Speech net zo vlammend als Max Havelaar en win een reis naar Afrika

▶Zin: pagina 20 en 21

nrc·next

donderdag 8 september 2011
www.nrcnext.nl
prijs 1,30 euro

Uitgave van NRC Handelsblad Jaargang 6 No.125

Digitaal knutseren

De aanval op DigiNotar was kinderspel. De Nederlandse hackerswereld is niet onder de indruk. ▶pagina 4 en 5

Foto Thomas Donker

Internationaal
Niemand weet waar Gaddafi is

Gaddafi is spoorloos. Hij zat waarschijnlijk niet in het konvooi naar Niger, niet in Bani Walid, niet in een gat in de grond. Zijn onvindbaarheid zorgt voor instabiliteit. Niger, Burkina Faso en Tsjaad hebben een belangenconflict. Gaddafi paaide hen, maar ze voelen internationale druk.

▶pagina 6 en 7

Nederland
Aanklacht tegen Zorreguieta

Tegen de vader van prinses Máxima, Jorge Zorreguieta, is aangifte gedaan wegens het laten verdwijnen van mensen tijdens de Videla-dictatuur in Argentinië. Justitie zou door nieuwe Nederlandse wetgeving verplicht zijn de nu 83-jarige Zorreguieta te arresteren en te berechten.

▶pagina 8 en 9

Economie
Saab vraagt surseance aan

De noodlijdende autofabrikant Saab heeft gisteren uitstel van betaling aangevraagd. Het einde van Saab is nu echt nabij. Victor Muller heeft het bedrijf in anderhalf jaar niet uit het slop weten te trekken. Hij legde er de laatste anderhalf jaar 13.000 euro op toe per geproduceerde auto.

▶pagina 12 en 13

Sport
IJshockeyteam dood bij ramp

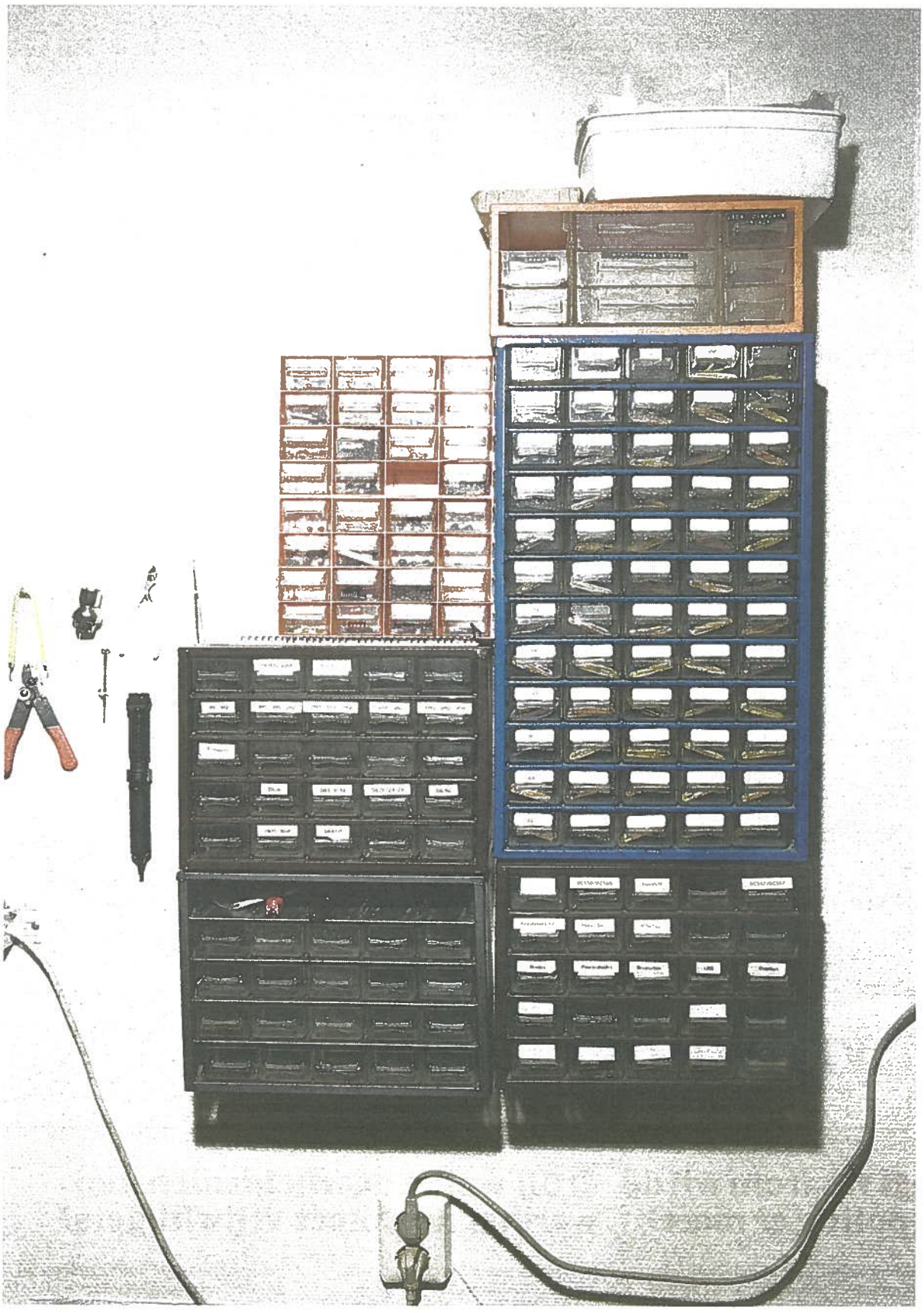
In het westen van Rusland zijn bij een vliegtuigongeluk 43 spelers en stafleden van een Russisch ijshockeyteam om het leven gekomen. Twee mensen overleefden het. In Rusland, waar ijshockey de nationale sport is, is geschokt gereageerd. De media spreken van een nationale tragedie.

▶pagina 16 en 17

8 710114 600035 43611

Handige jongens, die hackers

Spelletje soms best serieus



▸ Het Nederlandse DigiNotar werd waarschijnlijk gekraakt door Iraniërs. Hun beveiliging bleek een lachertje.

▸ Maar wat doen Nederlandse hackers zelf?

Door CAROLA HOUTEKAMER

DEN HAAG. Onzichtbaar, ongrijpbaar en oppermachtig. Het imago van hackers is dramatisch en zelfs angstaanjagend. De ene keer zijn het cyberanarchisten die naar believen wraak nemen op overheden en bedrijven, zoals het losse collectief Anonymous („*We are Legion. We do not forgive. We do not forget. Expect us.*"). Nu weer Iraniërs die een Nederlands beveiligingsbedrijf kraken om dissidenten te bespioneren en *en passant* de Nederlandse overheid in verlegenheid brengen. En je had al die handige jongens die met gekraakte ov-kaarten gratis het land doorkruisen.

Wat vinden de hackers zelf van dat imago? De Iraniër had „niet gruwelijk veel skills" nodig om DigiNotar te kraken, bleek uit onderzoek achteraf. Maar hij zou meer van dat soort bedrijven hebben gehackt, en dat is wel knap, vindt Mark Janssen (ook bekend als 'Foobar' – hackers doen graag aan *nicknames*). DigiNotar is het gesprek van de week in de Haagse hackerswerkplaats Revspace, waar Janssen voorzitter van is. „De discussie die nu ontstaat is nuttig. Zijn certificaten wel veilig?"

Maar het hackwerk dat doorgaans de aandacht trekt is kinderspel, vindt 'Stitch', het cafeïnerijke hackersdrankje Club-Mate in de hand. Welke Nederlandse hacker kent nou niet iemand die ooit een keertje in naam van Anonymous, Lulzsec, Antisec, of AntisecNL heeft meegeholpen met zo'n beruchte 'DDoS-aanval'.

Stitch laat even zien hoe dat gaat. Je downloadt het programmaatje LOIC (paar minuten), vult de naam van de site in (10 seconden), drukt twee keer op een knop en daar ga je. Als je dat met een paar honderd man tegelijk doet, gaat de site plat. Dat is geen hacken, vindt hij. Dat is digitaal graffiti spuiten.

Wat doen ze dan wel?

Van alles.

Je hebt de beveiligingsexpert die legitiem voor z'n werk op systemen inbreekt. Je hebt de elektrotechnicus die met z'n soldeerbout apparaten ombouwt. Je hebt de *lockpicker* met z'n lopersetjes, de *coder* die aan software sleutelt en de *social engineer* die met bluf wachtwoorden en rekeningnummers lospeutert bij bedrijven.

De groep van zo'n paar duizend man (voor wie hacken ruim definieert) is overwegend man en blank, en hun motieven lopen uiteen. De maatschappelijk geëngageerde hacker wil de kwetsbaarheid van publieke systemen als het elektronisch paspoort en de stemcomputer aantonen, of helpen internetcensuur in dictaturen te omzeilen. De *filesharer* hackt andermans servers om voor de lol films en muziek te verspreiden. De uitvreter hackt omdat hij geen zin heeft te betalen voor treinkaartjes, of steelt waardevolle gegevens (dat heet dan cybercrime).

En sommige hackers willen gewoon dingen slopen. Uit protest, of omdat het kan.

De Iraanse 'überhacker' spreekt

Hij wil *Anonymous* en andere hackers wel workshops geven. Want hij heeft de skills van 1.000 hackers bij elkaar. **Dat pocht de 'Comodohacker', die de hack bij DigiNotar heeft opgeëist.** De Iraniër zegt dat hij zich al zes jaar bezighoudt met cryptografie. Je kunt hem per mail interviewen. „WOOOOORLLLLDDD! Wait for me, you have so much more SHOCKINGS to see from me! From a person who came to this world just 21 years ago! JUST WAIT!"

Is het hem echt? Het zou goed kunnen, zeggen beveiligingsbedrijven. Omdat hij in maart een vergelijkbare hack bij het certificaatleverancier Comodo opeiste (vandaar zijn naam). **Hij levert meerdere technische bewijzen aan.** Zoals de standaard rekenmachine uit Windows, maar dan ondertekend met een vals Google-certificaat. Ook verklapt hij wat het hoofdwachtwoord van de productiedomeinadministrator van DigiNotar was: Pr0d@dm1n. Als dat waar is, schamperen IT'ers op Twitter, is het helemaal terecht dat DigiNotar met de grond gelijk wordt gemaakt.

Zelfverklaard motief van de Comodohacker: **wraak voor Srebrenica, waar Nederland „achtduizend moslims liet vermoorden"**. „You need to study more about Srebrenica, study more about how Serbian soldiers was wild animal, how they was killing innocent people of Bosnia, it was 16 years ago, but nothing is changed, today see how Israel is killing Palestinian children", schrijft hij. Maar ook de ontwikkelaars van het Stuxnet-virus („mijn hack was veel gecompliceerder") wil hij helpen. Dat virus bracht eerder dit jaar schade toe aan het nucleaire programma van Iran. En dat zou betekenen dat hij **waarschijnlijk niet in dienst is van de Iraanse overheid.**

Thalia Verkade

De mecanoknutselclub

Hacken is, strikt genomen, het ene ombouwen om het voor het andere te gebruiken. Die definitie hanteren ze in ieder geval in hackerspace Hack42 in Arnhem. Een groep van zo'n dertig man heeft zijn intrek genomen in een leegstaand gebouw van de Sociale Dienst. De ruimtes zijn volgestouwd met computers, draden, oude elektronica, printers, camera's, naaimachines, boormachines en soldeerbouten. Links een oude telex die op Twitter is aangesloten, rechts een snijplotter, op de wc blacklight. Een schakelaar bij de deur post automatisch op de site of de ruimte open is of dicht.

Arnhemse hackers houden van knutselen, zoveel is duidelijk. Eén is er bezig met een vogelhuisje van oude moederborden, een ander heeft een muizenval gemaakt die pingpongballen lanceert. Er zijn plannen om een eigen lasercutter en een 3D-printer te bouwen. Hacker 'Stoneshop': „Dit is een Mecanoclub voor grote mensen." Vanavond krijgen de aanwezigen de opdracht om iets nieuws te maken van een wekkertje en een knijpkat.

Netwerkbeheerder Mendel Mobach (BugBlue) verbouwt zijn knijpkat tot een energiezuinige taser. Mobach viste ooit bankrekeningnummers uit de ov-fietssite. Hij weet wel hoe hij botnets – op afstand bestuurbare netwerken van geïnfecteerde computers – kan aanleggen, sites kan infiltreren en beveiligingssystemen kan omzeilen. Net als veel andere bezoekers. Maar om daarmee nou in het nieuws te komen? Nee. Wat haalt het uit? Creatief sleutelen is leuker. Het is al moeilijk om binnen je bedrijf iets aan te kaarten, zegt iemand die bij de Belastingdienst werkt. „Vind je een lek, het boeit ze niet."

Een handjevol activisten

Kijk naar internetjournalist Brenno de Winter, zeggen de Arnhemse hackers. De Winter is regelmatig bezoeker van Hack42 en reisde vorig jaar wekenlang op een gekraakte ov-chipkaart, ter demonstratie. Andere journalisten en politici volgden. „En dan gebeurt er verder niks." Sterker nog, Trans Link Systems deed aangifte en het OM spande een rechtszaak tegen De Winter aan. Maar aan de ov-kaart veranderde niets.

De freelance journalist vindt de aanklacht tegen hem onbegrijpelijk, zegt hij. „Het OM ziet dit als georganiseerde misdaad. Ze maken geen onderscheid tussen cybercrime en het aantonen dat een systeem zwak is."

En de ov-chipkaart ís een zwak beveiligd systeem. Op een terrasje in Utrecht, een paar dagen eerder, trekken drie hackers tegelijkertijd een ov-chipkaartlezer uit hun zak. Binnen een paar minuten zijn de reisgegevens van de verslaggever uitgelezen. Saldo opladen? Ja, kan ook. Maar doen ze niet. Ze hacken niet om gratis te reizen, zeggen ze. Het gaat om het punt.

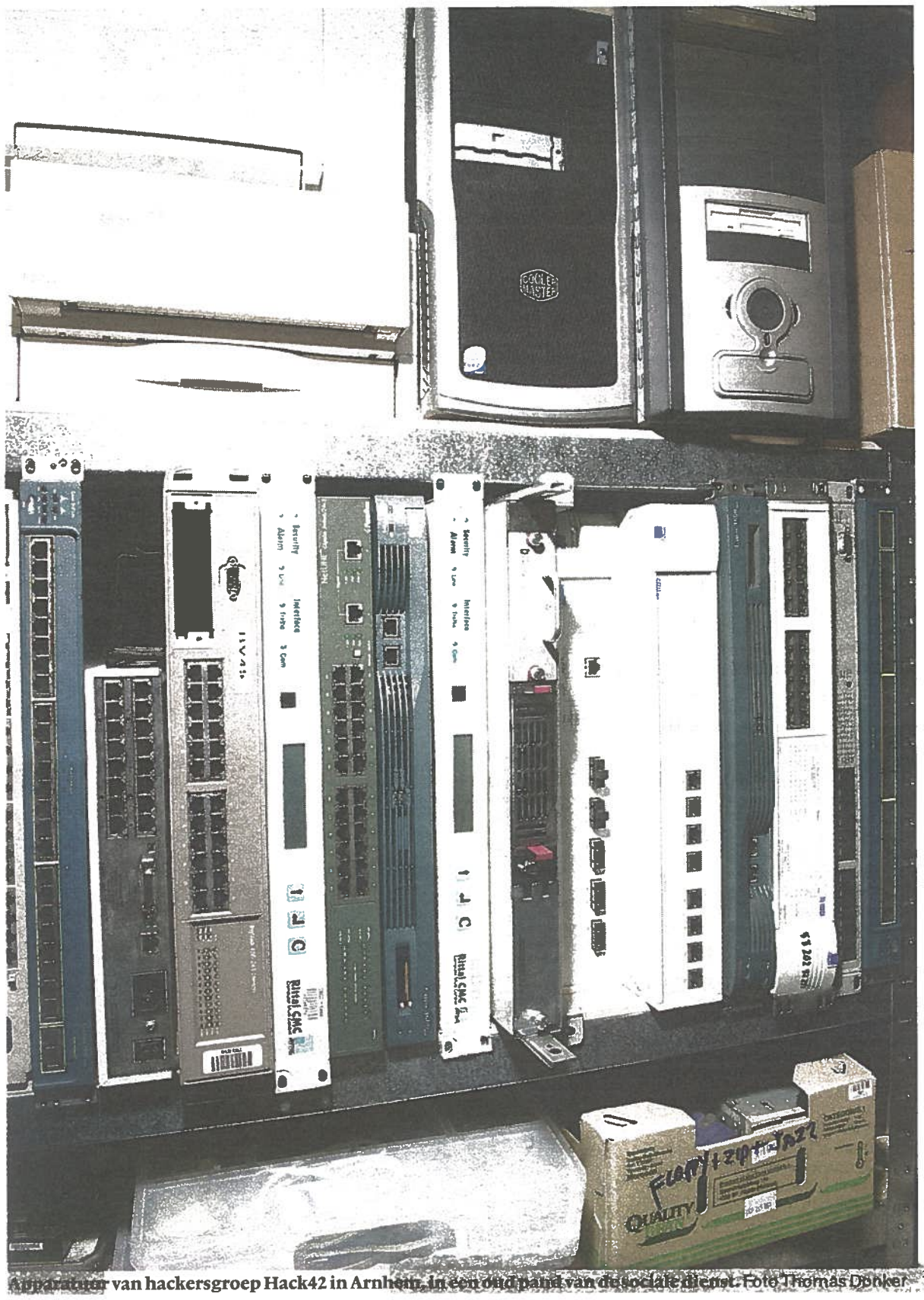
De Winter vindt het wel belangrijk om dat punt rond te blijven bazuinen. Werkt een systeem niet goed? Dan moet dat bekend worden. En verbeterd. Je ziet het nu ook weer met de zwakke beveiliging van overheidssites met de certificaten van het lekke Diginotar. Daar werd overigens uiteindelijk wel ingegrepen.

Zoals De Winter zijn er nog een paar activisten. Oprichter van XS4All Rop Gonggrijp liet Nederland weer met een rood potloodje stemmen en zet zich in voor WikiLeaks. De vakgroep Digital Security in Nijmegen kraakte de ov-chip en werkt aan betere open source-varianten. Jurre van Bergen (Dr Whax) maakt zich druk over de veiligheid van overheidssites.

Maar heel veel activisten zijn er niet, zegt hacker/beveiligingsexpert Jeroen van Beek in een cafeetje in Amsterdam. Het lukte Van Beek om de chip in het elektronisch paspoort te kopiëren en gewijzigde gegevens op een chip te zetten die zich voordoet als paspoortchip. Hij kan sommige carkits afluisteren en beelden op beveiligingscamera's onderscheppen. En hij harkt met zelfgeschreven software belastingaangiften en paspoortkopieën binnen die mensen per ongeluk delen via peer-to-peer-netwerken. Gewoon om te laten zien hoe makkelijk identiteitsfraude is.

Van Beek voelt geen diepe behoefte om misstanden aan de kaak te stellen. „Ik wil weten: wat kan de techniek?" Hij heeft, net als veel andere hackers, een baan als beveiligingsconsultant. Dat doet hij tegen commerciële tarieven, en liever voor bedrijven dan voor de overheid. „Die hobbelt altijd achter de feiten aan." Bedrijven nemen beveiliging veel serieuzer, zegt hij, om problemen voor te zijn en te voorkomen dat klanten weglopen na het zoveelste lek.

Waarom dan die paspoorthack? „Uit nieuwsgierigheid."



Apparatuur van hackersgroep Hack42 in Arnhem, in een oud pand van de sociale dienst. Foto Thomas Dokker

Chantage? Mwoah

Beveiligingsconsultant Barry van Kampen (Fish_) weet nog wel hoe op een ochtend „een Oostblokker" aan zijn deur stond om te vragen of hij interesse had in wat lucratief cyberwerk. „Toen werd ik wel bang, ja."

Aan hacken kan je goed geld verdienen, legt Van Kampen uit bij een biertje in Utrecht. Je kunt bijvoorbeeld een lek dat je in een systeem hebt gevonden verkopen. Aan het getroffen bedrijf, aan een tussenpersoon, of op de zwarte internetmarkt. En dan komt cybercrime dichtbij.

Van Kampen kent wel mensen die ongevraagd lekken opsporen en die kennis verkopen aan de bedrijven. Betalen ze niet, dan zetten ze het lek online. Chantage? Mwoah. Als er twee wielen van je auto vallen, wil je toch ook dat de fabrikant iets onderneemt?

Maar de stap naar echte cybercrime is in Nederland nog best groot, zegt Van Kampen.

Sommige hackers vertellen dat ze wel eens zijn gevraagd om spionagesoftware te installeren, of om hardware te slopen. Maar je denkt in Nederland wel drie keer na voordat je daar ja op zegt. In armere landen is het een stuk makkelijker om handige jongens over te halen tot misdaad. Nigel Brik (Zkyp), net als Van Kampen lid van de Utrechtste hackersgroep Randomdata: „Je bent arm, ontevreden en je hebt te veel hersenen. Wat doe je?"

Cybercrime en hacken ligt ook voor Justitie dicht bij elkaar. Zelfs als je niks verdient kun je vervolgd worden.

Twee weken geleden legde de rechtbank van Rotterdam drie maanden voorwaardelijke celstraf op aan de Amsterdamse student Rickey Gevers en vier anderen, voor 'deelname aan een criminele hackersorganisatie'. De vijf kraakten een paar jaar lang de systemen van de universiteiten van Michigan en Kaiserslautern om illegaal films, muziek en software te delen. In 2008 werden ze gepakt.

Hij hackte destijds veel computers, mailt Gevers, omdat hij graag digitaal rechercheur wil worden. Door te hacken leerde hij hoe systemen in elkaar zitten en hoe andere hackers te werk gaan. „Filesharen was een bijproduct."

Hij heeft zijn lesje wel geleerd, zegt Gevers. „Ik was nog jong." Hij deed z'n meeste hacks tussen z'n zestiende en z'n negentiende, zegt hij. Dan „is het een kick wanneer je een volwassen systeembeheerder met praktijkervaring te slim af weet te zijn."

Gevers vindt dat het OM in zijn geval wel begrip heeft getoond voor het feit dat het een uit de hand gelopen project was waar ze geen geld aan verdienden.

Justitie zoekt nog naar de juiste strafmaat voor ongeoorloofd pubergedrag. Wat leg je bijvoorbeeld een zestienjarige jongen op die meehelpt met het platleggen van de site (niet het betaalverkeer) van Mastercard, als wraak op de Wikileaksboycott? Is het cybercrime? Hoe erg is dat?

De puber die een half jaar geleden van z'n bed werd gelicht en twee weken vastzat, liep regelmatig rond in de Haagse hackerspace. De aanhouding leidde bij Revspace tot felle discussies over wat kan en wat niet kan. Betaald internet omzeilen in een hotel? Een rainbowtabelletje draaien om achter een wachtwoord te komen? Demonstreren door een site plat te leggen? De meningen verschillen. Op de vaste vergaderavond gaat de discussie verder.

„Die Mastercard-actie? Kan ik wel sympathie voor opbrengen."

„Als je op die manier wraak neemt telt enkel het recht van de sterkste."

„Nou, dat is toch gewoon evolutie?"

„Soms is het goed om je te verzetten."

„Organiseer dan een demonstratie in het echt, dat kost nog moeite. DDoS-sen is zo makkelijk, dat kan iedereen."