

Bestrijding cybercrime schiet tekort

Doembeeld terrorisme denkbaar

Van onze binnenlandredactie

AMSTERDAM – Overheid en bedrijfsleven doen veel te weinig om computercriminaliteit te bestrijden. Driekwart van alle overheidsinstellingen heeft geen enkel noodplan in geval van cybercrime. In het bedrijfsleven is iets minder dan de helft in staat meteen maatregelen te treffen. Dit blijkt uit onderzoek van advies- en organisatiebureau Ernst & Young. Hierin staat dat cybercrime een onbeheersbaar probleem dreigt te worden. Overal ter wereld vragen deskundigen zich af of veilig internetten nog wel mogelijk is.

Criminaliteit via de computer internationaliseert en wordt al maar professioneler. Het doembeeld van een terroristische aanslag is zeker denkbaar, aldus de onderzoekers, die stellen dat de noodzaak om de ICT-infrastructuur volledig te beveiligen „al maar urgenter” wordt.

Voor de overheid is te weinig geïnteresseerd in de bestrijding van cybercrime. „Juist waar beveiliging het hardst nodig is, faalt het beleid”, aldus de onderzoekers, die refereren aan de onlangs gehackte OV-chipkaart. Door gebreken in de beveiliging lijkt een succesvolle invoering van die kaart nog mijlenver weg. Een ander voorbeeld is Engeland, waar vorig jaar oktober gevoelige informatie van 25 miljoen burgers door

een fout van de overheid zoek raakte.

„Ik zie iedere dag bij bedrijven dat de risico's hand over hand toenemen”, aldus Monique Otten van Ernst en Young. „De tijd om hier onverschillig over te kunnen zijn, is echt voorbij. We staan anders aan de vooravond van grote digitale narigheid. Iedereen moet wakker worden geschud. Dit is noodzaak willen we tijdig en adequaat kunnen reageren op digitale aanvallen die grote gevolgen hebben voor de samenleving.”

Uit het onderzoek blijkt ook dat slechts een kleine groep bedrijven aangifte doet van computercriminaliteit. Twee op de tien bedrijven ondernemen zelfs helemaal geen actie.

