IoT ontleende Ronald aan het EU-project CASAGRAS. De toelichting hierop met praktische voorbeelden,

Bart van Staveren (l) en Ronald Paans (r).

vormden de inleiding naar de risicoanalyse zoals die volgens Ronald door een auditor dient te worden uitgevoerd.

Alle stappen van de risicoanalyse werden doorlopen met steeds IoT in het achterhoofd. Zowel presentatie als discussie werden tijdens het diner met groot enthousiasme voortgezet.



Discussie

In de discussie kon het onderwerp privacy en de (vermeende?) verschillen in de manier waarop generaties dat aspect beleven, niet ontbreken. Dat blijft een onderwerp van gesprek, evenals het thema dat niet zozeer de gegevens het probleem vormen als wel het machtsmisbruik dat houders van informatie soms kenmerkt.

Wordt de mens een object, nu hij/zij met allerlei 'things' met van alles is verbonden? Een interessante vraag die niet eenvoudig te beantwoorden bleek.

Zijn sensoren wel te vertrouwen? Meestal wel, maar als dat niet kan is daar dan in het systeemontwerp rekening mee gehouden?

Hoe kan misbruik worden tegengegaan? Het gebruiksgemak van apparaten en software nodigt uit maar de gegevens die daarbij aan het gedrag van personen kan worden ontleend, kan misbruikt worden. Daar staat het menselijke gedrag tegenover de corporate voordelen. IT is in de maatschappelijke processen doorgedrongen en de vraag is of er nog alternatieven zijn. Kunnen wij nog terug naar een analoog proces? Uitval van systemen kan niet meer worden opgevangen. Nadenken over de vraag of wij nog zonder IT kunnen, levert discussie op. Hoe realistisch zijn de oplossingen?

Tenslotte dankte Bart van Staveren voor de aanzetten die Ronald gaf tot denken en doen op dit actuele maar nog moeilijk grijpbare terrein.

Links

[1] De naam Esmeralda lezing is ontleend aan "Sprookje" van Jaap Fischer over het selectieproces van een prinses door haar bruidegom:

En toen mocht Hans. En Hans zei: Ja, ik weet het nog niet, maar het moet een meisje zijn met prachtige kleren en goudblonde lokken met ogen als meren die niet kunnen jokken een mond als van honing en dan weer scherp als een mes en hopelijk is haar vader koning en zij dan prinses. Maar, ze moet Liesje heten.

En toen keek de prinses hem aan en zei: "Ik heet Esmeralda, maar zeg maar Liesje".

Esmeralda als metafoor van een centraal vraagstuk van de IB-er: authenticatie door rollen.

Cees Coumou is sinds medio 2003 gepensioneerd als senior EDP Audit manager bij KPMG. Sindsdien is hij onafhankelijk adviseur en docent aan de IT-Audit Master van de Vrije Universiteit, de opleiding Master of IT auditing van de Universiteit van Amsterdam. Zijn werk op het gebied van organisatieadvisering betrof de laatste decennia met name onderwerpen als risicomanagement, continuïteitsmanagement en informatiebeveiliging. Tussen 2005 en 2012 redigeerde hij voor PvIB 8 boeken over trends in IT-beveiliging op basis van gesprekken met vele verschillende professionals.Hij is bereikbaar via cees.coumou@planet.nl.

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

OEROUDE DREIGING: DE MENS

In dit nummer hebben we het verschillende malen over de zogenaamde "nieuwe dreigingen". Technologie speelt daarin eigenlijk altijd de hoofdrol daar we al snel vrees hebben dat het inbreuk maakt op onze vrijheden, security kan omzeilen of gewoonweg voor onszelf onveilig is. Voor het gemak vergeten we daarbij te zeggen dat technologie helemaal niets uit zichzelf doet. Het is de mens die technologie gebruikt, maakt en inzet voor allerhande doeleinden. Feitelijk is de mens de grootste dreiging voor zichzelf en anderen. Het is immers niet het mes dat bestraft moet worden, maar de mens die het mes gebruikt om een ander te doden. Het blijven roepen dat technologie gevaarlijk is en gereguleerd moet worden helpt niet, we moeten de mens aanpakken! Of heeft dat eigenlijk helemaal geen zin en is de "slechtheid" van de mens iets waarmee we maar moeten zien te leven?

Tom Bakker

Er zijn verschillende kanten met betrekking tot de mens als zwakste schakel. Als dreiging voor de mens zelf denk ik aan het gebrek aan security-awareness. Veel security-awareness-programma's hebben de focus alleen op kennisverhoging. Als je gaat zeggen of vragen dat je je wachtwoord geheim moet houden en niet moet delen met anderen, zal men reageren van 'ja dat ken ik nu wel zo langzamerhand'. Interessanter is dat ondanks deze aanwezige kennis men toch wachtwoorden deelt. Dat heeft dus met gedrag te maken. Blijkbaar is dat een hardnekkig probleem. De mens moet eerst iets meegemaakt hebben zoals malware binnenhalen door bijvoorbeeld 'klakkeloos klikken'. Of een identiteitsdiefstal om het gedrag te veranderen. Het is natuurlijk best wel begrijpelijk omdat beveiliging vaak ook lastig kan zijn of gemaakt wordt en dat dan de weg van de minste weerstand gezocht wordt. Beveiligingsmaatregelen worden zo omzeild en de risico's worden even vergeten. Het mooiste zou zijn dat security-by-design standaard is. Maar dan zo dat de gebruiker eigenlijk niets merkt van de beveiliging. Beveiliging gebeurt onder water. Bijvoorbeeld email altijd automatisch versleuteld. Opslag van gegevens versleuteld, two-factor-authenticatie et cetera. Misschien wordt de zwakste schakel dan minder relevant.

De dreiging voor anderen? Dat is wat ik zie als het fenomeen van het grenzeloos 'vertrouwen in de computer'. De 'computer' vertelt altijd de waarheid: 'het is zo want het staat zo in ons systeem'. Denk aan de sketch uit de komische serie Little Britain waar 'the computer says no' steeds het antwoord is op elke vraag. Zo kunnen bestanden onjuiste gegevens bevatten die, jawel, door de mens ingevoerd zijn. En als dat de waarheid moet zijn . . . . Daar zijn genoeg voorbeelden van. Probeer maar eens onjuiste gegevens te (laten) corrigeren. Koppelingen en synchronisatie van bestanden maakt het nog veel erger. Veel succes! Hoe moeten we dat aanpakken? Misschien een meer kritische houding ten opzichte van de techniek.


Tom Bakker


Lex Borger


Rachel Marbus

Rachel Marbus

Toen ik (een klein beetje lang geleden) begon met mijn studie rechten, werd het debat over regulering van technologie volop gevoerd. En ik kan u vast verklappen dat we er nog steeds niet helemaal uit zijn of en hoe dat dan allemaal zou moeten. Prachtige boekwerken zijn daarover volgeschreven door vooraanstaande wetenschappers. Een gedeelte van dat academisch debat wat mij altijd is bijgebleven, is gebaseerd op onder andere het werk van Thaler and Sunstein [1]. In Nudge laten zij zien dat technologie heel mooi ingezet kan worden om mensen een duwtje in de juiste richting te geven (even los van de vraag welke richting dan juist is). Basisgedachte is dat technologie een onlosmakelijk onderdeel uitmaakt van onze maatschappij en dat je het aldus ook kunt inzetten om goed te doen. Het benadrukt in plaats van de dreiging de positieve kant van technologie en is voor mij een van de eerste vormen van positief omdenken in het reguleringsdebat. Dat er dreigingen zijn, is eveneens een onlosmakelijk onderdeel van onze getechnologiseerde maatschappij. Maar een beetje meer positief omdenken over hoe daarmee om te gaan zou denk ik veel meer zoden aan de dijk zetten om negatieve gevolgen te voorkomen.

Lex Borger

Technologie is gevaarlijk. Daar hoeven we geen discussie over te voeren. Of we het nu over wapens hebben of over vitale infrastructuur, dit blijft een universeel gegeven. Technologie bestuurd door computers is net zo gevaarlijk. Accenten verschuiven: computers kunnen meer beheersen dan de mens, maar ze hebben hun grenzen. Wanneer die overschreden worden, dan excelleert de mens.

Regulering is gewoon een maatregel die in een bepaalde context effectief kan zijn om risico's te beheersen. En het maakt niet uit of dit technologische risico's zijn of risico's die voortkomen uit menselijke fouten of opzettelijk handelen. Beide aspecten zijn slecht, maar op een andere manier. Opzettelijk handelen pak je niet aan met regulering, daarvoor hebben we ons rechtssysteem. Het mes dat gebruikt wordt in een moord wordt niet bestraft, de gebruiker van het mes wordt gestraft. Maar er zijn wel reguleringen om het mes veiliger te maken in gebruik.

Echter houdt het niet op met regulering: deze moet bekend zijn, begrijpelijk en uit te voeren. Regulering is slechts een bestuurlijke maatregel, eenvoudig geformuleerd en gepubliceerd. Het is echter een tandeloze tijger zonder naleving, een andere bestuurlijke maatregel, die veel meer geld en inspanning vergt. En bedenk dat zelfregulering ook zelfnaleving nodig heeft... En dan heb ik het niet over alle andere mogelijke maatregelen op de vlakken van de mens, processen en techniek. Dat is out-of-scope bij het argument.

De mens maakt fouten. Dit is een spreekwoordelijk gegeven. Fouten kunnen bedieningsfouten zijn, maar ook inschattingsfouten. De mens is een sociaal wezen en kan dus fouten maken in de sociale omgang. Dan spreek je van 'social engineering'. Regulering is hier niet het eerste middel waar ik aan denk; training is belangrijker. Techniek bediend door ongetrainde mensen is veel gevaarlijker dan techniek bediend door computers of getrainde mensen.

De technologische dreigingen kunnen we aanpakken met maatregelen, waaronder regulering en naleving. De mens is inherent slecht, opzettelijk en onopzettelijk. Een deel daarvan is aan te pakken met training, regulering en rechtspraak, maar wat er tussen de mazen valt hebben we maar gewoon te accepteren. Dit is niets nieuws. Hoe dit verband houdt met nieuwe technologie en nieuwe dreigingen daarover kan wel wat gezegd worden. Hiervoor kan ik de boeken 'Liars and Outliers' van Bruce Schneier [2] en 'Human Factor' van David Lacey [3] aanbevelen als relevant leesvoer.

Links

[1] Nudge: http://www.nudges.org

[2] Liars and Outliers: https://www.schneier.com/books/liars_and_outliers/

[3] Managing the Human Factor in Information Security: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470721995.html

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

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

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

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

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

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

ABONNEMENTEN 2016
De abonnementsprijs in 2016 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

GRIJZE HAREN

In het verre verleden werd ik manager over een afdeling die de infrastructuur en de exploitatie van de systemen moest beheren. We hadden een aantal vestigingen. Die vestigingen waren met elkaar verbonden in een netwerk. Allemaal heel overzichtelijk. Mijn collega's hadden een eigen werkplek die we centraal beheerden. Eigenlijk was dat best wel saai, want het ging altijd goed. In 1994 vertelde een collega ons over het internet. Het was nog klein en er waren nauwelijks mensen op actief. Ik prijsde me gelukkig met die kleine schaal, want ik had al door dat het internet het leven van een beheerder weleens sterk zou kunnen veranderen.

Ik heb het lang kunnen tegenhouden dat er een Apple-computer ons bedrijf binnen werd gedragen. Toen dit gebeurde was dit voor een collega die deze machine onontbeerlijk vond om zijn grafisch werk te kunnen doen. De machine werd niet in het netwerk opgenomen en de bijbehorende printer ook niet. In die tijd kon ik vanuit mijn positie veel "vernieuwingen" tegenhouden.

Er is sinds die tijd veel veranderd. Vandaag de dag worden deze beslissingen meer en meer door de gebruikers genomen, de IT-er moet het maar veilig houden. Onze systemen zijn geoutsourcet en alle klantgegevens staan buiten de deur. Mijn printers worden via het netwerk beheerd vanuit India. Het geoutsourcete bedrijfsrestaurant wil wel zijn eigen netwerk en dat moet op mijn infrastructuur geïmplementeerd worden. Het gebouw wordt ook beheerd door een externe partij en ook deze partij wil verbindingen over mijn netwerk. De medewerkers komen met hun eigen laptops met allerlei besturingssystemen waarvan ik het bestaan niet eens wist. De mobiele telefoons die wij als bedrijf leverden worden niet meer geaccepteerd, iedereen neemt gewoon zijn eigen telefoon mee waarop natuurlijk ook mail ontvangen moet kunnen worden, inclusief de bijlagen. Iedereen wil alles wat technisch ook maar mogelijk is.

Ik maak me daar ernstig zorgen over. Ik durf niet meer te garanderen dat mijn data honderd procent veilig is en dat er niemand aan kan komen. Ik durf niet te garanderen dat mijn medewerkers geen acties met data uitvoeren die ze niet zouden moeten doen. En die activiteiten kunnen tot datalekken leiden. Er zijn zo verschrikkelijk veel manieren om bij bedrijfsinformatie te komen dat het bijna onmogelijk is om die garanties af te kunnen geven. Mijn techneuten glimlachen naar mij als ik ze bezorgd vraag over de veiligheid van de data. Op de een of andere manier word ik niet rustiger van die glimlach… Ik krijg er grijze haren van.

Hoeveel van mijn collega's zouden dezelfde zorgen hebben? Of ben ik gewoon teveel aan het piekeren? Zou de manager Infrastructuur van LinkedIn zich ook weleens zorgen hebben gemaakt? Of mijn collega bij Sony ? Of die van de datingsite BeautifulPeople.com? Zouden die zich zorgen hebben gemaakt voordat hun hack naar buiten werd gebracht? In mijn bedrijf wordt voor honderdduizenden euro's aan maatregelen genomen om een eventuele hack tegen te gaan en toch blijf ik afhankelijk van die ene beheerder die een keer niet goed heeft opgelet. Ik heb weleens het idee dat ik een fort beveilig met veel ingangen. Ik ken de meeste wel, van een paar ingangen weet ik dat ze er zijn maar ik weet alleen niet waar. Het wordt tijd dat ik met pensioen ga.

Berry

SECURITY ACADEMY

Behaal de S-CISO certificering!

Vanaf september 2016 maakt het **Cyber Security & Governance Certification Program van SECO-Institute**. onderdeel uit van het portfolio van de **Security Academy**. Binnen dit programma kunt u opgeleid worden tot aan CISO niveau.

De opleidingen van de Security Academy bestaan uit een **Foundation-** (2 dagen). **Practitioner-** (5 dagen) en een **Expert-level** (15 dagen). Deze opleidingen onderscheiden zich door de student voor te bereiden op de praktijk. in plaats van alleen theorie te behandelen.

Daarboven kunt u (bij minimaal 3 jaar ervaring) de titel **S-CISO** aanvragen. Bent u reeds in het bezit van een **CISSP, CISM of C/CISO certificering**. dan kunt u direct instromen op Expert niveau.

Zie voor meer informatie: **www.seco-institute.org**

Waar anderen stoppen, gaan deze opleidingen en certificeringen verder: The next level in Security & Continuity!

www.securityacademy.nl info@securityacademy.nl +31(0)348-408061