

Utrecht, 10 oktober 2006

Informatiebeveiliging: dweilen met de kraan open

Aantal incidenten nam af, maar per incident werd meer schade berokkend

Eénderde van de Nederlandse organisaties was het afgelopen jaar slachtoffer van beveiligingsincidenten. Het aantal incidenten nam daarmee af ten opzichte van het voorgaande jaar; de incidenten zelf worden echter steeds ernstiger. Bovendien geeft een groot aantal organisaties aan op dit moment niet ‘in control’ te zijn van hun beveiliging. De vrees bestaat daarom dat veel organisaties kwetsbaar blijven voor beveiligingsincidenten. Ook organisaties die de beveiliging wél prominent op de agenda hebben lopen vaak achter de feiten aan. De criminaliteit bedenkt constant nieuwe inbraakstrategieën; organisaties worden in een reactieve rol gedwongen. Van vooruitlopen op nieuwe ontwikkelingen is geen sprake.

Deze conclusies zijn afkomstig van het door Capgemini uitgevoerde onderzoek ‘Informatiebeveiliging 2006’. Aan dit onderzoek is deelgenomen door directieleden en managers van meer dan 250 Nederlandse bedrijven en overheidsorganisaties. Het onderzoeksrapport wordt woensdag 11 oktober gepresenteerd op de beurs Infosecurity.nl in de Jaarbeurs te Utrecht.

Schade

Het jaarlijks terugkerende onderzoek laat een dalende tendens zien voor wat betreft het aantal beveiligingsincidenten. In 2006 was 32% van de ondervraagden slachtoffer van incidenten; in 2003 lag dit percentage nog op zo’n 69% en vorig jaar werd ongeveer 35% getroffen.

Daartegenover staat dat de gemiddelde directe en indirecte schade per incident is toegenomen; de criminele organisaties die schuil gaan achter de beveiligingsincidenten beschikken over steeds meer financiële middelen en zijn steeds beter georganiseerd, en kunnen daarom, op grote schaal, grote schade berokkenen. Ook zorgwekkend is dat slechts 21 procent van de geïnterviewden

aangeeft te voldoen aan compliance wet- en regelgeving. Op basis hiervan kan sterk worden getwijfeld of organisaties eventuele incidenten en de gevolgen hiervan onderkennen.

Schijnzekerheid

“Het gaat niet meer alleen zoals vroeger om het platleggen van een website” zegt Jule Hintzbergen, werkzaam als adviseur op het gebied van informatiebeveiliging bij Capgemini. “Vandaag de dag gaat het meer en meer om financieel gewin, bijvoorbeeld door middel van phishing en zogenaamde *scams*, waarmee forse bedragen worden geïncasseerd zonder dat gedupeerden zich dat realiseren. Het gaat dan vaak niet om gigantische bedragen per transactie maar juist om grote hoeveelheden kleinere bedragen. Bedrijven en organisaties lijken niet in te spelen op nieuwe dreigingen, maar blijven acteren op onderkende risico’s van vroeger. Dit is absolute schijnzekerheid. Verder geeft het onderzoek aan dat er een verschil is tussen de werkelijk opgetreden incidenten en de perceptie van welke incidenten de meeste zorgen baren.”

Schieten met hagel

Medeonderzoeker Geert-Jan van de Ven vult aan: “Maar liefst de helft van de ondervraagden geeft aan geen risicoanalyse te hebben uitgevoerd om relevante dreigingen en noodzakelijke beveiligingsmaatregelen vast te kunnen stellen. Uiterst onverstandig, omdat zo geen goede set van samenhangende maatregelen kan worden bepaald. Alle genomen maatregelen zijn dan ‘best guesses’ en bieden geen enkele garantie”.

Dit beeld lijkt onderbouwd te worden door de feiten. De helft van de respondenten heeft het afgelopen jaar geen aandacht geschonken aan het beveiligingsbewustzijn van de medewerkers. Al geruime tijd wijzen diverse onderzoeken uit dat medewerkers in de organisatie de vatbaarheid voor bedreigingen vaak onbewust vergroten. Het is niet altijd wenselijk om veilig gedrag met technische middelen af te dwingen; het geniet daarom de voorkeur goede voorlichting te geven over het hoe en waarom van een veilige manier van werken, en de bedrijfsprocessen daarop af te stemmen.

Veel van de respondenten (64%) vindt het een verantwoordelijkheid van de overheid om vitale infrastructuren zoals internet te beveiligen. Omdat de behoefte aan beveiliging van die infrastructuur in sterke mate afhankelijk is van specifieke bedrijfsprocessen kan en mag een

manager deze verantwoordelijkheid absoluut niet negeren. Helaas moet worden geconstateerd dat dit wel gebeurt. Risicomanagement is van groot belang; de organisatie *moet* ‘in control’ zijn.

Over Capgemini Public Security

De Public Security-specialisten van Capgemini hebben de ervaring en expertise om, in samenwerking met de klant, te zorgen voor optimale beveiliging, zodat organisaties ‘in control’ komen - en blijven. De consultants van Capgemini zijn ingezet bij een veelheid aan opdrachten - van het leveren van interim security managers tot het begeleiden van uw organisatie in een compliance/certificering traject, en van ethical hacking tot de bestrijding van social engineering. Op technologisch gebied loopt Capgemini voorop bij het integreren van nieuwe ontwikkelingen, die het bijvoorbeeld mogelijk maken om snel identiteitanalyses uit te voeren.

Over Capgemini

Capgemini, een van de meest toonaangevende aanbieders van consulting-, technology- en outsourcingdiensten ter wereld, werkt op een unieke manier samen met zijn klanten. Deze werkwijze noemt Capgemini de “Collaborative Business Experience”. Door zich te richten op gezamenlijk succes en het behalen van aantoonbare toegevoegde waarde helpt Capgemini bedrijven bij het ontwikkelen van nieuwe groeistrategieën, het optimaal benutten van de mogelijkheden van technologie, en te groeien als gevolg van een krachtige samenwerking. Capgemini heeft wereldwijd ongeveer 61.000 medewerkers in dienst en realiseerde in 2005 een omzet van 6,954 miljard euro. Meer informatie over afzonderlijke disciplines, vestigingen en onderzoek is te vinden op www.nl.capgemini.com.

EINDE PERSBERICHT

Voor meer informatie:

Capgemini, Lucas Stassen, woordvoerder

Telefoon: 030 689 52 81, Mobiel: 06 417 25 315

E-mail: lucas.stassen@capgemini.com