

# ‘Eeuwige strijd’

**Onlangs lukte het leerlingen van het Eddy Hillesum Lyceum in Deventer om de mailbox van een docent te ‘hacken’ en er toetsopgaven uit te vissen. Regelmatig merken scholen dat leerlingen hun systeem proberen te hacken. Wat kun je er als school tegen ondernemen?**

Tekst: Mirjam Janssen

Beeld: iStock

Uit een ‘ethical hack’ – een soort proefinbraak – in 2007 door Kennisnet bleek dat het systeem van veel scholen niet waterdicht is. Het netwerk van de proefscholen bleek van buitenaf niet te kraken, maar van binnenuit bleken er wel mogelijkheden te zijn. Zo konden medewerkers van de scholen wachtwoorden verspelen doordat leerlingen over hun schouders meekeken bij het inloggen of doordat ze hun computer niet goed afsloten bij het verlaten van het lokaal. Ook voor de hand liggende wachtwoorden waren een risico. De meeste scholen zijn zich bewust van het gevaar en nemen hun maatregelen.

**Hackertjes** Lex Pronk, hoofd ict van het Bonaventuracollege in Leiden, heeft te maken met ‘2.700 hackertjes’ zoals hij zelf zegt. ‘Daar kun je heel erg tegen vechten, maar wij hebben een vrij open systeem. Hoe meer je dichttimert, hoe meer ze gaan proberen. En uiteindelijk kunnen ze toch nergens bij. Het leerlingen- en het administratieve systeem zijn gescheiden. Mochten ze proberen iets uit te halen dan hebben wij dat zo door. Wij monitoren de hele dag het gebruik van de computers, als iemand iets probeert, sta ik even later achter hem. Een keer zijn de leerlingen erin geslaagd het systeem van de school te kraken, ze hadden er een spelletjes-server van gemaakt. Daar zijn ze met een waarschuwing vanaf gekomen.’

**Rechten** Erik Steenhardt, systeembeheerder van scholengemeenschap Echnaton in Almere merkt weinig van pogingen tot hacken. ‘De leerlingen komen er bij ons niet doorheen. Ze kunnen niet in Dos, niet op de C-schijf en ze mogen geen bestanden wijzigen. Ze kunnen alleen in Word werken en

beperkt surfen op internet. De docenten werken op een apart systeem en hebben andere rechten. Mocht een leraar per ongeluk zijn wachtwoord verspelen en hij merkt het tijdig, dan kunnen we zijn account meteen blokkeren. Maar als we daarmee te laat zijn, is de schade toch beperkt. Want de leraren kunnen alleen in hun eigen deel van het systeem en nooit in dat van de hele school.’

**Token** Adriaan Noteboom, hoofd ict aan het Driestar College in Gouda, maakte een paar jaar geleden kennis

met de inventiviteit van leerlingen. Drie vwo’ers wisten door hacken een aantal wachtwoorden van docenten te achterhalen. ‘We zijn er achter gekomen doordat mediatheekmedewerkers zagen dat docenten waren ingelogd op computers van de leerlingen, en dat kan niet. De leerlingen hebben niets veranderd, wel hadden ze een repetitie eraf gehaald. De leerlingen zijn van school gestuurd. Inmiddels is onze beveiliging een stuk verbeterd. Naast een vast wachtwoord hebben docenten bij ons nu ook een ‘token’, een apparaat dat je bij de com-



## PRAKTIJK

puter moet houden en dat een eenmalig wachtwoord genereert. Dat maakt het veel moeilijker het systeem binnen te komen. Toch hebben we nog steeds een relatief open systeem. Het blijft zoeken naar een evenwicht. Je wilt dat je systeem veilig is, maar tegelijk moeten docenten ook een keer zelf een programma kunnen uitproberen.’

### Georganiseerde aanval

Louis Troussel, hoofd ict van het Bonhoeffer College in Enschede, maakt regelmatig mee dat leerlingen een aanval uitvoeren op het schoolsysteem. ‘Het blijft een eeuwige strijd. Ik heb de indruk dat leerlingen binnen Nederland informatie uitwisselen. Bij ons legden ze bijvoorbeeld het hele computernetwerk plat door de kabel van een computer verkeerd aan te sluiten. In dezelfde periode gebeurde dat ook op andere plaatsen in het land. Er zit een soort circuit achter.’

Troussel heeft de indruk dat niet ieder type leerling even sterk tot hacken is geneigd. ‘Onze school biedt opleidingen aan van vmbo tot vwo. Op vmbo zorg & welzijn hebben we nooit problemen. Bij andere vmbo-richtingen komt het voor dat ze mechanische onderdelen uit de computer proberen te halen, maar meer ook niet. Je moet vooral goed op de vwo’ers letten. Die leerlingen zijn heel inventief. Gelukkig hebben we twee medewerkers die zelf ook veel trucs kennen, zo ontwikkelen we onze tegenzetten. We hebben gescheiden netwerken voor de leerlingen en voor de administratie en we houden de elektronische leeromgeving goed in de gaten. Juist die is gevoelig. Maar helemaal te voorkomen is hacken nooit. Als het gebeurt, is het soms een kwestie van slim reageren. Dan straffen we de leerling niet, maar mag hij vertellen wat hij heeft gedaan. Soms zijn ze daar zo trots op dat ze alles loslaten. En daar maken wij dan weer gebruik van.’

### ZO BEPERK JE DE RISICO'S

- Zorg voor een fysieke scheiding tussen het leerlingen- en het administratieve gedeelte
- Wees voorzichtig met gebruik van administratieve programma's in de klas
- Geef leerlingen geen recht op het installeren van programma's
- Kijk uit voor het onversleuteld uitwisselen van gegevens via internet

*‘Je moet vooral goed op de vwo’ers letten’*