“Hacken is kinderspel. Maar met het geld aan de haal gaan?”

De opkomst van Anonymous en LulzSec, de Playstation-files, de bank-Trojanen en de forse toename van het aantal gehackte sites in België: cybercrime is niet meer weg te slaan uit het nieuws. Twee notoire pentesters laten hun licht schijnen over de zaak. “Wij worden betaald om te doen wat we graag doen”, klinkt het, “waarom zouden we dan overlopen naar de *dark side*?” #Frederik Tibau

ALLA BEZROUTCHKO

FILIP WAEYTENS

De Russische Alla Bezroutchko raakte geïnteresseerd in security toen ze na haar studies aan de slag ging als systeemadministrator. “Het gaf een kik, inbreken in een computersysteem”, spreekt ze uit ervaring. “Maar een job in de securitysector zag ik (nog) niet zitten. Of toch niet in Rusland. De bedrijven daar zijn té sterk gelinkt aan de overheid. Dat lag me niet zo.”

Via een tussenstop bij Belgacom kwam Bezroutchko terecht in het pentesters-team van Skynet (pentesters zijn it’ers die van ‘legaal’ hacken hun beroep hebben gemaakt), waar ze zou blijven tot goed en wel een jaar geleden. Intussen heeft ze met haar man een eigen bedrijfje opgericht (www.gremwell.com), dat gespecialiseerd is in ethische hackpraktijken en consultancy.

Filip Waeytens werkte als office manager in de toeristische sector tot hij zich realiseerde dat er meer te rapen valt in it. “Computers waren sowieso een hobby, en tijdens mijn doortocht bij backboneprovider Ebone raakte ik geïnteresseerd in het veiligheidsaspect. Terwijl mijn collega’s films keken, las ik securityboeken. Niet veel later mocht ik de firewalls van grote klanten zoals Dell beheren.”

Toen Ebone op de fles ging, belandde Waeytens bij Skynet, waar hij Alla leerde kennen. Later werd hij binnengehaald als securitymanager bij Esselte, tot ook hij als onafhankelijk pentester aan de slag ging. Overigens is Waeytens één van de initiatiefnemers van BruCon, de Belgische hackersconferentie die plaatsvindt op 19 en 20 september.

Hebben jullie eigenlijk sympathie voor ‘hacktivism’-activiteiten, waarbij websites worden gekraakt voor ‘het goede doel’, of als daad van protest?

ALLA BEZROUTCHKO: “Dat hangt er van af. Doen de hackers meer kwaad dan goed, of is het tegendeel waar? Soms vestigen hacktivisten de aandacht op een probleem, en dat is positief. Maar tegelijk zijn ze ook de oorzaak van veel ellende, bijvoorbeeld als er persoonlijke informatie publiek wordt gemaakt.”

FILIP WAEYTENS: “Voor mij is hacktivisme een misdaad. Websites zijn het bezit van iemand anders, en het is wettelijk verboden om daar toegang tot te zoeken. Het is toch

niet omdat er digitaal gewerkt wordt, dat er plots andere regels gelden? Als je wil reageren op dingen die niet door de beugel kunnen, schrijf dan een blog. Of mobiliseer mensen via Facebook."

Alsmaar meer Belgische sites worden gehackt. Het Belgische CERT diende de voorbije weken duizenden particulieren en bedrijven aan te schrijven met de boodschap dat hun webstek gekraakt was. Hoe komt dat?

WAEYTENS: "De jongeren hebben momenteel schoolvakantie (lacht). En uiteraard zijn de mediagenieke optredens van de hackersgroepen Anonymous en LulzSec een katalysator. Heel wat pientere computerwhizzkids willen zelf ook wel eens iets uitproberen, dat is *cool*. Ik betwijfel trouwens of Belgische sites kwetsbaarder zijn dan andere. Ik heb in het verleden aan pentesting gedaan voor bedrijven in het Midden-Oosten, en die zijn niet beter af als wij."

BEZROUTCHKO: "Security heeft eindelijk de 'echte' wereld bereikt, dat verklaart voor een stuk de verhoogde aandacht in de media. Tien jaar geleden kreeg je niet uitgelegd dat servers kwetsbaar waren voor hackers, zelfs topmanagers konden dat niet vatten. Maar intussen zijn computersystemen zo cruciaal geworden voor ondernemingen -en is hacken zo winstgevend voor criminelen- dat iedereen er mee bezig is. Zelfs Jan met de pet kan een slachtoffer worden."

België zou een gemakkelijk doelwit zijn voor cybercriminelen omdat er geen globaal federaal beleid voorhanden is inzake informatieveiligheid.

WAEYTENS: "Volgens mij is niet zozeer het ontbreken van een beleid het probleem. Wel dat de echte slimmeriken, de mensen met de beste security-skills, veel meer kunnen verdienen op de private markt. Je moet al een echte idealist zijn, of de morele nood voelen om voor de overheid te werken, eer je daarvoor kiest. En laat ons eerlijk zijn: zoveel idealisten lopen er niet rond in it."

"Wist je trouwens dat België één van de laatste landen was om een CERT-team op te richten? Zelfs de landen in ex-Joegoslavië waren sneller. Dit gezegd zijnde, merk ik wel dat er wat beweegt bij CERT.be. Dat is positief. We laten hier een kans liggen hoor. Als klein land zou België een voortrekkersrol moeten spelen op het vlak van cybersecurity. We zouden moeten specialiseren in dat domein."

Niet zo lang geleden werd het netwerk van Sony gehackt. En de jongens van Anonymous willen op 5 november Facebook platgooien. Zijn we in een nieuwe fase beland? Worden grote publieke netwerken het doelwit?

WAEYTENS: "Anonymous wil nog eens in het nieuws komen, *that's all*. Een goed georganiseerde misdaadorganisatie gaat Facebook toch niet aanvallen? Die richt haar pijlen toch op een bank? En gaat dat toch niet aan de grote klok hangen?"

BEZROUTCHKO: "Als er één ding veranderd is, dan wel dat je je tot voor kort nog een onveilig netwerk kon permitteren, omdat er toch niet veel incidenten waren. Vandaag is het tegendeel waar. Je valt onmiddellijk door de mand met een netwerk vol gaten. Vraag maar eens aan Facebook of Twitter."

In heel wat landen is elke vorm van pentesting verboden. Niemand mag er een netwerk hacken, ook jullie niet. Is jullie job wel legaal?

BEZROUTCHKO: "We werken in de schemerzone (lacht). Daarom ook dat we pas aan de slag gaan als we een getekend contract in handen hebben. Onze advocaat oppert dat niemand ons iets kan maken zolang we zo'n contract op zak hebben. En in België is het niet verboden om in het bezit te zijn van hacking tools."

"Hacktivism is een misdaad. Als je wil reageren op dingen die niet door de beugel kunnen, schrijf dan een blog."

BLACK HATS

Heel concreet: wat vragen klanten juist?

BEZROUTCHKO: "Negen op de tien keer moeten we webapps testen. Bedrijven die een dergelijke toepassing gebouwd hebben, of laten bouwen hebben, willen wel eens weten hoe veilig die is. Zeker als het de bedoeling is een iso-certificaat te bekomen. Dat willen ze vaak hebben om extra centen binnen te halen."

"Er zijn bedrijven die de wijzigingen die we voorstellen binnen het uur doorvoeren. Andere stellen het zo lang uit, dat we bij een volgende test net hetzelfde moeten zeggen. Veel hangt af van de interne cultuur binnen het bedrijf."

Waeytens: "Kleine bedrijven reageren vaak sneller dan grote. In een grote onderneming is security nog vaak een departement dat is weggestoken onder verschillende managementlagen. Dat werkt niet snel, wel integendeel, en heel wat aanpassingen gaan verloren in de hiërarchie."

Komen jullie vaak in contact met black hats? Met hackers die overgelopen zijn naar de *dark side*?

WAEYTENS: "Ik werk veel rond BackTrack Linux, waarvoor ik vaak rondhang op irc (internet relay chat). Daar word ik regelmatig gecontacteerd door vreemde vogels die me vragen om deze of gene site te hacken. Het is dan zaak om meteen *neen* te zeggen, en je grens te trekken. Anderzijds is het wel nuttig om te weten waar die mensen mee bezig zijn. Soms is het echt beangstigend wat ze allemaal zeggen, maar je mag die dingen niet al te serieus nemen. Er zitten heel wat opscheppers bij."

BEZROUTCHKO: "Ook ik word wel eens gecontacteerd na het publiceren van een exploit, maar dan negeer ik dat gewoon. Wij worden goed betaald door onze klanten om iets te doen dat we graag doen.

Waarom zouden we ons dan inlaten met dingen die niet door de beugel kunnen? Keer op keer worden we gevraagd of het niet kietelt, maar neen, dat is echt niet het geval (lacht)."

WAEYTENS: "Als je als pentester ook een black hat opzet, dan kan je er van op aan dat je vroeg of laat ontmaskerd wordt. En dan is je reputatie meteen om zeep. Dat kan toch niet de bedoeling zijn?"

Hoe kan een bedrijf er zeker van zijn dat je de kennis die je opdoet, niet gaat misbruiken of doorverkopen aan de concurrentie?

BEZROUTCHKO: "Wat is het leukste denk je? Hacken en daar nog voor betaald worden ook, of data ontvreemden om door te verkopen aan derden, met al de stress die daarmee gepaard gaat?"

"Kijk, ergens inbreken is kinderspel. Maar eer je dan met het geld aan de haal kan gaan? Neem de recente Trojanen in de banksector. Daar gaat het niet over eenmansoperaties, maar wordt er gewerkt met tussenpersonen en met geldezels. Dat is maffia hoor, dan gaat het echt niet over een *geek* die met een stukje pizza achter zijn computer zit."

Staan de vaardigheden van pentesters wel op het niveau van de skills van black hats?

WAEYTENS: "Dit is onze job, we zijn er de hele dag mee bezig. Bij veel black hats is dat niet zo. Wij krijgen ook voortdurend gevoelige informatie doorgespeeld van bedrijven, en zien zo heel wat netwerkarchitecturen. Black hats moeten die dingen zelf uitpluizen."

"Kwaadwillenden hebben dan weer het voordeel dat ze in teams werken. Ze hebben iemand die de servers hackt, iemand die de software kopieert, ... Je kan nog het best vergelijken met een bankoverval. Daar rijdt iemand met de wagen, kraakt een tweede de kluis, terwijl een derde de camera's uitschakelt. "Overigens raakt ook de white hat gemeenschap gefragmenteerd. De beroemdheden in de security-sector hebben allen hun specialiteit. Je hebt mensen die enkel iPhone of Android doen, er zijn er die specialist zijn in *reverse engineering*... Er komen alsmaar meer specialisatieniveaus bij, waardoor het steeds moeilijker wordt om het overzicht te bewaren."

Vandaag is het al mobiel wat de klok slaat. Hoe gaat het er *security-wise* aan toe in dat wereldje?

BEZROUTCHKO: "We zitten nu in de onderzoeksfase, zowel de white hats als de black hats. Iedereen wil snel snel een app, maar als die dingen dan niet nagekeken worden, raak je in de problemen. Denk maar niet dat Apple en Google alle code scannen op zwakheden."

Waar wordt het vaakst tegen gezondigd?

WAEYTENS: "De top tien is eigenlijk nog steeds dezelfde als enkele jaren geleden. Cross-site scripting, access control, sql-injectie, file upload problemen, ... : die dingen veranderen niet. Hoe dat komt? Omdat security te laag op het prioriteitenlijstje staat van de ontwikkelaars."

BEZROUTCHKO: "De meeste programmeurs hebben strikte deadlines, en het gros van de apps werkt niet stand alone: ze moeten kunnen praten met andere toepassingen. Wanneer die dingen klaar zijn en werken, zijn de ontwikkelaars al tevreden."

"Dat dezelfde fouten gemaakt blijven worden, heeft ook een financiële oorzaak. Als je 5.000 euro betaalt voor een toepassing, ga je dan nog eens 5.000 euro extra ophoesten om het ding te laten testen?"

WAEYTENS: "*In the end* gaat het om risicoberekening. 'Wat gaat een incident me kosten?' Is de pentest duurder, dan kiezen de meeste bedrijven voor het incident, maak je geen illusies."#

Quantum legt zich toe op deduplicatie en schijven

Quantum, dat al lang gekend is om zijn tapetechnologie, legt zich voortaan toe op twee technologieën: deduplicatie en software om bestanden te delen op StorNext-schijven. #Marc Husquinet

Quantum verloochent uiteraard zijn verleden van tapespecialist niet waarin "we de absolute leider zijn, ondanks het feit dat de markt achteruitgaat", aldus Jon Gacek, in januari van dit jaar aangesteld als ceo. Met als enige concurrent StorageTek, overgenomen door Sun, op zijn beurt overgenomen door Oracle, blijft het bedrijf zijn Scalar-gamma in de handel brengen.

Quantum heeft het de laatste jaren echter bijzonder moeilijk gehad om zich op de markt te handhaven. Zijn omzet daalde namelijk van 1,1 miljard dollar in 2002 naar 634 miljoen dollar in 2006, om in 2007 weer de stijgen naar 1,1 miljard na de overname van Adic, en vorig jaar weer te dalen tot 681 miljoen dollar. "Maar sindsdien genereren we weer cash", zegt de baas van Quantum trots. "We moeten aan de markt bewijzen dat we er weer staan." En dat Quantum een wereldwijd bedrijf blijft met inmiddels zo'n 2.000 medewerkers.

Specialisten

Maar Quantum wil zich voortaan als "specialist" profileren om het met de woorden van zijn ceo te zeggen, en vooral groeiniches veroveren door zich dus niet meer te beperken tot data management maar ook software en bestanden erbij te nemen. Zo'n niche is de markt van het opslagbeheer, die met ongeveer 15% per jaar groeit, of die van de opslagtoestellen met een groei van 20% per jaar.

> **"We moeten aan de markt bewijzen dat we er weer staan."**

Na de recente overname van Pencatera, houdt het bedrijf zich voortaan ook bezig met virtuele omgevingen met als ambitie een back-uptoestel voor dit soort vm te ontwikkelen. Maar Quantum legt zich vooral toe op zijn twee laatste nieuwigheden. Enerzijds DXi 2.0, een softwarepakket voor de bewaring, deduplicatie en replicatie van gegevens dat volgens het bedrijf performanter zal blijken en een betere verhouding tussen prijs en prestaties zal leveren dan de concurrerende producten. Een product dat sinds deze zomer in de platformen DXi 6700 en DXi 8500 ingebouwd zit. De andere nieuwigheid is het StorNext M330-toestel voor organisaties die geconfronteerd worden met (zeer) grote volumes gegevens, en meer bepaald videostreams die moeten worden beheerd en gedeeld.

Hoewel Quantum op dit ogenblik nog geen cloud-aanbod heeft, denkt zijn ceo dat "StorNext een etappe op weg naar cloud computing en een tiering-niveau kan zijn."#