Verslag Cyber Security Congres 2016

Betere samenwerking maakt van mens de sterkste schakel in de keten Iedere onderwijsinstelling heeft te maken met cyberaanvallen. Zonder voldoende weerbaarheid gaat het onderwijs een onveilige toekomst tegemoet. Tijdens het Cyber Security Congres op 18 november zijn bestuurders, managers en security officers tot de conclusie gekomen dat kennisdeling en samenwerking onmisbaar is om de weerbaarheid te versterken.

Opening

Never waste a good crisis. Hoe vervelend een cyberaanval ook is, het leidt hopelijk wel tot meer kennisdeling en meer actie voor cybersecurity, zegt Marjolein Jansen, vicevoorzitter van het College van Bestuur van de VU. Ze spreekt haar zorgen uit over de lage investeringen binnen het hoger onderwijs in een goede infrastructuur voor cybersecurity. "Onze business continuïteit is in toenemende mate afhankelijk van IT. Als hoger onderwijs hebben we een zekere mate van wendbaarheid en weerbaarheid nodig, anders vrees ik dat we niet meer zo veilig zijn als voorheen."

De toekomst van cybersecurity

Waar moeten we precies bang voor zijn? Herbert Bos, hoogleraar systeem- en netwerkbeveiliging aan de VU, heeft wel wat voorbeelden. Het meest beangstigende aan de hacks die zijn team recent uitvoerde, is dat er geen bugs aan te pas kwamen. Zo toonden ze een kwetsbaarheid in Android aan, die een slimme hacker toegang geeft tot twee apparaten voor de prijs van één. Geen bug, maar een *feature*. De lessen die Bos het publiek voorhoudt: al is de software perfect ontwikkeld en goed geconfigureerd, je kan nog steeds worden gehackt. Hoe complexer en efficiënter de software en hardware, hoe kwetsbaarder. Zijn team won verrassend weinig bounty's, prijzengeld voor het aantonen van zwakke plekken, maar desondanks noemt Bos bounty-projecten een nuttig middel voor het hoger onderwijs, mits slim ingezet. En moge het nog niet duidelijk zijn: de meeste hackers staan aan de goede kant. Geef ze de waardering die ze verdienen.

Parallelsessies

Er volgen parallelsessies over benchmarking, crisismanagement, awareness en samenwerken.

Sessie benchmarking

In de sessie over benchmarking vertellen Ludo Kuipers van Kennisnet en Ronald Sarelse van de Radboud Universiteit over het SURFaudit framework. Een audit aan de hand van het SURF normenkader brengt het informatiebeveiliging en privacybeleid (IBP beleid) van de onderwijsinstelling in kaart en legt de zwakke plekken bloot. Er zijn vijf niveaus van volwassenheid, waarbij niveau vijf volgens Kuipers en Sarelse zelden wordt bereikt. Het is mogelijk om het eigen niveau te bepalen met behulp van self-assessment tools. Betrouwbaarder is een korte peer review, waarbij een security officer van een andere instelling checkt of de score die de instelling zichzelf toekent, overeenkomt met zijn eigen oordeel. Er is discussie over de vraag of er een uitgebreide peer audit in SURF-verband moet worden georganiseerd. Een externe audit en ISO-certificering behoren ook tot de mogelijkheden, maar met het Peer-Review programma en de tweejaarlijkse SURFaudit benchmark kom je een heel eind. Dit jaar doen er elf instellingen mee.

Sessie awareness

In deze sessie werden voorbeelden getoond van datalekken, identiteitsfraude, datamanipulatie, spionage, misbruik van ICT-voorzieningen en verstoring van de infrastructuur die in de media zijn gepubliceerd. Imagoschade is een groot risico. Op organisatorisch vlak wordt beleid gemaakt om cybersecurity onder controle te krijgen. Op technisch vlak wordt de juiste techniek ingezet om security en privacy in te regelen. Maar daarmee zijn we er niet. Het is van groot belang om kennis en bewustwording bij te brengen bij mensen die werken en leren in de digitale wereld. Een aantal voorbeelden van hoe de deelnemers van de sessie bewustwording creëren:

1. Er zijn instellingen die hun privacybeleid hebben verbeterd door een WBP-melding af te geven aan leveranciers. Ook hebben ze onder andere tips aangereikt voor inloggen en het vergrendelen van laptops. Het resultaat is dat 88 procent van de bedrijfsprocessen inmiddels is aangesloten.
2. Sommige instellingen zetten ICT-studenten in om bewustwording onder studenten te creëren door te laten zien wat er allemaal kan gebeuren.
3. Criminelen weten precies wanneer colleges beginnen en spelen daarop in. Vrijdagmiddag of maandagochtend zijn momenten waarop phishing-acties plaatsvinden.

De meeste deelnemers zijn echter zoekende. Sommige vingerwijzende acties kunnen negatief uitwerken, een positieve benadering door beloning is mogelijk effectiever. Creatief omgaan met bewustwording en stap voor stap aandacht blijven schenken aan dit onderwerp is de beste oplossing.

Een betere samenwerking kan het effect van security awareness te versterken. De deelnemers van de sessie hebben voornamelijk behoefte aan het delen van ervaringen in de wiki/ toolkit van Cybersave Yourself en het delen van slides en trainingen over security awareness. Er is ook behoefte aan een Engelse versie van de materialen in de toolkit. Een mailinglijst om ervaringen te delen over CSY zou een brug moeten slaan tussen P&O, communicatie en security officers.

Sessie crisismanagement

Bij de sessie over crisismanagement wordt teruggeblikt op de cybercrisisoefening OZON, die op 4 en 5 oktober werd georganiseerd door SURFnet samen met 27 onderwijs-, onderzoek- en zorginstellingen. Deze oefening was een initiatief van SURFcert. Remon Klein Tank geeft als initiatiefnemer van de oefening een korte inleiding hoe de oefening is voorbereid, waarna Maarten Brouwer, Mladen Acinger en Rogier Ragetlie de ervaringen van de oefening van respectievelijk de Universiteit Wageningen en de Erasmus Universiteit delen. De presentatie wordt afgesloten door Alf Moens (SURFnet) die een aantal uitkomsten van de oefening deelt en aangeeft dat het komende jaar zal worden geëxperimenteerd met ander soort oefeningen.
Een aantal belangrijke leerpunten uit de oefening zijn:

1. Binnen een instelling worden de gevolgen van een cybercrisis vaak te klein of juist veel te groot ingeschat, waardoor men niet in actie komt door een gebrek aan urgentie of juist door een gevoel dat de crisis überhaupt niet kan worden beheerst.
2. Een cybercrisis duurt vaak veel langer en is van een onduidelijkere aard dan verwacht, waardoor er extra goed moet worden gelet op het behouden van focus.
3. De oefening heeft ook gefungeerd als teambuilding-oefening. Mensen weten elkaar nu veel beter te vinden als het over dit onderwerp gaat.

Sessie samenwerken

Communities drijven op een gemeenschappelijke win-win situatie. Juist op gebieden waarop instellingen niet hoeven te concurreren, kan een community erg succesvol zijn door een collegiale en open sfeer. Zo kan de mens als zwakste schakel worden omgezet in de sterkste schakel. In de sessie over samenwerking wordt aan de hand van presentaties over SCIRT en SCIPR de opzet, de werking, maar vooral ook het belang van communities besproken. Het is belangrijk dat deelnemers door hun instellingen in de gelegenheid worden gesteld om vanuit een eigen behoefte en inbreng te participeren. Instellingen zouden op allerhande gebieden in communities kunnen participeren, waarbij de instelling in de ene community meer kennis of vaardigheden zal halen en in een andere community juist meer kan brengen, waarbij die balans van ondergeschikt belang is.

Crisisscenario panel

Dagvoorzitter Chris van 't Hof selecteert drie willekeurige mensen uit de zaal die aan een denkbeeldige crisis worden gezet: een enquête op de website van de VU bevat opeens een aantal onbetamelijke vragen, die door goedgelovige studenten zijn beantwoord. Terwijl het tijdelijke College van Bestuur overlegt over het communicatieplan, verschijnt er een artikel online ('VU lekt pikante lifestyle gegevens studenten') en verplaatst de zaal zich in de rol van de getroffen studenten. In alle commotie vergeet het college een bedankje aan de anonieme bron die ze wees op het datalek.

In een tweede crisisscenario ontspint zich een ethisch dilemma: er is geknoeid met de certificaten van de VU en er is een lek dat in het kader van responsible disclosure aan het Nationaal Cyber Security Centrum (NCSC) dient te worden doorgegeven. Het Ministerie van Defensie wil het lek tijdelijk open laten, om te onderzoeken wie er misbruik van maakt. Geen vergezocht scenario, verzekert Van 't Hof de congresbezoekers, want helaas aan de orde van de dag. Is de nationale veiligheid belangrijker dan privacy? De zaal reageert verdeeld.

Lightning Talks

Vier pitches leveren nieuwe ideeën op over informatiebeveiliging en privacy. Michael Mehrow van Windesheim bijt het spit af met een app voor crisissituaties. In het geval van een ontruiming biedt de app de mogelijkheid om studenten en medewerkers door middel van pushberichten te bereiken.

Tim de Graaf, student cybersecurity bij Fontys Hogeschool, stelt voor om securitytrainingen te integreren in een escape room.

Ricardo de Oliveira Schmidt van de Universiteit Twente beschrijft de analyse van een DDoS aanval in 2015 op een root DNS Event. Een dergelijke aanval kan zo schadelijk zijn, dat niemand nog toegang heeft tot het internet. De Oliveira Schmidt stelt vast dat een dergelijke impact vooralsnog niet heeft plaatsgevonden, maar dat we ons bewust moeten zijn van de werking van deze kritieke infrastructuur.

Bart Bosma van SURFnet presenteert het Cyberdreigingsbeeld 2016. Deze uitgave, die ook in boekvorm wordt uitgereikt aan de deelnemers, beschrijft de topdreigingen voor onderwijs, onderzoek en bedrijfsvoering en geeft een overzicht van de belangrijkste trends in cyberdreigingen voor het hoger onderwijs.

De economische en maatschappelijke noodzaak van cybersecurity

Rob van Wijk, oprichter en directeur van The Hague Centre for Strategic Studies (HCSS), professor International Relations aan de Universiteit Leiden en voorzitter van de Denktank Nationale Veiligheid, licht de economische en maatschappelijke noodzaak van cybersecurity toe. Centraal in zijn keynote staat de vraag: 'wat weten we eigenlijk?' Dat blijkt nogal weinig, met name als het over spionage gaat. Zeker over het onderwijs is er nauwelijks kennis beschikbaar. Ondertussen maakt digitale revolutie ons in hoge mate afhankelijk van ICT. Hoe welvarender en meer gedigitaliseerd een samenleving is, hoe aantrekkelijker voor cybergespuis. Van Wijk schetst een angstwekkend beeld van de hoogwaardig geavanceerde operaties die anno 2016 door beroepscriminelen worden uitgevoerd. Economische spionage zet de concurrentiepositie van Nederland onder druk. Ransomware is gemeengoed geworden en malvertising rukt op. Cybersecurity brengt hoge kosten met zich mee, maar Van Wijk geeft de boodschap mee dat onze welvaart het veiligste internet ter wereld vereist.

Cybersecurity op de bestuurstafel

Uit hoofde van zijn functie, Cybersecurity Lead Partner bij KPMG, praat John Hermans regelmatig bestuurders bij over cyberdreiging. Hoe verleidelijk het ook is om te roepen dat 'de boel achter slot en grendel moet', 100 procent veiligheid is een onbetaalbaar streven. Het is verstandiger om een risicoprofiel van de instelling op te stellen met aandacht voor cyber en aan de hand daarvan realistische maatregelen te nemen. De belangrijkste vraag daarbij: wat zijn uw kroonjuwelen? Wat is interessant voor een derde partij? Zo kunt u bepalen wat u ten alle tijden wilt beschermen. Net als Van Wijk benadrukt Hermans hoe belangrijk het is om de motivatie van de derde partij te achterhalen.
Het is kinderlijk eenvoudig om medewerkers zelf de deur wijd open te laten zetten voor cybercriminelen, toont Hermans aan met behulp van een paar sprekende voorbeelden. Maar weerbaarheid kun je oefenen. De mens, die zwakste schakel in de keten, kan zich opwerken tot de sterkste schakel. Hermans hamert bovendien op samenwerking. "Dit los je nooit alleen op. Dit is niet concurrerend, dus doe als de banken en zoek elkaar op!"

Debat 'De Cyberwereld Draait Door - Hoger Onderwijs Special'

Het afsluitende debat wordt voorafgegaan door een video van de cybercrisisoefening OZON. "Er gaat van alles fout en dat moet ook, want dat is waardevol voor als het echt zo ver is," becommentarieert Hans de Vries, hoofd van het Nationaal Cyber Security Centrum.

In het information sharing exchange center (ISEC) van het NCSC wordt kennis over aanvallen gedeeld, zodat concullega's niet tegen dezelfde zaken aanlopen. "Polderen zit ons in de bloedvaten," zegt De Vries. "Wij snappen dat je elkaar nodig hebt om het proces goed te organiseren."

Vandaag doen de bestuurders uit het hoger onderwijs hetzelfde. Uit de ervaring die de VU in maart 2016 opdeed met ransomware, leerde Marjolein Jansen om de situatie niet te isoleren tot een IT-probleem, maar eerder te escaleren. Liz Chermin van HAS Hogeschool werd door een student gewezen op een datalek in de DLO. "Dit soort studenten moeten we echt koesteren," zegt ze. Bert Voorbraak, CIO en directeur ICT Services van de UvA en de HvA, beschrijft een scenario waarin een student graag de publiciteit wil zoeken met het lek dat hij heeft gevonden en wijst op het belang van een breder communicatieplan.

Het centraal melden van een probleem wordt in de commotie nog wel eens vergeten. SURF is hiervoor het eerste aanspreekpunt. Zo nodig geeft SURF de kwetsbaarheid weer door aan het NCSC. De Vries:

"Het is heel belangrijk om sectoren met elkaar te verbinden. Via SURF weten wij waar een probleem elders ook speelt.

Anka Mulder, vice-president voor Education & Operations aan de Technische Universiteit Delft, benadrukt dat het op slot gooien van de ICT haaks staat op de openheid die het hoger onderwijs nastreeft. Tegelijkertijd beaamt ze dat haar instelling een paar interessante kroonjuwelen in huis heeft, zoals een kwantumcomputer. "Als sector is er zeker iets te winnen bij samenwerking, want veiligheid zit niet in onze genen," zegt ze. "Je gaat niet bij een hoger onderwijsinstelling werken omdat je geïnteresseerd bent in veiligheid."

Bij gebrek aan expertise in eigen huis, zijn kleinere instellingen volgens Chemin eerder gedwongen om de samenwerking op te zoeken. Als Van 't Hof vraagt naar de kroonjuwelen van de bestuurders aan tafel, blijken die op veel onderdelen overeen te komen, zoals de betrouwbaarheid van toetsgegevens en diploma's. De Vries adviseert om de meer basale infrastructuur op het gebied van cybersecurity te delen, net zoals dat op rijksniveau gebeurt. Uit de zaal klinkt instemmend gemompel. "Op het niveau van SURF proberen we die consolidatie voor elkaar te krijgen met bijvoorbeeld SURFcumulus en SURFdrive," zegt Voorbraak. "Als sector zijn we op de goede weg, maar er kan nog een tandje bij."

Jansen: "We staan pas aan de vooravond van kennisdeling op bestuurlijk niveau. We hoeven niet alles samen te doen, maar laten we de kroonjuwelen onder de loep nemen. Waar zit de natuurlijke affectie? Daar kunnen we slagkracht maken."

Om direct daad bij het woord te voegen, wordt ze door SURFnet-directeur Erwin Bleumink benoemd tot ambassadeur voor cybersecurity. "Cyber is onderdeel van onze wereld, niet van een andere" zegt Jansen. " Dat vraagt om een integrale veiligheidsaanpak, daar hoort de relatie tussen cyber en fysieke veiligheid ook bij. Ik zal me inzetten om bestuurders hiervan te doordringen, te beginnen met de bestuurders die hier vandaag niet zijn."

==========