



Illegale onderzoeksmethoden?

De afgelopen weken is de top van Hewlett Packard uitgebreid in het nieuws geweest. Het begon allemaal met een lek in de directie van HP. Bestuursvoorzitter Patricia Dunn wilde uitzoeken wie dit lek veroorzaakte. Hierbij is een bureau in de armen genomen. Verschillende media, waaronder The New York Times, melden dat het zou gaan om Security Outsourcing Solutions uit Boston. Het probleem hierbij is dat men door middel van een techniek, die "pretexting" heet gegevens van de directeuren en ook van journalisten natrok. Er werd ook gesproken van het afluisteren van journalisten en directeuren. De lekkende directeur is overigens gevonden. Volgens velen is de gevolgde methodiek strafbaar. De zaak is onder de openbaar aanklager van de staat Californië. De zaak die nu al "HP-gate" wordt genoemd koste uiteindelijk bestuursvoorzitter Patricia Dunn en topjuriste Ann O. Baskins de kop. Zij konden vertrekken.

Wat is pretexting?

Er is hier een techniek gebruikt die ook wel "pretexting" wordt genoemd. Pretexting is het verzamelen van gegevens over een bepaalde persoon, waarbij gebruik wordt gemaakt van het aannemen van een valse identiteit.. Natuurlijk is een (groot) deel van gegevens over een persoon openbaar en dus vrij verkrijgbaar. Zo zijn bijvoorbeeld Kadastrale gegevens bijvoorbeeld (tegen betaling) op te vragen. Afhankelijk van de bevoegdheden van het onderzoeksbureau zijn ook andere gegevens, bijvoorbeeld over betalings(wan-)gedrag en dergelijke op te vragen. Ook is van een persoon vaak heel veel informatie op het internet te vinden. Vaak veel meer dan de betrokken persoon zich bewust is. Het is vaak niet moeilijk om (legaal) een behoorlijk compleet plaatje over een persoon te vinden.

Het wordt anders er geprobeerd wordt om onder valse voorwendsels gegevens over iemand boven tafel te krijgen. In dit geval zijn telefoonrecords opgevraagd. Op die manier is te zien door wie en met wie de betrokken persoon de afgelopen tijd heeft gebeld.

In de genoemde zaak is gebruik gemaakt van persoonlijke gegevens, zoals het social security number om bij de telefoonmaatschappijen de logrecords op te vragen van de gesprekken van de afgelopen periode.

Het onderzoeksbureau, wat in opdracht van HP werkte, heeft door de telefoonrecords van de directeuren en van 9 journalisten op te vragen en te relateren aan vergaderingen van de Raad van Bestuur, na kunnen gaan waar het lek zat.

Het opvragen van dergelijke privégegevens, bovendien onder een valse identiteit, is illegaal. Het is een vorm van identity theft.

De vraag kan bovendien worden gesteld of het ethisch gezien verantwoord is om onethisch gedrag (het lekken van vertrouwelijke informatie) moet worden bestreden met onethische methoden.

Indien een onderzoek moet worden ingesteld naar onethisch gedrag in een organisatie, zijn er ook legale middelen beschikbaar om de dader op te sporen.

In bovengenoemde zaak had men bijvoorbeeld een "tap" op de bedrijfstelefoon kunnen plaatsen of op de mailbox van de betrokken medewerkers van het bedrijf. Dit zijn onder voorwaarden legale middelen om onethisch gedrag in een organisatie op te sporen en te sanctioneren.

Nieuwe database voor Process Dependency Analysis Tool (PDA2L)

Secure Connection komt binnenkort met een nieuwe database uit voor PDA2L. In deze database zijn de maatregelen geactualiseerd op basis van veranderende technieken, nieuwe inzichten en dreigingen niveaus. Alle klanten van PDA2L met een onderhoudscontract zullen deze database binnenkort ontvangen. Mocht u hierover vragen hebben, dan kunt u uiteraard altijd contact met ons opnemen.

Actueel

Toename van SPAM

Symantec concludeert in haar halfjaarlijkse Internet Security Threat Report dat het aantal SPAM als percentage over de totale hoeveelheid email in de periode jan-juni 2006 is toegenomen tot 54%. In het laatste halfjaar van 2005 lag dit percentage op 50%. Over de eerste helft van 2005 werd nog een percentage van 61% gemeten. Vanaf maart 2006 is ook het aantal "image" spam (een plaatje, waarin de boodschap staat, terwijl in de SPAM email verder geen enkele tekst staat) toegenomen. Deze vorm van SPAM is veel lastiger als SPAM te herkennen, omdat er niet op woorden kan worden gescand.

Kijkend naar de herkomst van SPAM blijft de USA de grootste leverancier met 58% van alle SPAM (was 56% over het laatste halfjaar van 2005). In de USA zijn veel particuliere breedbandverbindingen met PC's die altijd aanstaan. Veel van deze PC's worden door spammers misbruikt. Nederland komt overigens niet voor in de top 10 van herkomst van spam. België bezet met 4% een 8e plek in deze ranglijst.

Bron: Symantec Internet Security Threat Report Jan-Juni 2006
<http://www.symantec.com/>

