

een onderzoek van het CBS in oktober 2003 blijkt dat 52% van alle brandmeldingen bij brandcentrales false positives zijn (loos alarm). Kortom, detectie blijft een moeilijk probleem. De meeste bedrijven en instellingen doen inmiddels wat aan inbraakpreventie. Firewalls zijn de afgelopen tien jaar veranderd van moeilijk te installeren software tot plug-and-play apparatuur (hetgeen niet wegneemt dat een goede configuratie van een firewall nog steeds handwerk is en zorgvuldig door een kundig iemand gedaan moet worden). Ook besturings-systemen zijn de afgelopen tien jaar veel veiliger geworden, voornamelijk als reactie op het feit dat de dreiging van inbraak de afgelopen tien jaar zo is gestegen.

Detectie in de vorm van Intrusion Detection Systems staat momenteel nog steeds in de belangstelling, maar zoals gezegd is het inregelen van deze systemen voor veel instellingen een moeilijk te overwinnen obstakel. Er is op dit gebied dus nog wat te leren. Nog meer

## “Heel vaak wordt vergeten om zo'n calamiteitenplan op te stellen”

te leren is er op het gebied van reactie op een computerinbraak.

### Calamiteitenplan

Als er brand uitbreekt wordt normaal gesproken meteen het calamiteitenplan erbij gehaald. Hierin staat bijvoorbeeld wie er geïnformeerd moet worden en welke andere acties genomen moeten worden. Er zijn plattegronden in te vinden van de gebouwen, telefoonnummers van mensen, etc. Een calamiteitenplan biedt alle informatie die snel nodig is als er een calamiteit is. In het geval van een gedetecteerde computerinbraak horen de te nemen acties ook in een calamiteitenplan te staan. Het heet dan alleen geen calamiteitenplan maar een security policy. Heel vaak wordt vergeten om zo'n calamiteitenplan op te stellen. Als er

dan een inbraak wordt gedetecteerd is niet meteen duidelijk wat eraan gedaan moet worden. Laten we de inbreker nog op het systeem en proberen we te achterhalen waar deze vandaan komt? Of proberen we hem meteen van het systeem te weren? Moeten gebruikers hun wachtwoord wijzigen? Gaan we het systeem van een oude back-up terughalen (van wanneer?) of gaan we het systeem van de originele installatiemedia opnieuw installeren? Lichten we de pers wel of niet in? Ligt er al een persbericht klaar?

Net als bij een brand kost het oplossen van een inbraak tijd en moeite. Het is dan van grote waarde om vooraf al duidelijk te hebben welke stappen moeten worden genomen, zodat de mensen die het probleem oplossen (de brand blussen, de systemen opnieuw inrichten) zo min mogelijk overlast hebben. Ik raad daarom iedereen aan om naast preventie en detectie vooral ook vooraf aandacht te besteden aan wat er aan reactie moet plaatsvinden na een inbraak, en dit vast te leggen in de security policy. Want een inbraak zal, jammer genoeg, vroeger of later een keer plaatsvinden. •

Walter Belgers

