INTERVIEW FONTYS DOCENT MARCO VAN DER LEE EN LEERLINGEN BAS RIJKENBERG EN THANH LIEM NGUYEN

‘WAT BIJ DE STUDENTEN IN HET VAT ZIT, KOMT ER BIJ ONS OOK ECHT UIT’

Grote kans dat je er vanochtend in de krant nog over hebt gelezen: cybercriminaliteit. Het item is ‘hot’ en de verhalen zijn zowel gevreesd als dat ervan wordt gesmuld. Vaak gaat het over cybercriminelen die computersystemen van organisaties aanvallen, met als doel data te stelen of om gijzelsoftware achter te laten: of u even wilt betalen?

TEKST Ronald Frencken | **FOTO’S** Erik de Brouwer

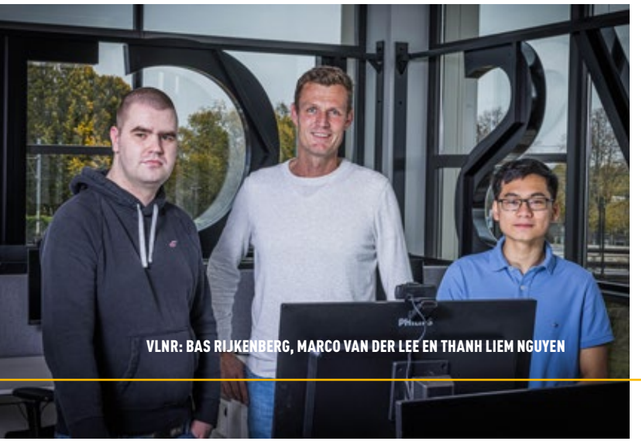
Veel verhalen over cybercriminaliteit laten zich lezen als een spannend boek, met herkenbare archetypen: de goeden, de cyberspecialisten, en de slechteriken: de hackers ofwel de ‘threat actors’. Bij Fontys Hogeschool ICT in Eindhoven weten ze alles van het kat-en-muisspel dat in deze wereld vaak op hoog niveau wordt gespeeld. Tijdens de module Cybersecurity maken tweedejaars ICT-studenten diepgaand kennis met cyberbeveiliging. Wij op onze beurt maken in dit verhaal kennis met hén, de studenten uit dit verhaal: de 25-jarige Bas Rijkenberg en Thanh Liem Nguye, 19, die wij op hun school ontmoeten. De eerste volgt bij Fontys de studierichting Infrastructure, de tweede de richting Technology. Beiden staan te trappelen om straks na het afstuderen de ICT-omgeving beter te maken - en veiliger. We maken ook kennis met Marco van der Lee, hun ruimhartige 48-jarige docent *slash* coach die hen helpt om hun potentieel te verwezenlijken.

FRISSE BLIK

Er is ook een rol weggelegd voor het Eindhovense ACA IT-Solutions, dat al meer dan dertig jaar gespecialiseerde ICT-oplossingen biedt, en daar graag studenten bij betrekt. Bij ACA vinden ze dat studenten hen met hun frisse blik en ideeën helpen scherp te blijven. Waarvan akte: ACA is officieel Partner in Education van Fontys. Dit is een samenwerkingsconcept waarbij bedrijven actief bijdragen aan het trainen van toekomstig ICT-talent. Dat krijgt zo een realistisch voorproefje uit de praktijk, en hen wordt ook nog eens een springplank geboden om na het afstuderen een succesvolle afsprong naar het bedrijfsleven te wagen. Win-win, en wie wil dat nu niet?

WAT WE ZIEN

Je zou je zomaar vergissen. Op de sfeervol ingerichte en inspirerende onderwijsetages van Fontys Hogeschool ICT in gebouw TQ op Strijp-T, waar we Bas, Thanh Liem en Marco spreken over de module Cybersecurity en hun project, moet je goed kijken voordat je in de gaten hebt dat er ook geleerd en gewerkt wordt. Dat je je überhaupt in een school bevindt, *for that matter.* Exit stille, lange gangen met links en rechts lokalen, bye bye jassenrekken. Wat we zien: meanderende looppaden, links en rechts glazen wanden in lichte tinten, her en der onderbroken door open ruimtes waar je op een ongedwongen manier naartoe wordt getrokken. Dan zijn er nog bespreekruimten en vanaf de paden zijn er overal fijne doorkijkjes naar wat daarachter gaande is – bijvoorbeeld de studenten verderop die met een bal bezig zijn, of kijk daar: twee anderen die



VLNR: BAS RIJKENBERG, MARCO VAN DER LEE EN THANH LIEM NGUYEN

‘DE MEESTE MENSEN WETEN DAT JE STERKE WACHTWOORDEN MOET GEBRUIKEN. MAAR DE PRIORITEITEN LIGGEN VAAK ANDERS.’

zich verdiepen in wat op een game lijkt die op de muur is geprojecteerd. Fontys bereikt ermee dat wat bij de studenten in het vat zit, er ook écht uitkomt. De prikkels die zij hier krijgen, halen ze bij voorkeur niet uit boeken maar vooral uit hun omgeving - bij medestudenten, bij docenten en natuurlijk bij het bedrijfsleven dat hun ideeën op prijs stelt - waardoor ze ook nog eens beter beklijven. Daar draagt het vrije uitzicht vanaf de tweede verdieping van TQ op Eindhoven Noord-West, het meest veelbelovende, innovatieve en inspirerende deel van Eindje, ontegenzeggelijk aan bij.

‘Een fout is zó gemaakt: een vreemd linkje, hé leuk, klik en het is gebeurd.’

OSINT

ACA IT-Solutions, dochterbedrijf van Crowe Foederer, heeft als Partner in Education een meerjarige samenwerking met Fontys. Wapenfeit daar was een boeiende samenwerking afgelopen voorjaar tussen ACA en een groepje Fontys ICT-studenten, onder wie studenten Bas en Thanh Liem. “Op verzoek van ACA deden we een OSINT-onderzoek, voluit: Open Source INTelligence-onderzoek. Dit is onderzoek naar data die op het internet zijn achtergelaten en die potentieel riskant kunnen zijn”, legt Thanh Liem uit. “Ook hebben we er de eerste fase van een zogenaamde penetratietest gedaan, een pentest. Je test dan een computersysteem op kwetsbaarheden bij aanvallen van buitenaf. Zo krijg je aanknopingspunten om de beveiliging te verbeteren. We zochten naar data die medewerkers van een bedrijf op het internet hebben achtergelaten, en we deden de penetratietest op hun server. Zo ontstond een beeld of er sprake kon zijn van een mogelijk bedreigende situatie voor het bedrijf. Uiteindelijk kwamen wij in onze eindrapportage met verbeterpunten waar het bedrijf ook echt iets mee kan.”

TRENDS EN PATRONEN

“Kijk”, zegt Bas, zorgvuldig zijn woorden kiezend, “weet je wat het is? De meeste mensen weten intussen dat je sterke wachtwoorden moet gebruiken, en dat je niet moet klikken als je de boel niet vertrouwt. Tegelijkertijd liggen de prioriteiten heel anders. Er wordt via allerlei sociale platformen veel privé-informatie gedeeld. Sterke wachtwoorden kiezen die toegang geven tot deze platformen komt daarbij pas op een tweede of derde plek. Het gaat goed mis als cybercriminelen inbreken op computersystemen en platformen, en hier gebruikersnamen en wachtwoorden buitmaken. Hebben ze die ter beschikking dan is het alleen nog maar een kwestie van deze met elkaar combineren. Zo ontstaan trends en patronen die inzicht geven in hoe computergebruikers denken, bijvoorbeeld over wachtwoorden die zij waarschijnlijk voor andere accounts en platformen gebruiken. Met die inzichten zijn criminele vervolgstappen, online of in de echte wereld, makkelijk gezet.”

LAAGHANGEND DIGIFRUIT

De wereld van de cybercriminaliteit laat zich lezen als een spannend verhaal, geschreven door mensen die spanning niet schuwen. Wat te denken van een ‘Password Spraying Attack’, een online computeraanval waarbij een kwaadwillende wachtwoorden op allerlei accounts en platformen uitprobeert, tot er een werkt: binnen! Het werkt helemaal geautomatiseerd. De cybercrimineel hoeft zelf geen wachtwoorden in te typen en leunt tijdens zijn aanval lekker achterover. Dit type aanvallen is vaak gericht op laaghangend digifruit; op makkelijke wachtwoorden dus. Uit onderzoek blijkt dat simpele wachtwoorden of wachtwoordcombinaties (‘password123’, ‘123456’, ‘Welkom2021’: ze bestaan nog!) met de pientere computers van nu binnen twee seconden te kraken zijn. Ook worden databases met eerder gestolen gebruikersnamen en wachtwoorden gebruikt, want het is alom bekend dat veel mensen hetzelfde wachtwoord voor meerdere accounts gebruiken. Een gemakkelijke binnenkomer…

‘HACKERTJE’ SPELEN

Het team waar Bas en Thanh Liem deel van uitmaakten, mocht tijdens het project zelf even ‘hackertje spelen’. Moet een goed gevoel zijn geweest: mogen inbreken op het computersysteem van een bedrijf, of niet, Bas en Thanh Liem? “Was zeker interessant”, zegt Thanh Liem. “Maar bij een OSINT-opdracht en bij pentesting is het wel de bedoeling dat je vooraf afspraken maakt met de opdrachtgever. Zomaar losgaan is er echt niet bij. Je spreekt bijvoorbeeld af dat je alleen kwetsbaarheden blootlegt, zonder ook daadwerkelijk op de server te gaan rondsnuffelen.” Daarnaast ging het natuurlijk om een leeropdracht onder begeleiding van de ervaren cybersecurityspecialisten van ACA IT-Solutions. “Tijdens het project maakten ze kennis met riskmanagement en de taken van de security engineer”, zegt Marco. “Ze leerden ook over zogenaamde ethical hacking technieken: welke tools kun je inzetten? Welke kwetsbaarheden zijn er, en hoe kun je die blootleggen? Hoe ver mag je gaan als Red Team, het aanvalsteam dat probeert in te breken, en wat mag het Blue Team, het team dat de aanval moet afslaan? Je spreekt het vooraf samen af.”

JUST CULTURE

Met het OSINT-project geven onze gastheren een bijzonder inkijkje in hedendaags ICT-onderwijs, waar leraren, studenten én het bedrijfsleven elkaar versterken, samen tot nieuwe inzichten komen en waar van een traditionele rolverdeling tussen de school, student en werkgever geen sprake meer is. Marco zou graag een frisse wind zien door de cybercultuur bij veel organisaties. Hij pleit voor een ‘just culture’, waarin medewerkers incidenten veilig kunnen melden, en waarin bedrijven bereid zijn open te staan voor fouten van hun medewerkers, om hiervan te leren. “Vaak worden zij nu nog afgerekend op hun cybergedrag. Terwijl organisaties er juist baat bij hebben als medewerkers het meteen aangeven als er iets is misgegaan. Vaak valt er dan nog veel te herstellen. Een fout is menselijk en is zó gemaakt: een vreemd linkje, hé leuk, klik en het is gebeurd. Daar valt nog veel te winnen. Dat doe je samen.” ■

‘Zomaar losgaan is echt niet de bedoeling.’