

'Nederland niet voorbereid op internetcriminaliteit'

Van onze redactie economie

AMSTERDAM – Een groot deel van de Nederlandse bedrijven en overheidsinstellingen is niet goed voorbereid op *cybercrime*. De beveiliging van de ICT-infrastructuur is vaak onvoldoende en een noodplan ontbreekt bij meer dan de helft van de instanties. Dat zijn de belangrijkste conclusies uit de ICT Barometer, een onderzoek van accountant Ernst en Young.

„Het beeld van een terroristische digitale aanslag zoals je die in films ziet, is allang geen fictie meer”, licht onderzoeker Monique Otten toe. „Het doembeeld van zo'n massale aanslag is zeker denkbaar.”

Hoewel uit het onderzoek, dat is uitgevoerd onder 600 directeurs, managers en professionals, blijkt dat steeds minder bedrijven last hebben van virussen en computerinbraak, voelt Otten zich toch genoodzaakt om de noodklok te luiden.

„Het lijkt er inderdaad op dat het beter gaat, maar daar tegenover staat dat internetcriminelen zich steeds

verder professionaliseren”, legt ze uit. „Ik zie iedere dag bij bedrijven dat de risico's hand over hand toenemen. Er moet echt meer aandacht worden besteed aan beveiliging.”

Iets minder dan de helft van de bedrijven en slechts een kwart van de overheidsinstellingen beschikt over een noodplan voor als het kritische bedrijfsproces uitvalt. Als een bedrijf slachtoffer wordt van *cybercrime*-activiteiten wordt slechts in 6 procent van de gevallen aangifte gedaan.

Daarnaast blijkt dat 83 procent van de respondenten nauwelijks tot geen vertrouwen heeft in de bestrijding van *cybercrime* door politie en justitie. Projectleider *cybercrime* Henk Klap van de politie Noord- en Oost-Nederland erkent dat het oplossen en verwerken van aangiftes verbeterd kan worden. „Op dit moment hebben we 250 specialisten. Daarnaast gaan we de komende jaren 8500 rechercheurs bijscholen.”

Klap vindt dat bedrijven en individuen zelf ook een verantwoordelijkheid hebben. „Als de beveiliging niet op orde is dan helpen wij niet.”

