Bart Jacobs, hoogleraar Security en correctheid van software:

Jagen op hackers bevordert slechte beveiliging

Eigenlijk is Bart Jacobs wiskundige, wat hem via verificatie van software op het spoor van computerbeveiliging zette. Sinds onder zijn supervisie de OV-chipkaart gekraakt werd, is hij in de media 'de hackingprof' uit Nijmegen. Gevreesd criticaster van de 'naïeve gedachte' dat beveiliging ooit klaar kan zijn. Een beetje tegen wil en dank: "Fundamenteel onderzoek is boeiender, maar databeveiliging is maatschappelijk belangrijk en buiten de wetenschap spreken maar weinigen zich er over uit zonder een bedrijfsbelang te dienen. Dus doe ik het maar."

door: ROLF ZAAL / R.ZAAL@SDU.NL **beeld:** DE BEELDREDAKTIE / ERIK VAN 'T HULLENAAR

Het lijkt er op dat de online criminaliteit terrein wint op de beveiligers. We zien de laatste tijd een staccato van debacles: OV-chipkaart, DigiD, gestolen klantgegevens, frauduleuze overboekingen, logins voor e-mail die op straat liggen. Het bestaan van hackers kan voor bedrijven al lang geen verrassing meer zijn, maar waarom acteren ze er zo weinig op? Door het op grote schaal voor eigen rekening nemen van schade wekken banken de indruk hacking als 'fact of life' te accepteren. Is er nog wel een valide business case voor gedegen beveiliging?

"Daar is geen generiek antwoord op mogelijk. In specifieke markten is de business case voor beveiliging er heel evident wel. Denk aan militaire toepassingen en geheime diensten. Reken maar dat ze daar hogere eisen stellen. Tegelijkertijd zien we ook situaties waarin men - al dan niet terecht - vindt dat beveiliging niet te veel mag kosten of niet ten koste mag gaan van het gebruiksgemak. De meeste banken hanteren verschillende niveaus van beveiliging. Onder een bepaald bedrag kun je met één code uit je random reader overboeken. Bij hogere bedragen moet je het totaalbedrag nog bevestigen. En weer een trapje hoger moet je ook het nummer van de doelrekening invoeren. Dan wordt het voor zo'n criminele 'man in the middle' echt lastig. Een bank kan wat beveiligingsniveau betreft dus best wel aan knoppen draaien, maar meer beveiliging maakt elektronisch bankieren in principe ook voor de consument ingewikkelder. Daarmee neemt de kans op fouten toe, en dat leidt weer tot meer telefoontjes naar de helpdesk. Dat willen de banken niet, dus accepteren ze dat er zo nu en dan een frauduleuze overboeking tussendoor slipt. Zolang het de winst niet in gevaar brengt, is dat kennelijk geen probleem.

Hetzelfde zien we eigenlijk bij de OV-chipkaart. Daar is gekozen voor een NFC-chip waarvan toen al duidelijk was dat hij te hacken zou zijn. Vervanging is duur en daarom draaien ze nu elke nacht een controle op alle transacties om na te gaan of er niet iemand met een zelf opgewaardeerd reissaldo heeft gereisd. Dat lijkt omslachtig, maar het is blijkbaar 'economisch verantwoord'.

Een factor die daarbij meespeelt is dat de overheid slechte beveiliging soms faciliteert door op de hackers te gaan jagen. Daarmee maken ze in feite het beveiligingsprobleem van een bedrijf tot een zaak van de gemeenschap. Natuurlijk moet je boeven oppakken, maar als de verantwoordelijke zelf zich structureel onvoldoende inspant om zich tegen digitale inbraken te wapenen, dan zou de overheid toch moeten zeggen: doe eerst je eigen werk goed en kom dan nog eens terug voor de echt zware inbraken die zich dan incidenteel voordoen. Maar dat is hier kennelijk niet het beleid. Dat is een van de factoren geweest waardoor de banken zo lang hebben kunnen talmen met het aanpakken van skimming. Tien jaar geleden was al volkomen duidelijk dat die magneetstrip op zo'n bankpasje te vervalsen zou zijn. Toen dat ook gebeurde werd het een zaak voor de politie, die uiteindelijk zelfs een landelijk Skimming Point inrichtte om de samenwerking met de banken te stroomlijnen. Nou, dan praat je kennelijk niet meer over de bestrijding van opzichzelfstaande fraudegevallen.

Door dit type standaard hacks routinematig te vervolgen bevordert de overheid de business case voor betere beveiliging niet. Wat wel had moeten gebeuren, is natuurlijk dat de minister van Financiën al bij de eerste berichten over skimming de banken publiekelijk te kijk had gezet door te roepen dat het een schandaal is en dat de banken onmiddellijk hun verantwoordelijkheid moeten menen.

Het heeft er even naar uitgezien dat het met de aanpak van OV-chipfraude dezelfde kant op zou gaan. Ook hier riep de overheid dat zelf opwaarderen fraude is en dat ze zouden vervolgen. Nu, ze hebben eenmaal iemand opgepakt en voor zo ver ik weet daarna niet meer. Waarschijnlijk zien ze nu ook wel in dat het niet de taak van de overheid kan zijn te repareren wat Translink zelf kennelijk fout heeft gedaan."

Staat beveiliging voldoende op de agenda bij algemeen management?

"Absoluut niet. Regelmatig zie ik begrotingen en aanbestedingen waarin nauwelijks iets over beveiliging wordt vermeld, terwijl er pagina's en pagina's vol geschreven worden over alle ins en outs van de functionaliteit. Beveiliging wordt kennelijk beschouwd als iets wat door IT'ers onder de motorkap wel in orde wordt gemaakt.

En dat is eigenlijk heel vreemd, want als je even om je heen kijkt, zie je dat beveiliging en privacy zo'n beetje faalfactor nummer 1 is bij grote IT-projecten."

Bart Jacobs: "Beveiliging wordt beschouwd als iets dat door IT'ers onder de motorkap wel in orde wordt gemaakt. En dat is heel vreemd."

Kun je als CEO erg veel meer over beveiliging zeggen dan dat het adequaat moet zijn?

"Zeker wel. Een gebruikelijke aanpak is het eisen van een analyse in termen van assets, threads en controls. Dat betekent dat je eerst kijkt wat je digitale bezit is. Voor deze universiteit zou daar bijvoorbeeld uit kunnen komen: personeelsdatabases, studentendatabase met cijferregistraties, en onderzoeksresultaten. De bedreigingen op deze assets verschillen. De personeelsdatabase bevat allerlei privégegevens en moet natuurlijk goed beveiligd zijn, ook al is er geen duidelijk profiel van mogelijke aanvallers. Maar die cijferdatabase, dat mag duidelijk zijn: er zullen studenten zijn die daar graag zo nu en dan iets in willen kunnen aanpassen. Nu, studenten zijn over het algemeen slim en hebben veel tijd maar weinig budget. Zoek dus een beveiliging die bij dat profiel past. Onderzoeksresultaten, daarin zijn concurrerende onderzoeksgroepen en bedrijven mogelijk geïnteresseerd. Misschien ook vreemde mogendheden. Daar is waarschijnlijk ook geld beschikbaar om in te breken, dan weet je dat je zelf dus ook moet investeren om dat tegen te gaan."

U heeft onlangs geroepen dat bedrijven er structureel van uit mogen gaan dat ze ongeveer een kwart van de investeringen in online systemen voor beveiliging zullen moeten reserveren. Is dat niet enorm veel geld?

"Nou ja, die 25 procent was eerlijk gezegd een beetje een slag in de lucht. Het zal per situatie verschillen. Maar goed, wat mag beveiliging kosten? Om het even bij de banken te houden; die besparen met elektronisch bankieren miljoenen. Voorheen hadden ze zalen vol met datatypistes nodig om al die handgeschreven overboekingen in te tikken. Nu doen de rekeninghouders dat voor ze. Dat levert een gigantische besparing op. Daar kan heus wel een behoorlijke beveiliging van worden bekostigd. Hetzelfde geldt voor de OV-chipkaart, dat project is ook opgezet als een efficiencyoperatie. Kosten voor beveiliging horen bij zo'n project integraal deel uit te maken van de business case. En niet alleen initieel, maar gedurende de gehele life cycle. Beveiliging is een proces en niet een ding, dat op een bepaald moment klaar is."

Als beveiliging binnenkort wordt opgewaardeerd van sluitpost naar een issue dat 20 tot 30 procent extra IT-budget vergt, dan lijkt me dat voor IT-bedrijven een verheugende ontwikkeling.

"Niet alleen voor IT-bedrijven. Een serieuze agendering van beveiliging zou een veel bredere economische impuls kunnen geven. In de jaren zeventig was er bezorgdheid dat al die milieueisen een enorme druk op de economische groei zouden veroorzaken. Het tegendeel is waar gebleken. 'Groene technologie' is een op zich staande economische factor aan het worden en we kunnen, dacht ik, toch wel stellen dat Nederland het wat dat betreft heel aardig doet."

Bart Jacobs (1963) is hoogleraar Security en correctheid van software aan de Radboud Universiteit Nijmegen, lid van de Cyber Security Raad van het Ministerie van Veiligheid en Justitie en voorzitter van de adviesraad van Bits of Freedom.