Online expertsessie ‘Een cyberaanval, en nu'

Op 13 maart jl. vond de VMRG online Expertsessie ‘Een cyberaanval, en nu?’ plaats. Experts Kelvin Rorive, oprichter van de Cyber Chain Resilience Consortium (CCRC), en Remco Visser, ICT manager bij Rollecate en helaas ervaringsdeskundige op het gebied van een cyberaanval, schoven aan tafel bij Henk Zoontjens, directeur bij de VMRG. We blikken terug met een greep uit de vragen die in deze sessie aan de orde kwamen.

Digitalisering in de bouw ontwikkelt zich snel en bedrijven worden gestimuleerd om mee te ontwikkelen. Dat is positief, maar brengt ook risico’s met zich mee. Kun je daar iets meer over vertellen?
Rorive: Bij digitalisering draait het niet alleen om het eigen bedrijf. Bedrijven zijn via digitalisering steeds meer met elkaar verbonden. Als er in die keten iets fout gaat, beperkt het zich vaak niet tot één bedrijf. Mijn ervaring is dat bij 9 van de 10 cyberaanvallen de oorzaak lag bij een bedrijf waar mee samengewerkt werd in de keten.

De oorzaak van een cyberaanval ligt vaak niet bij het eigen bedrijf. Jullie hebben helaas een cyberaanval gehad, hoe ging dit bij jullie?
Visser: Bij ons lag de oorzaak inderdaad ook bij een toeleverancier. De mailomgeving van deze leverancier was gehackt. Vanuit hun mailsysteem is een mail naar ons gestuurd met een foute link waarop geklikt is. Al snel bleek dat we niet meer bij bestanden konden en er data gestolen was. Ook kwamen we op meerdere plekken een bestand tegen van de hackers die losgeld vroegen en dreigden om de gestolen data op het dark web te zetten. We hebben toen een extern bedrijf ingeschakeld dat gespecialiseerd is in cybercriminaliteit.

Wat is het dark web en wat gebeurt daar?
Rorive: Dat is een deel van het internet dat door normale zoekmachines niet gevonden wordt en waar veel criminele activiteiten plaatsvinden.

Wat gebeurde er toen je een in cyberaanvallen gespecialiseerd bedrijf ingeschakeld had?
Visser: Zo’n gespecialiseerd bedrijf neemt de regie meteen over. Het bedrijf ligt dan stil, want er moet eerst forensisch onderzoek plaatsvinden en alleen dit onderzoek duurde al bijna een week. Het is namelijk belangrijk om te weten waar de oorzaak ligt. Alles wordt gescreend en stukje voor stukje weer opgebouwd en vrijgegeven in een veilige omgeving, dus niet in het netwerk. Ook is er aangifte gedaan bij de Autoriteit Persoonsgegevens en bij de politie.

Hoe vaak komt dit nou voor?
Rorive: Waar we harde cijfers van hebben, is van de bedrijven die een cyberverzekering hebben en dan gaat het om één op de drie bedrijven. Slachtoffers komen in alle sectoren voor, en helaas zien we in de industrie en handel een stijgende lijn.

De phishingmail is blijkbaar niet als zodanig herkend, hoe kwam dat?
Visser: De mail kwam van een bekende afzender, waar al mailcontact mee was. De vreemde link in de mail wordt pas zichtbaar als je er met je muis eroverheen gaat. Maar dat gebeurt niet in de praktijk, als de mail er niet verdacht uit ziet.

Henk Zoontjens (r) in gesprek met Kelvin Rorive (l) en Remco Visser.

Interactieve cybercrisis oefening.

Kan een bedrijf een cyberaanval voorkomen?
Rorive: Mensen moeten zich ervan bewust zijn dat criminelen altijd ergens binnenkomen als ze maar willen. Als bedrijf is het belangrijk om het de crimineel zo lastig mogelijk te maken, dus om de cybersecurity zo goed mogelijk op orde hebben. Daarnaast is het goed om mensen te leren om gezond achterdochtig te worden. Dat betekent bij twijfel een mail weggooien of er een expert naar laten kijken. Dan is het risico al fors kleiner dat je slachtoffer wordt.

Hoe verloopt de communicatie bij zo'n cyberaanval?
Visser: De eerste gedachte die in je bedrijf opkomt, is angst voor imagoschade. Er is nog een taboe om te communiceren dat je gehackt bent. Cyberschaamte wordt dit ook wel genoemd. Het gespecialiseerde bedrijf dat we ingeschakeld hadden, heeft de communicatielijnen van ons overgenomen. Je hebt wel met de hackers te maken, dus de juiste communicatie naar de juiste mensen op het juiste moment is heel belangrijk.

Ligt de verantwoordelijkheid bij de IT manager om het bedrijf zo goed mogelijk voor te bereiden op een cybercrisis?
Visser: Cybersecurity begint bij de directie. Als daar geen bewustwording is of noodzaak gezien wordt, dan kun je weinig als medewerker.

Cybersecurity begint bij de directie. Wat als een directie de noodzaak hiervan niet ziet?
Rorive: Er komt Europese wetgeving aan op dit gebied, dat is de NIS2. Die stelt de bestuurder aansprakelijk bij nalatigheid. De wetgeving geldt voor bedrijven van een bepaalde omvang en met een kritische maatschappelijke rol. Maar als niet je eigen bedrijf, maar jouw opdrachtgever wel aan deze wetgeving moet voldoen, krijg je daar als bedrijf toch mee te maken. Het is dus voor elk bedrijf goed om zich te verdiepen in deze wetgeving.

Heeft het zin om je bedrijf voor te bereiden op een cybercrisis als er bij een aanval toch een expertbedrijf ingeschakeld wordt?
Rorive: Vanuit de stichting die ik opgezet heb, laten wij bedrijven oefenen met een cyberaanval situatie. Uit onderzoek onder cyber expertbedrijven blijkt dat het ongelooflijk verschil maakt op het moment dat er bij een gehackt bedrijf al een crisisteam zit dat volledig weet wat er gaat komen. Ook economisch gezien. Het droog oefenen van een cybercrisis is dus echt heel erg belangrijk

Interactieve cybercrisis oefening
De VMRG biedt in samenwerking met CCRC een interactieve cybercrisis oefening aan voor directies en iedereen die verantwoordelijk is voor security van haar aangesloten bedrijven. Deelnemers krijgen een realistisch oefenscenario voorgelegd. In een drie uur durende sessie gaat men in kleine groepjes onder begeleiding van een specialist ervaren en leren wat er komt kijken bij het afhandelen van een cybercrisis. Deze cybercrisis oefening vindt plaats op woensdagmiddag 8 mei in Nieuwegein. Aanmelden kan direct met de QR code of via de website van de VMRG: https://vmrg.nl/ academy/cursussen/Cyber crisis-oefening ▮