CYBER DEFENCE BIJ KPN

De heer Ted van der Houwen, KPN

De geschiedenis van security bij KPN begint bij haar oprichting in 1852. In dat jaar legde de rijksoverheid openbare telegraafverbindingen aan die ze zelf zou exploiteren. De telegraaf was belangrijk als instrument voor de ontwikkeling van handel en industrie en voor het binnenlands bestuur. De Rijkstelegraaf vormde een onderdeel van het ministerie van Binnenlandse Zaken. Een tweede reden voor een openbaar telegraafnet was het verbod op aansluiting van particuliere Nederlandse lijnen op het staatsnet van ons buurland Pruisen.

In 1881 werden de eerste telefoniediensten geïntroduceerd, eerst nog door particuliere telefoonbedrijven, maar vanaf 1897 besloot de staat vanwege slechte verbindingen en lange wachttijden deze diensten zelf te exploiteren. Door de inzet van de telefonistes en het fysiek schakelen was de authenticiteit goed te borgen.
Hoe anders ziet de wereld er nu uit, de Wereldwijde KPN-infrastructuur wordt gebruikt door 42 miljoen klanten, waarvan 33,9 miljoen mobiele klanten, 4,4 miljoen met een vaste telefoonaansluiting, 2,5 miljoen met een internetaansluiting en 1,2 miljoen televisieklanten.

Daarmee is KPN net als andere grote instellingen een geliefd doelwit voor cybercriminelen en doet KPN er alles aan om aanvallen te voorzien en waar mogelijk te voorkomen of in ieder geval zo snel mogelijk te pareren. KPN heeft daarvoor, net als bijvoorbeeld Defensie en grote financiële instellingen, een speciaal CERTteam. CERT staat voor *Computer Emergency Response Team*, een term met een knipoog naar de *Community Emergency Response Teams*: een uit de VS overgewaaid begrip voor teams die als eerste ter plekke zijn bij een calamiteit.

DENKEN ALS EEN CRIMINEEL

"Wij zijn de brandweer en werken preventief en correctief", KPN-er Folkert Visser is lid van KPNCERT, maar formeel werkzaam bij de afdeling *Security & Improvements* van de Operator-tak van KPN. Want zo werkt dat bij de vooral virtueel opererende CERT-teams: de teamleden zijn 'gewoon' werk-

KPN Netwerk Operations Center

zaam in de lijn als engineer, architect of beheerder. Ze hebben hun eigen (klant) netwerk of –platform, dat ze veilig houden en schakelen met elkaar op basis van hun gezamenlijke passie: het pareren van cyber-aanvallen. Een speciale opleiding bestaat niet, ervaring in hun dagelijkse werk en belangstelling zijn de redenen waarom men deel uit gaat maken van een CERTteam. "Ik ben eigenlijk wel een nerd", aldus Folkert Visser. "Je moet denken als een crimineel om te weten waar lekken en risico's zitten. Het is gewoon een wapenwedloop, je loopt per definitie achter de feiten aan. Voor beveiliging richt je je dus op een risicoanalyse: waar zou je het meeste last van hebben. Maar een hacker houdt zich niet aan jouw risicoanalyse. Hem maakt het niet uit waar hij begint."

Het KPN CERTteam is één van de oudste CERTteams van Nederland en al ontstaan bij het begin van de explosieve groei van het internet rond 1995. Het CERTteam is 24x7 paraat, en bestaat uit meer dan 40 experts met vooral een technische achtergrond op het gebied van informatiebeveiliging. Zij maken deel uit van het virtuele team, dat actiefkennis deelt, niet alleen onderling maar ook met de rest van de organisatie. "Onderling houden wij elkaar scherp via de CERT Academy, waarin we thema's uitdiepen, bijvoorbeeld over rechtspraak, calamiteitenoefeningen en conferenties op het gebied van security. En als het om acute calamiteiten gaat natuurlijk ook met CERTteams van andere organisaties, want het bestrijden van cyber-aanvallen is een gezamenlijk belang."

INTERNATIONALE SAMENWERKINGSVERBANDEN

Folkert: "Wij monitoren continu de ontwikkelingen op het gebied van cyber-aanvallen via ons lidmaatschap van internationale samenwerkingsverbanden van CERTteams, zoals FIRST en TRUSTED *Introducer* en een aantal vertrouwelijke samenwerkingsverbanden.

Naast deze proactieve kant van ons werk hebben we ook een 24-uurs bereikbaarheidsdienst. Onze collega's bij KPN kunnen ons dag en nacht bellen voor advies en in noodgevallen rukken we uit."

Zo was er pas een aanval (DDoS attack) op een grote buitenlandse instelling. Vanuit computers overal ter wereld werd hun netwerk overbelast. Ook tientallen consumentenklanten van KPN bleken ongewild deel uit te maken van deze 'botnet'-aanval. Hun computers waren besmet.

BOTNET

Botnet is jargon voor een collectie van softwarerobots of "bots", die automatisch en zelfstandig opereren. De term wordt vaak geassocieerd met ongewenste software of het automatisch versturen van ongewenste email van computers waarop deze software is geïnstalleerd (spam) maar kan ook refereren naar een netwerk van computers die distributed computing software gebruiken (Bron: Wikipedia).

Het KPN CERTteam was via haar internationale contacten op de hoogte van de aanval en kon snel de betreffende computers lokaliseren en isoleren. Vervolgens werden de eigenaars geadviseerd hoe ze hun computer weer schoon en veilig konden krijgen. Nadat dit is gebeurd en de betreffende computer weer clean is, wordt het isolement opgeheven. Dit soort incidenten heeft het KPN CERTteam wekelijks bij de hand.

CYBERWAPENWEDLOOP

De cyberwapenwedloop is een serieuze zaak. "Hacken is al lang geen sport meer", volgens Folkert. "Het is steeds meer georganiseerde misdaad. Er zijn complete 'bedrijven' gespecialiseerd in het opzetten van botnets. Het versturen van spam levert nog steeds veel geld op. En er zijn steeds meer aanvallen met een politieke of ideologische achtergrond, zoals STUXNET schijnbaar gericht op het Iraanse kernenergieprogramma."

De recente DigiNotar-affaire laat zien hoe iets dat begint met wat een simpele hack lijkt, in korte tijd een hele samenleving lam kan leggen, als er niet snel adequaat gereageerd wordt. "De dreiging verschuift ook. Vroeger waren bij KPN alleen PC's en servers een doelwit, toen kwam de e-mail en nu ook de mobiele telefoons en de interactieve tv's. KPN heeft al deze ontwikkelingen meegemaakt. Bij productontwikkelingen doen we altijd een risicoanalyse om te kijken waar beveiligingsrisico's kunnen gaan ontstaan." Want het is niet de vraag óf er aangevallen gaat worden, maar wel wanneer, hoe en wat er aangevallen wordt. Je moet er niet aan denken wat er kan gebeuren als er operationele apparatuur van Defensie wordt gehackt. Een CERTteam is dus onmisbaar en bestaat bij gratie van de kennis en ervaring en het enthousiasme van de teamleden.

KPN neemt haar maatschappelijke verantwoordelijkheid daarmee serieus. En is ook met een compleet dienstenportfolio voor haar klanten actief op het gebied van beveiliging. Met bijvoorbeeld advies over *security-, identity management-* en continuïteitvraagstukken en met een volledig security portfolio, waarin het leveren van kostenefficiënte *managed security & continuity services en solutions* centraal staan.

REFERENTIES

- Wilt u meer informatie dan kunt u contact opnemen met het Defensie Cliënt Team van KPN via 030-6635589

ted.vanderhouwen@kpn.com
www.kpn.com\corporatemarket