

CYBERCRIME Ernst & Young constateert gebrek aan voorbereiding en aan zelfvertrouwen 'Nederland wapent zich slecht'

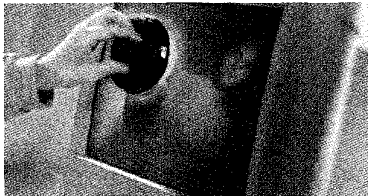
■ Risico's worden onderschat, vooral door overheid

De Nederlandse overheid en in mindere mate het bedrijfsleven onderschatten de risico's van cybercriminaliteit. Een digitale aanslag heeft daardoor goede kans van slagen. Dat blijkt uit de achtste ICT Barometer van Ernst & Young, die deze week is gepubliceerd. Vooral de overheid bekommert zich te weinig om cybercrime, blijkt uit de peiling onder ruim 600 managers en leidinggevenden bij de overheid en bedrijven. Driekwart van alle overheidsinstellingen en ruim de helft van de bedrijven heeft geen noodplan voor het geval een kritisch bedrijfsproces uitvalt of niet meer goed werkt. Gemiddeld over alle organisaties is dat 59 procent. En dat terwijl de bedrijfsprocessen in ruim driekwart van alle organisaties (zeer) sterk afhankelijk zijn van ICT. In bedrijven met meer dan 500 werknemers is dat zelfs 85 procent. Het vertrouwen in de eigen organisatie op het punt van bescherming tegen cybercrime is in veel gevallen zoek. Binnen de overheid zegt 62 procent onvoldoende fiducia te hebben in de beveiliging. Iets beter is het gesteld in het bedrijfsleven, waar ruim de helft erop rekent dat de werkgever voldoende maatregelen heeft getroffen.

EDP-auditor Monique Otten spreekt van 'falend beleid'. Zij zegt dagelijks te constateren dat de risico's bij bedrijven hand over hand toenemen en voorspelt 'grote digitale narigheid' als alle betrokkenen niet wakker worden geschud.

Bedrijven doen maar zelden aangifte

bij politie of justitie wanneer ze met internetcriminelen zijn geconfronteerd. Ze vinden het probleem niet belangrijk genoeg (60 procent) of lossen het in eigen beheer op (45 procent). Een kleine minderheid van 11 procent zegt geen vertrouwen te hebben dat politie en justitie kunnen helpen. Ernst & Young vroeg echter door en wilde ook weten of bedrijven in het algemeen vertrouwen hebben in politie en justitie voor de bestrijding van cybercrime. Niet of niet zoveel, antwoordt



dan 83 procent. De onderzoekers zien hierin 'mede' de verklaring voor het geringe aantal aangiften, terwijl dat eerder als factor van ondergeschikt belang naar voren kwam.

Ondanks de alarmerende uitspraken van Ernst & Young kan uit dezelfde peiling worden opgemaakt dat het in de praktijk juist de goede kant op gaat. Slechts 0,4 procent werd getroffen door computerinbraak en 3 procent door een computervirus. Dat is aanzienlijk minder dan in het vorige onderzoek van september 2006, toen cyberaanvallen 1 procent en virussen 7 procent van de bedrijven teisterden. Om nog maar te zwijgen van september 2004, toen deze scores nog op 5 en 28 procent lagen. "Het lijkt erop dat de investeringen in ICT-beveiliging hun vruchten afwerpen", aldus de onderzoekers.

Gemeten over de laatste twaalf maanden

had 5 procent weleens te maken met computerinbraak, 7 procent met digitale spionage en 12 procent met het hengelen naar vertrouwelijke gegevens (phishing). Een kwart moest zich teweerstellen tegen virussen. Maar de overlast ervan is de laatste jaren duidelijk afgenomen, erkent Ernst & Young. Stabiël op 32 procent is de hinder die aanbieders van illegale producten en diensten, zoals internetcasino's en medische preparaten, veroorzaken. Daarvan is het nog maar de vraag of organisaties zich er gericht tegen zouden moeten beveiligen, anders dan door het installeren van bijvoorbeeld een spamfilter. Gevraagd naar de risico's van nieuwe technologieën zeggen de ondervraagden zich het meest (31 procent) zorgen te maken over verwijderbare opslagmedia als USB-sticks. Medewerkers die vanuit huis inloggen en draadloze netwerken ziet men als bijna net zo riskant. Veel minder vrees (13 procent) bestaat er voor webapplicaties.

Geert Kelfkens / g.kelfkens@sdu.nl

Vooraf ontbreken van noodplannen baart zorgen

