

## Resultaten ethical hack 2004

**Op alle zes scholen was op gebied van beveiliging in principe wel wat aan te merken. Bij drie scholen was sprake van een situatie waar kwaadwillende personen te eenvoudig ongeautoriseerde toegang van binnenuit en van buitenaf konden verkrijgen.**

Hieronder de bevindingen.

- **Draadloze netwerken** Er zijn op twee locaties draadloze netwerken aangetroffen. In beide gevallen waren de netwerken onbeveiligd en van buiten het schoolterrein benaderbaar. Het was mogelijk draadloos de schoolsystemen te benaderen, via het draadloze netwerk te internetten en het netwerkverkeer af te luisteren. Extra opvallend was dat op één van de locaties de beveiliging verder goed op orde was; dit toont aan dat beveiliging net zo goed is als de zwakste schakel.
- **Wachtwoorden** Er werden enkele accounts aangetroffen zonder wachtwoord of met een standaard wachtwoord.
- **Hardware** Steeds meer apparatuur is 'netwerkgeschikt', heeft daarvoor een eigen 'naam'/ip-adres, en is daardoor potentieel benaderbaar vanaf internet. Tijdens de test werden ondermeer printers, cdrom-servers, printerswitches, switches, een videosever en een kopieermachine aangetroffen die een mogelijke toegang bieden voor hackers.
- **Updates** Op diverse scholen was toegang tot systemen mogelijk doordat niet de laatste versie van de software was toegepast.
- **Logbestanden** Het vermoeden bestaat dat de meeste scholen niet regelmatig in logbestanden kijken. Logbestanden geven ondermeer zicht op 'wie er aan de voordeur morrelt'.
- **Rechten** Rechten op systemen worden niet altijd zorgvuldig toegekend en beheerd.
- **Internet prikborden en nieuwsgroepen** In een aantal gevallen werden op internet berichten van systeembeheerders aangetroffen waarin ze bijvoorbeeld om hulp bij een probleem verzoeken. Op zich niet erg, maar het bespreken van problemen met systemen moet met de nodige omzichtigheid gebeuren aangezien dit een aangrijpingspunt vormt voor een aanval. Is iemand bekend als beheerder dan is het bijvoorbeeld extra interessant het wachtwoord van deze persoon proberen te kraken. Wordt publiekelijk besproken welke soft- of hardware men gebruikt, dan kan een potentiële hacker met die informatie nagaan welke kwetsbaarheden te misbruiken zijn.
- **Goedkoop is duurkoop?** Op een van de scholen werd een Alcatel Speedtouch 510 aangetroffen. Dit modem staat volgens de experts die de test uitvoerden niet bekend als heel veilig.
- **Websites** De meeste websites waren ondergebracht bij een provider en vielen zo buiten de test. Belangrijk is te beseffen dat scholen die hun website hosten op eigen machines, extra aandacht moeten besteden aan beveiliging. Host u de website zelf, dan loopt u een groter risico.

Sommige mensen vragen zich af waarom je een school goed moet beveiligen. [Hier vindt u wat argumenten.](#)