

'Cybercrimineel sluipt zo naar binnen bij overheid'

Van een onze verslaggevers
AMSTERDAM - Het Nederlandse bedrijfsleven heeft zich nog volstrekt onvoldoende gewapend tegen computermisdaad (cybercrime). Vooral de overheidsdiensten schieten ernstig tekort. Zo heeft driekwart van de Nederlandse overheidsorganisaties geen maatregelen genomen om cybercrime te verhinderen, een noodplan ontbreekt als het onverhoopt helemaal mis mocht gaan. Van de bedrijven heeft minder dan de helft een noodplan.

Dat blijkt uit de gisteren gepubliceerde ICT Barometer van advies- en accountantskantoor Ernst & Young. Inmiddels blijkt een achtste van alle bedrijven te maken te hebben met *phishing*, het aanbieden van valse websites om zo achter codewoorden van klanten te komen waarmee vervolgens wordt ingebroken of rekeningen worden leeggehaald.

„Als er niet snel wat gebeurt, is een digitale aanslag met terroristisch karakter niet meer denkbeeldig”, zegt onderzoekster Monique Otten van Ernst & Young. „Computerhackers worden steeds beter in het doorbreken van veiligheidsbarrières, de combinatie gebruikersnaam en wachtwoord is vaak makkelijk te omzeilen. Bedrijven moet



• Een digitale terreuraanslag door hackers is volgens Ernst & Young niet denkbeeldig.

FOTO: REINIER VAN WILLIGEN

zich standaard beter beveiligen.”

Uit het onderzoek blijkt verder dat bij de overheid 62% van de respondenten onvoldoende vertrouwen heeft in de beveiliging tegen cybercrime. In het bedrijfsleven is dat iets minder dan de helft. Van de ondervraagden heeft ruim 80% weinig vertrouwen in politie en justitie. Vaak wil men ook geen aangifte doen omdat het dan tot een openbare rechtszaak kan komen. Het bedrijf staat dan voor joker. De meeste bedrijven lossen daarom inbreuken op hun computersysteem intern op, twee op

de tien bedrijven ondernemen zelfs helemaal geen actie.

Volgens Henk Klap, projectleider cybercrime bij de politie in Noord- en Oost-Nederland, moet de politie de mogelijkheden voor aangifte verbeteren. Ook zou hij graag meer meldingen binnenkrijgen. „Het is goed om te weten wat er allemaal speelt”, stelt hij.

Van de 8500 rechercheurs zijn er nu 250 computerexperts. Het KLPD heeft een team van 30 hooggeschoolde 'cybercops'. Van die 8500 rechercheurs hebben er inmiddels 2000 een cursus computercriminaliteit gehad en dit wordt nog opgevoerd.

„Het is natuurlijk geen wonder dat het grootste deel van de cybercrime die we bestrijden op het financiële vlak is.” Klap rekent ook fraude met banken tankpassen, waarbij de gegevens worden gekopieerd en de pincode wordt ontfoetseld, tot computermisdaad. Het wordt echter een andere zaak als mensen via internet kopen en ondeugdelijke zaken krijgen geleverd, dat is 'gewone oplichting'.

