de Correspondent

Opnieuw relevant > Analyse

30.11.2016 • Leestijd 10 - 14 minuten

Vandaag werd bekend dat er zeer gevoelige informatie uit terrorismedossiers van politiedienst Europol is uitgelekt. Een medewerker had ze opgeslagen op een externe netwerkschijf. Welkom in de wereld van het internet der dingen, waar het hartstikke leuk en gezellig is, maar ook extreem onveilig.

Met dank aan dat fijne internet der dingen liggen zeer gevoelige terrorismedossie

rs op straat

Correspondent Technologie & Surveillance

Maurits **MARTIJN**

Foto: Arjen Born (voor De Correspondent)

Zevenhonderd pagina's uit vertrouwelijke terrorismedossiers van politiedienst Europol liggen op straat. Televisieprogramma *Zembla* ontdekte het lek en wijdt er vanavond, woensdag 30 november, een uitzending aan.

Europol spreekt zelf van een 'zeer ernstig incident.' De informatie gaat over 54 Europese terrorismeonderzoeken die voornamelijk plaatshadden tussen 2006 en 2008. Het gaat onder andere om informatie uit onderzoeken naar de Hofstadgroep, de aanslagen in Madrid maar ook onderzoeken die niet in de openbaarheid zijn gekomen. Er staan namen, adressen en telefoonnummers in van mensen die in verband zijn gebracht met terrorisme. Op dit moment doet Europol in acht Europese lidstaten onderzoek naar de gevolgen van het lek.

Hoe *Zembla* deze gevoelige data exact heeft ontdekt, is nog niet duidelijk. Wel duidelijk is dat een medewerker van Europol - tegen de regels in - de dossiers mee naar huis had genomen.

Om die vervolgens op te slaan op een externe netwerkschijf.

Deze schijf was aangesloten op het internet.

Zonder wachtwoord.

En zo is dit lek een extreem voorbeeld van wat er kan gebeuren in de wereld van het internet der dingen. We sluiten steeds meer apparaten aan op het internet. Hartstikke handig en leuk, maar de beveiliging van deze apparaten laat nogal eens te wensen over. En wijzelf zijn vaak laks en lui.

Twee jaar geleden onderzocht ik met een hacker wat er mis kan gaan op het internet der dingen. Ik ontdekte dat het een koud kunstje is toegang te krijgen tot de meest intieme gegevens van argeloze mensen. Wij kwamen óók exact dezelfde apparatuur tegen die de medewerker van Europol gebruikte, de iOmega-schijf van Lenovo.

De les die ik van dit stuk leerde: een lek met hoogstgevoelige informatie uit terrorismedossiers is uitzonderlijk; de redenen die eraan ten grondslag liggen, zijn systemisch.

Lees hieronder mijn stuk.

Zo begluur en bestuur je Nederland

Geluid? Loopt!

Camera? Loopt!

Actie!

We zien het interieur van een doorsnee woonkamer. Links: een tuindeur. Rechts: een open keuken. In het midden de bank, een glazen bijzettafel en een kastje. We zien een wat oudere man in de tuin rommelen. Aan de keukentafel zit een vrouw van ongeveer dezelfde leeftijd. Naast haar staat een jongere vrouw die een klein meisje helpt met viltstiften en papier. Vanuit ons perspectief lijkt het een kleurplaat, waar ze mee bezig is. Maar het zou ook een brief kunnen zijn. Of gewoon een tekening.

We passen ons beeld aan. Tikkie naar rechts, stukje naar onder. Inzoomen.

Bingo. Kleurplaat.

We kijken verder rond. We zien de schilderijen aan de muur en de pannen in de keukenkast. We bekijken het parket op de vloer en de patronen op het plafond. Dan zetten we het geluid aan. Een beetje blikkerig, maar de gesprekken zijn goed verstaanbaar. We horen ze lachen, praten, lopen.

Ja, dit voelt vreselijk ongemakkelijk.

Waarom hier een camera hangt, weten we niet. Wie deze mensen zijn en waar ze wonen, ook niet. We weten wél welk

merk camera zij bezitten, wat het typenummer is en welke software erop draait. Ook bekend: de gebruikersnaam en het wachtwoord, waarmee van afstand op de camera kan worden ingelogd. Als we dat doen, zien we op het scherm van onze laptop wat het oog van de camera registreert, kunnen we de camera besturen en de instellingen veranderen. Zodat de camera, bijvoorbeeld, 's nachts uitgaat.

Ik heb lang getwijfeld of ik dit wel moest doen. Ik ben hacker, voyeur en inbreker ineen. Ik pleeg computervredebreuk én huisvredebreuk. Maar uiteindelijk besluit ik die morele en juridische grenzen voor een paar uur te overschrijden. Dit is de enige manier om dit verhaal te vertellen.

Het is het verhaal van *The Internet of Things,* het internet der dingen, de technologische ontwikkeling waarbij steeds meer apparaten aan het internet worden verbonden, zodat ze met elkaar kunnen communiceren en van afstand te bedienen zijn. Printers, webcams, televisies, externe harde schijven, geluidsinstallaties, thermostaten: we willen ze *wireless, connected* en *remote accessible*.

Handig, efficiënt en leuk, maar recent staan ook de risico's van *The Internet of Things* volop in de aandacht.

Terecht.

Foto: Arjen Born

Met Slotboom achter Shodan

Mijn gids door het internet der dingen is Wouter Slotboom (35), beveiligingsexpert en ethisch hacker. Een jaar geleden testten wij samen de veiligheid van de wifinetwerken van drie cafés; vandaag testen we de veiligheid van het hele Nederlandse internet.

Dat klinkt grotesker dan het is. We maken gebruik van Shodan, een openbare zoekmachine, die wel 'de Google voor hackers' wordt genoemd. Waar Google de inhoud van webpagina's ontsluit, biedt Shodan informatie over de apparaten die op het internet zijn aangesloten.

Slotboom en ik stellen van tevoren een aantal regels op.

- We doen ons onderzoek in één werkdag.
- We gaan steekproefsgewijs te werk.
- We maken geen gebruik van geavanceerde

hackingtechnologie- of trucs; alles wat we doen moet voor iedereen opzoekbaar zijn.

- Komen we iets tegen dat een direct gevaar oplevert - bijvoorbeeld een energiecentrale die van een afstand is te besturen - dan lichten we die partij eerst in. We willen geen slapende honden wakker maken.

Een kritisch lezer kan nu tegenwerpen: dat doe je al. Door uit te leggen dat Shodan bestaat en te beschrijven hoe het werkt, kun je mensen op verkeerde ideeën brengen.

Als je weet hoe het werkt, kun je Shodan inderdaad voor kwade doeleinden gebruiken. Kinderporno op iemands back-upschijf zetten. Een beveiligingscamera uitzetten. Kopieën van paspoorten downloaden. Het punt is: Shodan creëert zélf geen slechte beveiliging en kwetsbaarheden, het brengt die enkel in kaart.

De zoekmachine laat zo zien dat miljoenen consumenten en bedrijven apparaten aan hun (thuis)netwerk hangen zonder die te beveiligen: ze gebruiken geen wachtwoorden of vergeten de fabrieksinstellingen te veranderen. Dat maakt hen kwetsbaar zonder dat ze het zelf doorhebben.

Zo bezien is Shodan ook een prachtige uitvinding. Het legt kwetsbaarheden bloot die voorheen onzichtbaar waren.

Dit is geen nieuwe boodschap. Het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie waarschuwt sinds 2012 voor deze kwetsbaarheden. 'Shodan,' zegt een woordvoerder, 'kan door goed- en kwaadwillenden gebruikt worden om aan het internet gekoppelde apparaten te vinden.' Maar de woordvoerder benadrukt dat de verantwoordelijkheid voor de apparaten uiteindelijk bij de

gebruikers zelf ligt.

Kruip een dag met Slotboom achter Shodan, en je komt erachter dat die boodschap nog niet bij iedereen geland is.

Surveillancecamera's: check

We beginnen met surveillancecamera's. We zoeken in Shodan op een aantal bekende cameramerken voor de consumentenmarkt. Ze kosten vaak niet meer dan honderd euro en zijn eenvoudig te installeren. Door die camera's aan het internet te verbinden, is het mogelijk ze vanaf verschillende apparaten online te bekijken. Neem de snackbarhouder die thuis op zijn tablet zijn zaak in de gaten wil houden. Of de ouders die tijdens een avondje uit op hun telefoon willen kijken of hun kind rustig ligt te slapen.

Tien zoekacties, elfduizend resultaten.

We zien al direct dat veel van de camera's namen hebben gekregen. 'Opa en Oma cam,' bijvoorbeeld. 'Voordeur.' 'Tuinhuis.'

We zien een gokhal. De voor- en de achterdeur van een huis. Een onbestemde kantoorruimte. Een ijssalon, waar een meisje net een ijsje

Sommige camera's zijn goed met een wachtwoord beveiligd. Daar komen we niet binnen. Maar andere camera's hebben helemaal geen wachtwoord. We krijgen een ip-adres, plakken dat in onze browser en klaar. Weer andere camera's hebben de inloggegevens en wachtwoorden die de fabrikant de

koopt

apparaten standaard meegeeft. Heel vaak is dat: admin/admin. Of: admin/1234.

Sterker: je kunt op Shodan zoeken naar alle apparaten die zélf aangeven dat ze dergelijke fabrieksinstellingen hebben. Dat zijn er schrikbarend veel. 'Het is vergelijkbaar met je huissleutel onder de mat leggen en een briefje op de voordeur hangen met de tekst: 'De sleutel ligt onder de mat,' aldus Slotboom.

We doen een willekeurige steekproef bij 25 camera's uit de resultatenlijst.

Bij tien daarvan hebben we beeld. Naast de hierboven beschreven woonkamer, hebben we toegang tot een camera in een babykamer. We kijken mee in een kapperszaak, waar op dit moment geen klanten zijn. We zien een gokhal. De voor- en de achterdeur van een huis. Een onbestemde kantoorruimte. Een pandjeszaak. Een ijssalon, waar een meisje net een ijsje koopt.

Hier laten we het bij. Nog wel belangrijk om te vermelden: wij doen dit handmatig en steekproefgewijs. Een hacker kan heel eenvoudige geautomatiseerd zoeken naar onbeveiligde camera's en in luttele seconden bij iedereen inloggen en naar binnen kijken.

Printers, back-upservers, routers: check

We gaan verder met de printer. Hartstikke handig natuurlijk, om draadloos te kunnen printen of van overal ter wereld printopdrachten naar je printer te kunnen sturen. Maar zonder beveiliging kunnen er vreemde dingen gebeuren.

Foto: Arjen Born

Wij zoeken weer naar de bekende merken en vinden bijna elfduizend apparaten. We doen een steekproef. Sommige printers zijn beveiligd, bij andere zitten we direct in het systeem. We zouden de instellingen kunnen aanpassen, we kunnen zien welke printopdrachten op dit moment worden uitgevoerd en we kunnen die stopzetten. Bij sommige printers zit een opslagfunctie, waardoor we de printgeschiedenis kunnen inzien. Maar we zouden ook zelf opdrachten kunnen geven en documenten uit de printer laten komen.

We nemen contact op met Hewlett Packard, een van de gehackte merken, waarvan we 1.325 apparaten vinden die zonder wachtwoord door ons te hacken zijn. Een woordvoerder benadrukt dat de veiligheid van de klanten heel belangrijk is voor HP. 'Daarom sporen we klanten aan om printers veilig te gebruiken,' aldus de woordvoerder. Dat 'aansporen' doet HP door de gebruikers op hun site te informeren. En: 'Bij de nieuwe printerseries hebben we deze

informatie ook toegevoegd aan de installatiehandleiding.'

Volgende apparaat: de externe harde schijf. Juist, dat ding waarop je belangrijke documenten, foto's en andere zaken zet die niet verloren mogen gaan. We vinden duizenden back-upservers die aan het internet zijn gekoppeld - vaak de zogenoemde Netwerk Attached Storage (NAS)-schijven.

En ook hier blijkt uit onze relatief kleine steekproef dat we in ongeveer een derde van de gevallen gewoon binnenkomen. We hebben toegang tot vakantiefoto's van gezinnen, notariële akten en contracten van bedrijfsovernamen. We zien paspoorten en diploma's, jaarrekeningen en patenten.

Als een hacker een zwakke plek in een bepaalde router kent en erachter komt dan 200.000 mensen die router gebruiken, kan hij die allemaal infecteren met malware

Eind 2012 maakte het televisieprogramma *KRO Reporter* een reportage over online printers, back-upservers en camera's. Een van de apparaten die het programma onder de loep nam, was de populaire NAS-schijf van iOmega, een onderdeel van Lenovo. Daarop werden onder andere patiëntengegevens van artsen en correspondentie van de Koninklijke Marechaussee gevonden. Na die uitzending beloofde iOmega een software-update om het probleem te verhelpen.

Via Shodan vinden wij in Nederland nog steeds ruim 2.500 iOmega-schijven, waarvan er 1.119 zonder login en wachtwoord te hacken zijn. Een woordvoerder van het bedrijf vertelt ons dat iOmega sinds de uitzending van *Reporter* is gaan werken met een ingebouwd

standaardwachtwoord in de NAS-schijven. Dat kan wel zo zijn, maar wij vinden wereldwijd nog steeds 15.202 iOmega-apparaten die zonder wachtwoord zijn te betreden. Het standaardwachtwoord is via Google wederom simpel te achterhalen. De woordvoerder van Lenovo benadrukt dat de verantwoordelijkheid uiteindelijk bij de gebruiker zelf ligt.

Dat brengt ons bij het laatste huis-tuin-en-keukenapparaat dat wij onderzoeken. De router, een apparaat dat iedereen met een internetverbinding in huis heeft. Een apparaat dat de draadloze apparatuur in huis of op het werk aanstuurt via één internetaansluiting. Die routers zijn gekoppeld aan een modem, die verbinding met het internet maakt.

Via Shodan zijn er honderdduizenden routers te vinden. Ze sturen informatie mee over het merk, het typenummer, de wijze van beveiliging.

Nu zijn we bij het hacken voor gevorderden aanbeland.

Want heeft een hacker eenmaal toegang tot een router kan hij, bijvoorbeeld, het internetverkeer van de gebruiker omleiden, zodat iedere keer als die gaat internetbankieren, hij niet op de site van zijn bank terechtkomt, maar op een perfect nagemaakte site van de hacker. Een andere mogelijkheid is dat de router wordt ingezet als wapen. Als een hacker een zwakke plek in een bepaalde router kent en erachter komt dat 200.000 mensen dat type router gebruiken, kan hij die allemaal infecteren met malware, waardoor ze in zijn bezit komen. Vervolgens kan hij van al die routers een digitale bom maken, een zogenoemd *botnet*, die hij de opdracht geeft om miljoenen pakketjes met data naar een adres te sturen - een website of een systeem-

waardoor deze worden platgelegd. Regelmatig worden op deze manier digitale aanvallen uitgevoerd.

Foto: Arjen Born

Kerncentrale? Windmolens? Stoplichten?

De afgelopen jaren hebben onderzoekers en journalisten veelvuldig kwetsbaarheden gevonden in systemen en apparaten die behoren tot de vitale infrastructuur, in sectoren als energie en watervoorziening. Zo ontdekte een hacker in 2012 dat de rioleringspompen, sluizen en gemalen van de Zeeuwse gemeente Veere te hacken waren. De zwakke plekken zaten in de zogenoemde SCADA-systemen en waren online te vinden en vanaf een laptop vrij simpel over te nemen en te besturen.

Niet gek dat het Nationaal Cyber Security Centrum (NSCS)

al een paar jaar waarschuwt voor de kwetsbaarheden die de koppelingen van SCADA-systemen aan het internet teweeg kunnen brengen. Een van de problemen, schrijft het NCSC, is dat veel van de bedrijven zelf niet weten hoe kwetsbaar ze zijn. De systemen zijn door derden gebouwd.

Inmiddels zijn ook Slotboom en ik bij de SCADA-systemen aangekomen. We zoeken naar een paar bekende merken en serienummers die we via Google hebben gevonden en vullen die in op Shodan. We zien een windmolen, we komen verwarmingssystemen van grote bedrijven tegen. Namen we bij de camera's, de printers en de routers de proef op de som door te kijken wat we allemaal konden als we eenmaal binnen waren, bij deze systemen doen we dat bewust niet. Slotboom: 'Ik vind het letterlijk levensgevaarlijk. Misschien is het wel een molen of een hijskraan die aan- of uitgaat op het moment dat je zo'n systeem betreedt.'

De risico's van genetwerkte apparaten kunnen niet genoeg benadrukt kunnen worden. Maar is dat genoeg? Want wie draagt de verantwoordelijkheid voor de veiligheid van al die genetwerkte apparaten? Consumenten? Fabrikanten? De overheid?

Naar schatting zijn er nu 25 miljard apparaten aan het internet verbonden. Over vijf jaar zou dat aantal volgens prognoses zijn verdubbeld. De meest onverwachte apparaten komen online - van tandenborstels tot stoplichten. Los van de vraag wat het nut en noodzaak van *alles online* is, kunnen de gevolgen van een ondoordachte beveiliging desastreus zijn. Een gehackte elektrische tandenborstel is één, een gecompromitteerde kerncentrale is een ander verhaal.

Met medewerking van onderzoeksassistent Anne Schepers.

Bekijk hier andere versie(s) van dit artikel.