

Gratis snoep en 24 uur toegang

Elke dag maken duizenden mensen gebruik van het draadloze netwerk en andere digitale systemen die hen toegang geven tot de gebouwen, de koffieautomaat en het kopieerapparaat. Maar hoe veilig is die digitale VU eigenlijk?

DOOR WELMOED VISSER
ILLUSTRATIE BEREND VONK



Laten we dit verontrustende verhaal beginnen met een geruststelling: op de VU kun je veilig internetten. Niemand kan meekijken als je een betaling doet op internet, of chat met je nieuwe lief. De draadloze verbinding, waarmee je inlogt met je VUnet-ID of als gast, zit sinds een paar jaar redelijk dicht. Het contact tussen het netwerk en jouw laptop, telefoon of iPad verloopt versleuteld en volgens informaticastudent en hackingexpert Youri van der Zwart kost het jaren om deze sleutels te kraken. Te lang dus om er als kwaadwillige hacker iets mee te kunnen. In tegenstelling tot veel andere openbare wifi-netwerken, zoals dat van de NS, is de wifi op de VU veilig. Internetbankieren, appen en chatten kun je dus rustig doen op de VU. "Tenzij er een lek zit in de apps, of programma's die je gebruikt", vult Van der Zwart aan. "Maar dat ligt dan niet aan de VU."

Een heel ander verhaal zijn de pasjes voor medewerkers en studenten. Met die pasjes kom je gebouwen binnen, kun je

kopietjes maken en je fiets in de kelder stallen. En sinds anderhalf jaar zijn deze pasjes ook te gebruiken als betaalmiddel: bij een oplaadpunt zet je er geld op met je pinpas. Vervolgens kun je ze gebruiken bij de snoepautomaten en (als student) om je koffie en kopietjes te betalen. Het zijn zelfs de enige pasjes die de automaten en kopieerapparaten accepteren. Belangrijk dus dat die veilig zijn en dat ze alleen werken als je er inderdaad geld op hebt gezet. En dat is dus niet het geval.

Winegums

“Welke snoepjes zullen we vandaag eens nemen?” Informaticastudent en hacker Bram heeft zijn polsen vol hangen met bandjes van hackersconferenties, zoals anderen hun toegangsbandjes van Lowlands blijven dragen. Hij steekt een van de ov-chipkaarten die hij in een stapeltje in zijn zak draagt in een snoepautomaat op de campus en kiest een zak roze cadillacs. Het saldo van de kaart gaat van 5,01 naar 3,11 euro. Hij heeft dus 1,90 euro betaald voor de winegums. Tot zover niets vreemds. Behalve dat we een ov-kaart hebben gebruikt in plaats van een pas voor studenten en medewerkers. In allebei zit hetzelfde type chip, een zogeheten RFID-chip (radio frequency identification) van het type MIFARE Classic. “Die zijn gemakkelijk te kraken. En je kunt ook de informatie van de ene chip op de andere zetten. Dat heb ik hier gedaan. Dit was ooit een ov-chipkaart, maar nu gedraagt hij zich als VU-pas”, legt Bram uit. “Omgekeerd kan ook.”

Je hoeft volgens Bram helemaal geen supergoeie hacker te zijn om dit voor elkaar te krijgen. Voor een paar tientjes koop je een apparaatje waarmee je de informatie uitleest die op de personeelspas van de VU staat (toegangsrechten, koffiesaldo, kostenplaats; dat soort dingen) en op de ov-chipkaart, waarvoor een gelijksoortige pas wordt gebruikt.

Best slordig

Als je die code eenmaal gekopieerd hebt, kun je 'm op allerlei andere kaarten met

hetzelfde type chip zetten. Dat is wat Bram heeft gedaan. Hóé precies, demonstreert hij op de redactie met mijn personeelspas. Hij heeft er een paar minuten voor nodig, meer niet. De code achterop de pas is in principe genoeg om een bijna identieke pas na te maken, die door apparaten niet van de echte wordt onderscheiden. Bram: “Mensen zijn best slordig met die VU-passen. Ze verliezen hem, laten hem slingeren.”

‘Je trekt een trui aan met een VU-logo erop en niemand die er iets van denkt’

En als je eenmaal een pasje gekopieerd hebt, zet je de informatie op een lege RIFD-kaart. Wat je met je nieuwe pas kunt en welke deuren je binnenkomt, is afhankelijk van de rechten van de medewerker van wie je de pas hebt gekopieerd. Maar een upgrade naar

een pas waarmee je 24 uur per dag overal binnenkomt, is gemakkelijk te maken. Bram deed het met trial-and-error bij een rustige deur in het W&N-gebouw, waar geen camera hangt. Hoe lang hem dit heeft gekost? “Na een paar pogingen was het bingo”, vertelt hij. “Als je kwaad

‘Veiligheidsprobleem bekend’

Het is bekend bij de VU dat de toegangspasjes te kraken zijn. “Maar zo gemakkelijk is dat nu ook weer niet”, zegt Els van Haasen, manager services van de Facilitaire Campus Organisatie. “We weten ook dat er enkele gehackte pasjes in omloop zijn, maar dat zijn er heel weinig en die worden tot nu toe alleen gebruikt om koffie te halen. Dat houden we strak in de gaten.”

Dat ook het proefdiercentrum en de extra beveiligde laboratoria (waar met gevaarlijke stoffen wordt gewerkt) met hetzelfde systeem werken, klopt. Maar daar is de beveiliging wel veel strenger, aldus Van Haasen. “Daar hangen camera's en er zitten vaak sluizen. We houden bovendien heel strak in de gaten wie er binnen is geweest. Als dat iemand zou zijn met een gekraakte pas, blokkeren we die onmiddellijk.”

De VU is bezig met een nieuw systeem, hetzelfde soort RFID-pas, maar dan veel beter beveiligd. Dat staat voor volgend jaar gepland. Het is een operatie die nu begroot is op 5 ton.



wilt, kun je met zo'n pas alles meenemen wat je wilt. Je trekt een trui aan met een VU-logo erop en niemand die er iets van denkt.”

De deuren van het W&N-gebouw werken met dit systeem. Daar wordt gewerkt met potentieel gevaarlijke zaken als lasers en radioactieve stoffen. “Het W&N-gebouw is een oud gebouw, dat is misschien een verklaring waarom ze nog met een verouderd systeem werken”, suggereert Bram, “maar met deze pasjes kom je ook het Initium, de rechtenfaculteit, binnen. Bij zo'n nieuw gebouw zou je toch verwachten dat ze niet kiezen voor toegangspasjes waarvan bekend is dat ze zo gemakkelijk te kraken zijn?” Want het verhaal dat de VU-pasjes gemakkelijk te kraken zijn, is al lang bekend bij de bewaking. “We hebben ze het een paar jaar geleden al gemeld”, vertelt Bram. “Toen zeiden ze dat ze er niets mee gaan doen.”

Deur gewoon open

En wat te denken van het proefdiercentrum? Ook daar wordt gewerkt met hetzelfde type pasjes, weet Bram. “Maar bij het proefdiercentrum is trouwens het grootste veiligheidslek dat medewerkers de deur vaak gewoon open laten staan.” Bram vallen die dingen op. Hij heeft oog voor veiligheidskwesaties. Precies dat maakt hem een hacker. “Bedrijven huren hackers in om bij henzelf in te breken”, zegt Van der Zwart, “en daarbij is vertrouwen essentieel.”

Gekraakte wachtwoorden

Hacken is een hobby, misschien zelfs een verslaving, in elk geval iets wat je doet voor je lol. Even kijken of je ergens binnenkomt. Het zal toch niet? Het gevoel van spanning dat daarbij hoort. En soms heb je ineens een veel grotere vis te pakken dan je zelf ooit voor mogelijk had gehouden: alle wachtwoorden van de medewerkers en studenten van de exacte faculteit bijvoorbeeld. Dat gebeurde bij de overgang van het oude netwerk naar VUnet, zo'n twee jaar geleden. Informaticastudent Sernin van de Krol is er nog steeds een beetje beduusd van: “Hoe kan het nou dat je juist die wachtwoorden niet goed afschermt? Met een vriend zat ik wat te klooiën tijdens een college toen ineens al die wachtwoorden – weliswaar gecodeerd, maar heel makkelijk te kraken – op ons scherm verschenen. Oeps, foutje. We zijn in de pauze maar even naar de UC-IT gegaan om het te melden.”

Dan ga ik met Bram op excursie: deuren in het W&N-gebouw die gewoonlijk gesloten blijven, gaan open met zijn kaart. De enige deur die weigert, overigens niet in het W&N-gebouw, is die van de Advalvas-redactie, waarop pas een nieuw elektronisch slot zit. Zijn er dan ook nog andere toegangspasjes op de VU-campus? Bram: “Ja, het nieuwe systeem is veiliger, daarvoor heb je een helemaal identieke kopie van een kaart nodig en die is een stuk moeilijker te maken.”

Vals geld

Terug naar de snoepmachine: het zakje roze winegums valt naar beneden. Er is 1,90 euro afgetrokken van het saldo op de kaart. Daarmee zijn de snoepjes betaald. Bram stopt de kaart waarmee hij de snoepjes heeft betaald weer in zijn card-reader. Behalve het identificatienummer van de kaart, kan hij ook het saldo aanpassen. Dat zet hij weer terug op 5,01 euro. Hebben we de snoepjes nu gestolen? Bram denkt even na: “Nee, volgens mij krijgt de automaathouder gewoon zijn geld. Dat staat immers als saldo op die kaart, net als op andere kaarten. Daarin is geen verschil.” Maar wie heeft ze dan betaald? “Niemand. We hebben geld gecreëerd, vals geld dat niet van echt te onderscheiden is.”

Voor dit verhaal sprak Advalvas met een aantal hackers. De hacker die ons liet zien hoe hij een VU-pas heeft nagemaakt, hebben we op zijn verzoek geanonimiseerd. We noemden hem Bram.