Verantwoorde onthullingen #7

Student geeft universiteit dure les. Hoe @XS4me2all de servers van de Rijksuniversiteit Groningen overnam (2007-2014).

Deze keer een case met een hacker wiens identiteit nog onthuld moet worden. @XS4me2all kreeg in 2007 via enkele kwetsbaarheden toegang tot servers van de Rijksuniversiteit Groningen. Hij deed het voor de kick, maar ziet het nu als een jeugdzonde. Hij wil alsnog opbiechten, mits hij niet vervolgd wordt. Frank Brokken, security manager bij de RUG, heeft hier begrip voor en is ook benieuwd wie hun toen gehackt heeft. Op 4 juni zal ik tijdens het NCSC congres de heren aan elkaar voorstellen. Hier alvast hun verhaal.

Het is begin februari 2007 als Brokken een alarmerende mail binnen krijgt: er zouden meerdere van hun computers gehackt zijn. De afzender wil anoniem blijven, maar Brokken vermoedt dat het een van zijn studenten is. Hij roept het crashteam bij elkaar: de interne specialisten bij computerincidenten. Al snel komen ze erachter dat op de webserver illegale software en video's draaien. Ook de image- en installserver blijkt besmet met malware. Die server is normaal gesproken een hulpmiddel voor systeembeheerders om via het netwerk back-ups of updates te laden. Nu besmet hij automatisch elke computer die hier inlogt. Dat zijn er inmiddels meer dan 250. Op een van de PCs staat zelfs een key logger: de hacker kan dus de toetsaanslagen volgen om zo nog meer wachtwoorden of zelfs credit card gegevens af te vangen.

De universiteit doet aangifte bij de digitale recherche Noord. Brokken kent ze goed en heeft regelmatig contact met hen. Team High Tech crime van de Nederlandse politie wordt er ook bij betrokken. De zaak strandt echter bij het OM. Die besluit niet tot vervolging over te gaan omdat er te weinig concrete aanwijzingen zijn wie de mogelijke dader is. De hacker heeft gewoonweg te weinig sporen achtergelaten. Nader onderzoek wijst wel uit dat een van de systeembeheerders op verschillende plekken hetzelfde wachtwoord gebruikte. "Echt een stommiteit" zegt Brokken en ze hebben de betreffende man op het matje geroepen.

De universiteit neemt nog meer maatregelen. Er wordt een strikt wachtwoorden systeem opgelegd, soms met 2-factor authenticatie. De servers worden opgeschoond, firewalls opgetrokken en alle beheerswerkzaamheden gelogd. Zo kunnen ze in het vervolg beter zien of, waar en wanneer iets mis gaat. "Niet dat we nu bullet-proof zijn, maar zo kunnen we wel alles beter in de gaten houden." Een extern bedrijf doet vanaf moment regelmatig pen tests.

Brokken had al eerder de beveiliging willen opschroeven, maar kreeg daar bij het management de handen niet voor op elkaar. Nu wel. Het incident, dat vanaf dan bekend staat als "de februari hack", heeft hem in die zin geholpen. Hij vond het daarom ook belangrijk om het naar buiten te brengen. "Organisaties worden gehackt, dat is een fact of life. Niet omdat ze hun beveiliging niet op orde hebben, maar door een mentaliteit onder de medewerkers. Als je ziet hoeveel mensen er nog in phishing mails trappen... En dan zo'n mentaliteit van: dat moeten ze bij ICT maar oplossen. Dat is fundamenteel fout."

Op 7 maart komt woordvoerder Jos Speekman via het ANP naar buiten met het bericht dat de computers van de RUG gehackt zijn. Op de getroffen systemen zou software geïnstalleerd

zijn, waarmee cybercriminelen persoonlijke informatie kunnen stelen, zoals wachtwoorden en creditcardgegevens. Ze zouden de computers bovendien op afstand kunnen bedienen, bijvoorbeeld om illegaal films en software aan te bieden, of spam te versturen. De universiteit vermoedt dat de computers van binnenuit door een medewerker of student zijn gekraakt. De schade wordt geschat op 100.000,- euro. Het bericht wordt overgenomen door de Volkskrant, Trouw, Nu.nl, Webwereld en security.nl. Zo komt het bericht ook terecht bij de hacker.

@XS4me2all is dan een jongen van twintig. Formeel is hij op dat moment nog wel student, maar niet aan de universiteit Groningen. Eigenlijk doet hij niets meer aan zijn studie, omdat hij dagelijks tot in de late uren het internet afstruint, op zoek naar nieuwe hackmethoden en steeds grotere targets. Voor de kick. Hij leert zo veel meer dan bij zijn studie. Nu hij leest hoeveel schade hij heeft toegebracht schrikt hij zich rot. Eigenlijk had hij de systeembeheerder willen bellen om te vertellen wat hij had gedaan – dat deed hij wel vaker – maar nu lijkt het hem wijzer zijn mond te houden. Toch blijft de zaak aan hem knagen. Vijf jaar later hoort hij over mijn onderzoek. Hij wil alsnog via mij opbiechten wat hij heeft gedaan.

In zijn studentenkamer vertelt hij mij hoe hij te werk ging. Het eerste wat hij aantrof op het universiteitsnetwerk was een printserver die online stond. Het wachtwoord was versleuteld, maar hij kon wel de hash van het wachtwoord zien. Op internet circuleren allerlei lijstjes – rainbow tables - van dergelijke hashes waarmee je het wachtwoord kunt achterhalen. En ja, hij vond een match. Met gebruikersnaam “admin” en wachtwoord “S4k1nt0s!” kon hij erin. Nu kijken of deze administrator nog meer systemen online heeft staan. Dat bleek het geval. Maar hij kon niet overal in want de admin was van een bepaalde studierichting en kon niet inloggen buiten zijn eigen domein.

Hij herhaalde de truuk met de hashes en rainbow table bij andere systeembeheerders en kwam erachter dat er veel overlap was in hun beheersdomeinen. Via die overlap kon hij makkelijker overstappen van het ene domein naar het andere. Hij zag ook dat ze allemaal een ConsoleOne van Novell gebruikten om het systeem te beheren en die was ook via internet benaderbaar. Dat zal makkelijk zijn geweest voor de systeembeheerders als ze van een locatie alle systemen willen updaten. Maar ook voor @XS4me2all. Via de beheerdersingang, poort 1761 van de console, kon hij nu vanaf zijn studentkamer het hele netwerk van de Rijksuniversiteit Groningen besturen.

Om niet elke server stuk voor stuk te hacken had hij een ander plan bedacht. Hij nam de image en install server, daar installeerde hij zijn eigen malware in de gereedstaande images. Iedereen die nu inlogde, besmette dus zo zichzelf. Binnen een maand had hij toegang tot alles. Op een enkele computer zette hij ook wat malware die leek op een key-logger, gewoon om te zien of het kon, zonder hem te gebruiken want hij kon toch al overal in. Het leukste vond hij de wake on LAN functie, waarmee je op afstand computers aan kan zetten. Dat deed hij dan s ‘nachts. “Stel je voor, is daar zo’n schoonmaker aan het werk, gaan ineens alle computers aan… Kicken!”

Daarmee was zijn missie geslaagd. Het ging hem er niet om de universiteit schade toe te brengen. Het is puur de kick ergens in te komen. Vol enthousiasme vertelt hij erover aan

andere hackers op een gesloten chat forum waar hij lid van was. Die geloven hem niet en willen bewijs zien. Dat kan: geef mij een film en dan laat ik die vanaf hun server draaien. Als hij dit doet, kijkt er waarschijnlijk iemand mee die het waarschuwende mailtje naar de universiteit stuurt. Anders kan niet, want hij heeft tegen niemand verteld hoe ze er in konden. Hij was volgens hemzelf de enige.

@XS2all4me blijft de zaak volgen in de media. Gaandeweg krijgt hij meer respect voor security manager Frank Brokken die openlijk vertelt over het incident en zelfs zegt dat ze er veel van geleerd hebben. Hij ziet tot zijn verbazing op fok.nl ook een video van Studenten TV, met daarin een interview met de zogenaamde RUG hacker. Dat vond hij minder leuk. “Staat er zo’n gozer in het donker met vervormde stem… die zei echt onzin en maakte het probleem veel groter dan het daadwerkelijk was.” Hij had liefst zelf met Brokken willen praten, om te vertellen wat hij heeft gedaan en waarom, maar wil uit angst voor represailles niet naar buiten komen. Totdat hij in 2013 mij ontmoet. Zijn geweten knaagt, hij wil schoon schip maken. Ik stel voor te bemiddelen tussen beiden.

Ik stuur Brokken een mail waarin ik vertel over mijn onderzoek en hem vraag om meer documentatie. Ik stel ook voor een ontmoeting te arrangeren tussen hem en de hacker, mits de universiteit afziet van strafvervolging. Hij reageert positief: “In het delen van ervaringen ben ik altijd geïnteresseerd, ik zie geen reden om op het bekend maken van een kwetsbaarheid te reageren met juridische acties. De hacker hoeft wat dat betreft niet bevreesd te zijn en kan denk ik zelfs wel rekenen op een kopje koffie ;-)” Zijn mail is gesigneerd met PGP. Ik weet dan nog niet wat dat is en begrijp ook niets van al die codes onderin zijn mail, maar voor @XS4me2all is dit voldoende als vrijwaring. We kunnen van start.

In mijn gesprek met Brokken merk ik geen wrok of frustratie, maar eerder bewondering voor hetgeen de hacker heeft gedaan. “Ik vind het geweldig dat die jongen het op deze manier heeft gedaan. Als jij toegang hebt tot de server die software installeert op andere machines, wordt het werk door de organisatie gedaan. Dat is prachtig.” Brokken moet zelfs hartelijk lachen als ik vertel hoe s ‘nachts de computers werden aangezet. Na beide heren te hebben gesproken, schrijf ik dit stuk en zie uit naar 4 juni. Dan zijn we samen in het Worldforum voor een verantwoorde onthulling.

Chris van ’t Hof (www.cvth.nl)