Elke voordeur wordt wel een keer opengebroken als er maar voldoende tijd is

Ronald Prins

Fotografie: NFP Photography

Jip Olieroock MSc RO CIA
Drs. Laszlo Nagy EMIA RO

Audit Magazine sprak met Ronald Prins, medeoprichter en chief technology officer van Fox-IT, over 'cyber security', 'internet of things', 'red teaming' en tips voor de internal auditor.

De **uitdagingen** van **cyber** security

Wat zijn de laatste relevante ontwikkelingen op het gebied van data en welke gevaren spelen daarbij?
"Een ontwikkeling die een enorme impact op de samenleving heeft betreft internet of things. Hiermee bedoel ik dat meer en meer alledaagse zaken met internet worden verbonden. Denk bijvoorbeeld aan de 'slimme' energiemeters, inbraakbeveiligingsapparatuur en thermostaten. Hoewel het aansluiten van alledaagse dingen op internet oneindig veel nieuwe kansen en mogelijkheden oplevert, brengt het ook gevaren met zich mee. Systemen kunnen immers gehackt worden en (privacy)gevoelige informatie kan worden ontvreemd. Dit geldt niet alleen voor particulieren maar ook voor organisaties. Naast het stelen van informatie bestaan er ook fysieke gevaren in die zin dat de besturing van buitenaf kan worden overgenomen. Denk bijvoorbeeld aan het hacken van air-traffic-controlsystemen of van sluizen, gemalen en bruggen. Deze laatste categorie is de laatste jaren al meerdere malen in het nieuws geweest omdat was aangetoond dat het overnemen van dergelijke systemen soms kinderlijk eenvoudig was. Naast internet of things zie je ook een trend dat teneinde de veiligheid te vergroten, steeds meer kritische handelingen worden geautomatiseerd. In dergelijke gevallen wordt getracht het menselijk falen uit te sluiten door de mens als schakel uit de besturing te halen. Denk bijvoorbeeld aan de treinmachinist. Op het moment dat door menselijk falen een ernstig ongeluk plaatsvindt, is een eerste reactie vaak om de operatie verder te automatiseren. Met het oplossen van safetyproblemen worden dan vaak weer securityproblemen geïntroduceerd. De kans op een ongeluk wordt dan weliswaar verkleind maar tegelijkertijd ontstaan er weer nieuwe en externe dreigingen vanwege de kwetsbaarheid van systemen."

Hoe gaan we binnen Nederland met dergelijke gevaren om?
"Nederland loopt op het gebied van technologische ontwikkelingen en toepassingen graag voorop. Kijk bijvoorbeeld naar de digitalisering van het betalingsverkeer. Nederlandse banken lopen op dit gebied ten opzichte van bijvoorbeeld de Belgische banken echt voorop. We realiseren ons echter niet voldoende dat de consequentie hiervan is dat we door vallen en opstaan pas leren wat goede (preventieve) controls zijn. Door vooruitstrevend te zijn begeven we ons ook op onontgonnen terreinen met de consequentie dat we op het gebied van de beheersing eigenlijk continu achter de feiten aan lopen. In wezen is het een proces van 'trial and error'. Naarmate steeds meer zaken worden verbonden met internet ontstaan er derhalve ook steeds meer risico's: we weten

Over...

Ronald Prins is directeur en medeoprichter van Fox-IT (1999). Hij studeerde technische wiskunde aan de TU Delft en specialiseerde zich daarna als cryptograaf. Bij het Nederlands Forensisch Instituut was hij werkzaam als wetenschappelijk onderzoeker. In het kader hiervan heeft hij vele (cryptografische) beveiligingen doorbroken waar de politie tegenaan liep bij het uitvoeren van hun rechercheonderzoeken.

Fox-IT richt zich op het voorkomen, onderzoeken en beperken van de meest serieuze cyberdreigingen met innovatieve oplossingen voor met name overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven. Het in 1999 opgerichte bedrijf heeft als missie het leveren van technische en innovatieve bijdragen voor een veiligere samenleving. Bij Fox-IT werken ruim 150 beveiligingsexperts.

immers dat nagenoeg elk systeem te hacken is. Indien vitale infrastructuur wordt verbonden met internet moet men zich goed realiseren dat de mogelijkheid ontstaat dat er ernstige ongelukken kunnen plaatsvinden.
Vitale infrastructuur zou dan ook niet van internet afhankelijk moeten worden gemaakt. De overheid heeft echter nu juist in het kader van de privatisering steeds meer relevante taken overgedragen aan de markt. Denk bijvoorbeeld aan energiebedrijven, telecom en financiële instellingen. Hierdoor is de besluitvorming over het beveiligingsvraagstuk van deze organisaties ook uit handen gegeven.
De Nederlandse overheid zou ten aanzien van organisaties van nationaal belang veel meer moeten eisen op het gebied van de beveiliging. In Groot-Brittannië bijvoorbeeld zijn ze hier al een stuk verder mee. Daar heeft de overheid circa vijf bureaus gecertificeerd om de beveiliging van organisaties te beoordelen en te helpen verbeteren. De Britse overheid verplicht organisaties met voor de samenleving relevante functies vervolgens om met een van deze vijf gecertificeerde bureaus in zee te gaan om de beveiliging op orde te krijgen en te houden. Dit is zelfs via wetgeving geregeld. Op een dergelijke wijze zou de Nederlandse overheid ook moeten opereren. De Nederlandse overheid zou ten aanzien van cruciale organisaties meer dan nu een regierol moeten pakken. Van dergelijke organisaties mag ook worden verwacht dat zij hun systeembeveiliging continu monitoren, net zoals nu real time wordt gecheckt of bijvoorbeeld de Russen het Nederlandse luchtruim betreden. Een inbraak op een vitaal systeem, al dan niet in opdracht van een ander land, kan immers veel schade berokkenen. Hierbij geldt dat inbreken een aantrekkelijke optie is omdat het tegen lage kosten, zonder slachtoffers aan eigen kant en relatief anoniem kan worden uitgevoerd. Let wel, de incidenten die wij op dit gebied in de krant lezen zijn slechts het topje van de ijsberg!"

Fox-IT richt zich onder meer op cyber security. Wat treffen jullie aan als jullie bij bedrijven binnenkomen?
"Als wij bij bedrijven binnenkomen is het vaak vanwege incidenten. Wij treffen dan vaak teleurgestelde IT-medewerkers aan die in de veronderstelling waren dat ze de beveiliging op orde hadden. Vaak denkt de board dit ook omdat er immers wordt geaudit. Ons beeld is dat er nog regelmatig een groot gat zit tussen de wijze waarop een auditafdeling de beveiliging toetst en de werkelijke weerbaarheid tegen aanvallen van buitenaf. Dit is ook een erg lastig fenomeen om grip op te krijgen. Kijk maar naar de harde les die is geleerd bij de hack van DigiNotar, een van de meest geaudite organisaties in Nederland.
Vaak vindt beoordeling van de beveiliging plaats door te kijken naar de aanwezige beheersmaatregelen. Het beoordelen van de werking van dergelijke maatregelen is echter lastig. Dit valt te vergelijken met het testen van brandbeveiliging. Om echt vast te kunnen stellen of de organisatie voldoende weerbaar is tegen brand, zou je iets in de fik moeten steken! Er kan dus eigenlijk geen sluitend uitsluitsel worden gegeven over het in de praktijk daadwerkelijk in control zijn. Een dienst die wij hieromtrent leveren is red teaming. Red teaming betreft het samen met de opdrachtgever selecteren van de meest onwenselijke scenario's op het gebied van cyber security, om vervolgens met een team te proberen het systeem te hacken en betreffende scenario's te realiseren. Terwijl de inbraakpogingen worden ondernomen, wordt gekeken of de opdrachtgeversorganisatie tijdig de aanvallen weet te detecteren en hier adequaat op weet te reageren. Dergelijke testen zijn relevant omdat het enkel steunen op preventieve maatregelen in de praktijk onvoldoende is gebleken. Om de beveiliging goed te regelen is het met name belangrijk dat een mechanisme is opgezet om 'security breaches' tijdig te signaleren: elke voordeur wordt immers wel een keer opengebroken als er maar voldoende tijd is. Het testen van de werking van een dergelijk detectiemechanisme is de enige 'thermometer' die daadwerkelijk aan kan geven of de beveiliging van de systemen op orde is. Eigenlijk zouden auditors erop aan moeten sturen dat de organisatie af en toe red teaming uitvoert of laat uitvoeren. Dit levert inzicht in de sterkten en zwakten van de beveiliging en biedt concrete punten ter verbetering van de beheersing."

Wat zouden organisaties dan moeten doen?
"Organisaties kunnen veel minder doen om zich te bewapen tegen aanvallen dan ze zelf denken. Het is ontzettend moeilijk

voor een doorsnee bedrijf om een IT-securityfunctie neer te zetten waarmee je werkelijk in control kunt zijn. Denk bijvoorbeeld aan de analogie van een huis. Net als bij een bedrijf beveilig je je huis omdat je niet wilt dat er wordt ingebroken. Er bestaat echter geen slot dat niet geopend of omzeild kan worden. Het huis is dan ook niet enkel beveiligd door het slot, maar ook door het gegeven dat er zicht van derden op staat, bijvoorbeeld de buren of voorbijgangers, en omdat er altijd sprake is van een pakkans. Deze laatste elementen zijn in de digitale wereld echter niet of zeer beperkt aanwezig.
Organisaties zouden maatregelen moeten nemen die gericht zijn op de terreinen preventie, detectie en respons. Hierbij geldt dat bedrijven het uiteindelijk met de detectie en respons zullen moeten winnen. Denk aan het eerder genoemde

beveiliging goed in te richten betreft het gegeven dat de 'end users' toch nog altijd een zwakke schakel vormen. Je kunt als bedrijf veel investeren in awareness, maar bij een phishingaanval hoeft maar een medewerker erin te trappen en de hacker is binnen. De end user blijft in dit opzicht altijd een lastig te tackelen probleem. Binnen onze organisatie testen wij ook onze eigen beveiliging. Als we hierbij phishing mails inzetten dan blijkt er altijd wel iemand te zijn die erin trapt, terwijl je nergens op het gebeid van de beveiliging meer 'paranoïde' medewerkers vindt dan bij ons!
Het zijn overigens met name de grotere spelers die voldoende oog hebben voor de noodzaak om een goede beveiliging neer

Met het oplossen van safetyproblemen worden vaak security problemen geïntroduceerd

detectiemechanisme. Preventie alleen zal zonder detectie en respons nooit voldoende zijn omdat juist uit de praktijk van detectie en respons kan worden geleerd wat goede preventieve maatregelen zijn. Hierbij geldt dat met het continu ontwikkelen van nieuwe systemen en applicaties de 'goede preventieve maatregelen' ook steeds in ontwikkeling zijn.
Wanneer we echter teruggrijpen op de eerdergenoemde vitale systemen in de samenleving dan zal het voor iedereen duidelijk zijn dat het via 'trial and error' tot stand komen van preventieve controls een erg onprettige gedachte is. Het voelt niet lekker als er mogelijk mensenlevens op het spel staan. Organisaties doen er dan ook goed aan om te werken aan de bouw van een platform waarbinnen security een serieuze functie is met voldoende budget en instrumenten om de security te monitoren en, naargelang de situatie, tijdig bij te sturen. Het inzetten van red teaming is hierbij een goed middel om te testen of bijsturing noodzakelijk is."

U geeft aan dat het lastig is om de security voldoende goed te organiseren. Wat maakt dit zo moeilijk?

"Om de beveiliging goed te kunnen organiseren heb je als organisatie technologie, intelligence en de juiste mensen nodig. De technologie vergt investeringen waar organisaties lang niet altijd bereid toe zijn. Intelligence kan worden aangeschaft maar het moet voor een groot deel ook intern worden ontwikkeld en worden gecultiveerd. Dit staat in nauw verband met de derde factor: de juiste mensen. Als organisatie heb je 'skilled professionals' nodig om over de beveiliging te waken. Om van skilled professionals te kunnen spreken moet je mensen hebben die over de juiste en actuele kennis en vaardigheden beschikken. Om hiervan te kunnen spreken is het noodzakelijk dat deze medewerkers in hun dagelijkse praktijk frequent met beveiligingsincidenten worden geconfronteerd. Het lastige is dat lang niet alle soorten organisaties vaak genoeg met incidenten worden geconfronteerd, waardoor de ontwikkeling van de eigen medewerkers op dit onderwerp achterblijft. Daarbij geldt dat skilled professionals ook graag daar willen werken waar ze zich in het heetst van de strijd kunnen wagen. Een doorsnee organisatie is lang niet altijd interessant genoeg en het is daardoor moeilijker om over eigen skilled professionals te beschikken.
Een ander punt dat het in de praktijk lastig maakt om de te zetten en ook nog eens in staat zijn dit goed te organiseren. Het zijn juist de kleine en middelgrote organisaties die doorgaans onvoldoende in staat zijn om de security goed te organiseren."

Welke tips hebt u voor internal auditors?

"In de eerste plaats: hecht niet te veel waarde aan ISO-certificeringen en vinklijstjes. Fox-IT heeft zelf ook ISO-certificeringen en procedurele maatregelen zoals wachtwoordbeheer. Maar als wij red teaming op onze eigen organisatie toepassen komen altijd wel zwakheden boven water. Enkel het gebruik van dergelijke procedurele instrumenten is onvoldoende. Wij hebben ervaren dat er een enorm gat bestaat tussen dergelijke beheersinstrumenten en wat eigenlijk noodzakelijk is om security van systemen en organisaties echt te waarborgen.
Een andere tip betreft het altijd kritisch in de gaten houden van de gehanteerde scope. Wanneer wij met auditafdelingen praten merken wij dat de internal auditors allemaal rapporten van bijvoorbeeld penetratietesten opvragen, maar dan komt het nog wel eens voor dat door de beperkte gehanteerde scope de toegevoegde waarde erg of zelfs te beperkt is. Je kunt bijvoorbeeld penetratietesten op een SAP-systeem loslaten, maar dit biedt weinig garanties als de credentials via een inbraak op de Eldat-server gemakkelijk kunnen worden verkregen. Een vergelijkbare ervaring hadden wij bij de controle van de toegangsbeveiliging met detectiepoortjes. De organisatie had bij het beoordelen van de veiligheid het onderliggende systeem buiten de onderzoeksscope gelaten. Dat systeem bleek nu juist erg gemakkelijk binnen te dringen.
Ten slotte zijn er best wel wat mooie proefsoftwarepakketjes te verkrijgen. Auditors doen er goed aan eens een dergelijk pakket te proberen om wat testen te doen en vervolgens te kijken of deze terugkomen op de incidentenrapportages van de eigen organisatie. Wel even vooraf rugdekking regelen natuurlijk!" <<