nrc
ZATERDAG 28 FEBRUARI & ZONDAG 1 MAART 2026

Een **winkel van Odido** in Helmond. Hackers hebben klantgegevens bij de provider geroofd. FOTO ROB ENGELAAR / ANP

CYBERCRIMINALITEIT

Systeem gehackt – moet Odido losgeld betalen of niet?

Hackers publiceerden gestolen klantgegevens van Odido op het 'dark web'. De provider gaat nog niet in op hun eis voor losgeld. Nick Bos, oud-bestuurder van de Universiteit Maastricht, legt uit waarom de universiteit dat destijds wél deed.

Bas Blokker

AMSTERDAM

Op maandagavond, 23 december 2019 merkte de Universiteit Maastricht dat hackers waren binnengedrongen in haar computers. Een paar uur daarna lag het hele systeem plat. Korte tijd later meldden criminelen zich met hun eis: de universiteit moest tien bitcoins, toen ter waarde van in totaal een kleine 200.000 euro, betalen, dan zou ze een 'sleutel' krijgen waarmee het systeem kon worden heropend.

Zo bevond Nick Bos, destijds bestuurder van de Universiteit Maastricht en voorzitter van het team dat inderhaast werd ingesteld om de crisis het hoofd te bieden, zich ineens in de situatie waarin de top van provider Odido nu is beland. Cybercriminelen hebben zich dankzij een lek toegang weten te verschaffen tot jouw systeem (of data), eisen losgeld en de vraag is dan: wat doe je?

Om het maar meteen te verklappen: de Universiteit Maastricht heeft destijds betaald. En sindsdien voelt Bos de dure plicht om aan de buitenwereld uit te leggen wat er is gebeurd en waarom de universiteit besloot de eis van de cybercriminelen in te willigen.

Ervaringsdeskundige Bos en communicatiedeskundige Youssef Eddini, directeur van Van Luyken Groep, laten hun licht schijnen over een crisis als die waarin Odido zich bevindt, nadat hackers een weekend lang persoonlijke data van zo'n 6,2 miljoen klanten konden downloaden. De dieven hebben van Odido ook losgeld geëist: één miljoen euro of de klantgegevens zouden worden gepubliceerd. Tot nog toe heeft Odido niet willen betalen. Bos noch Eddini zijn betrokken bij de zaak rond Odido en ze doen dus geen uitspraken over wat daar nu speelt.

In zo'n situatie wordt een crisisteam bijeengeroepen, zegt Eddini, waarin de interne adviseurs uit het bedrijf en externe adviseurs uit verschillende disciplines plaatsnemen. Als communicatie-expert zou hij in zo'n team vooral de reputatieschade wegen. Daarnaast zijn er bij cybercriminaliteit experts op dat terrein aanwezig, die zicht hebben op de werkwijze van de hackers, op de schade die is aangericht, op de 'redelijkheid' van de eisen en volgens Eddini voeren zij soms ook de onderhandelingen met de cybercriminelen. „Het advies in zo'n geval komt er ruwweg op neer dat de cyberexperts hun oordeel geven over de waarde van de gestolen waar en de schade die ermee gemoeid is", zegt Eddini. „Zij kunnen tegen een bedrijf zeggen: gegevens van deze omvang en gevoeligheid wil je echt niet op straat laten komen."

Het crisisteam van de Universiteit Maastricht vroeg cyberbeveiligingsbedrijf Fox-IT als extern adviseur. „We waren letterlijk en figuurlijk overvallen", zegt Bos. „Dit was 2019, toen keken we nog anders aan tegen cybercriminaliteit dan nu. We waren niet helemaal groen, maar toch... We hadden bijvoorbeeld een ruimte ingericht voor de crisiscommunicatie. Maar toen Fox-IT binnenkwam, zeiden ze: je moet wel de gordijnen sluiten, honderd meter verderop kunnen ze nog zien wat je hier doet."

Een half jaar dicht

Twee omstandigheden waren voor de Universiteit Maastricht destijds anders dan voor Odido nu. De universiteit is een publieke instelling, Odido is een bedrijf. Bij Odido zijn klantgegevens geroofd en zijn de klanten dus de belangrijkste benadeelde partij. Bij de universiteit wisten ze niet of er ook data uit het systeem waren gedownload. Bos: „Toen we in contact kwamen met de hackers, bezwoeren die ons dat ze geen data hadden gedownload."

Om te bepalen of ze moesten ingaan op de losgeldeis, maakte de universiteit drie afwegingen. De eerste vraag was of ze zelf een sleutel konden ontwikkelen om hun systeem weer vrij te krijgen. „We kwamen er vrij snel achter dat je dat kunt vergeten. Dat duurt jaren."

De volgende kwestie: is het denkbaar dat we dit systeem als verloren beschouwen en een heel nieuw opbouwen? Volgens een van de ter zake kundige adviseurs zou dat minimaal een half jaar kosten „voordat je het rudimentair weer een beetje op orde hebt", zegt Bos.

De schade zou in dat geval gigantisch zijn. De 5.000 aan de universiteit verbonden wetenschappers zouden hun onderzoeksgegevens kwijt zijn. „Onze medische faculteit deed longitudinaal onderzoek, dat betekent dat je je patiënten zou moeten lastigvallen om iets van die gegevens te redden." De 22.000 studenten zouden een half jaar niet kunnen studeren en dus vertraging oplopen. „Het leed dat je daarmee veroorzaakt, is groot."

Toen ze zich realiseerden dat er in dat geval een schadevergoeding zou moeten worden betaald, werd een schatting van de kosten gemaakt. „Wij kwamen, grofweg, op 20 tot 25 miljoen euro per maand."

> Op enig moment ligt de schade van de gestolen gegevens niet meer primair bij het bedrijf, maar bij de klanten

Alles, zegt Youssef Eddini, schade aan het systeem, schade aan de bedrijfsvoering, geschatte reputatieschade – alles druk je uit in geld zodat je zicht krijgt op de totale schade die je riskeert, en die zet je af tegen het losgeld en de schade voor je reputatie als je wél betaalt. De waarde van de gestolen data, zoals in het geval van Odido, weegt daar zwaar in mee. Op enig moment ligt de schade van de gestolen gegevens niet meer primair bij het bedrijf, zegt Eddini, maar bij de klanten. „Dan gaat het schuren. Dat is het moment waarop je klanten zich beginnen af te vragen: waarom betalen ze eigenlijk niet gewoon?"

Sterker nog, een groep rond ethisch hacker Sijmen Ruwhof is een crowdfundingsactie begonnen om het losgeld dat van Odido wordt geëist, te voldoen. Volgens Ruwhof zijn de gegevens te kostbaar om niét te betalen.

Ontraden

Dat was afweging nummer drie voor de Universiteit Maastricht: moeten we de sleutel van de hackers kopen om het systeem te heropenen? „De overweging dat we zo de continuïteit van de organisatie konden garanderen, heeft er toe geleid dat we besloten hebben te betalen", zegt Bos. „Om tot dat besluit te komen, hebben we een week de tijd genomen. Die tijd hadden we ook nodig voor overleg met de politie, het ministerie, de onderwijsinspectie, de raad van toezicht, de decanen van onze faculteiten. Je hebt ook wel wat te verantwoorden. De politie heeft ons voortdurend ontraden te betalen."

Afgezet tegen de mogelijke schade voor de universiteit was de geëiste losgeldsom bijna bescheiden. „Voordat ze met hun eis kwamen, hadden we het bedrag wel wat hoger verwacht", zegt Bos. „Tien bitcoins, 200.000 euro, dat is zonde van het geld hoor, laat dat duidelijk zijn. Maar het staat absoluut niet in verhouding tot de schade die we anders zouden lijden. Als ze een hoger bedrag hadden geëist, dan was de afweging wel weer wat scherper geweest." Dat Bos het toch een „duivels dilemma" noemt, heeft dan ook niet zozeer met het geld te maken, maar „met het idee je een crimineel systeem in stand houdt".

Een wallet in Oekraïne

De overdracht van het losgeld had ook nog wat voeten in de aarde. „We hadden als universiteit geen ervaring met handel in bitcoin. Dat hebben we moeten leren." Op de zesde dag van die week, vlak voor Oudjaarsdag, heeft het crisisteam onder leiding van Bos zich in verbinding gesteld met de cybercriminelen en gezegd: wij overwegen te betalen maar we willen zeker weten dat jullie inderdaad de sleutel hebben en dat die werkt. De hackers hebben toen drie 'proef-sleutels' overgedragen, waarmee de universiteit enkele delen van hun systeem konden heropenen. Daarna is het losgeld voldaan en kreeg Bos een 'hele' sleutel.

De nasleep is saillant. De politie slaagde erin een deel van het losgeld te volgen naar een *wallet* in Oekraïne, die „van niemand" was. Het geld daarin is bevroren en dat is uiteindelijk geconfisqueerd. „De politie nam in 2024 contact met ons op. 'We hebben best goed nieuws', zeiden ze. De bitcoins in die wallet waren in de tussenliggende jaren meer waard geworden. Dat was nu een bedrag geworden van om en nabij 500.000 euro." De universiteit heeft van dat geld een fonds ingesteld voor studenten en wetenschappers in nood.

Denk niet dat we dus 'winst' hebben gemaakt, zegt Bos. De kosten die aan die crisisweek verbonden zijn, aan alle mensen die in vakantietijd moesten werken, de externe adviseurs en aan een rapport dat de universiteit aan een ander team van Fox-IT had gevraagd te maken – in het kader van de publieke verantwoording – liggen vele malen hoger dan de bitcoin-winst.

ShinyHunters

Omvang van het Odido-lek groeit

De hackers van ShinyHunters hebben sinds vrijdag gevoelige gegevens van zeker 600.000 particuliere Odido-klanten gepubliceerd. Dat blijkt uit een analyse van de gehackte bestanden door *NRC*.

Welke data precies uitgelekt zijn, verschilt van klant tot klant. Van zeker de helft van de particuliere klanten gaat het in ieder geval om naam, adres en het bankrekeningnummer dat via de dark web-site van de hackers te downloaden is. De gepubliceerde bestanden bevatten ook opmerkingen van klantenservicemedewerkers van Odido. Die aantekeningen bevatten dikwijls e-mailadressen en telefoonnummers van de klanten. Ook worden soms persoonlijke opmerkingen gemaakt, bijvoorbeeld over betalingsregelingen.

Tot nog toe heeft ShinyHunters twee bestanden met een miljoen rijen klantgegevens gepubliceerd – circa een derde van de data bevat betalingsgegevens. ShinyHunters zegt de komende tijd sneller en meer gevoelige data te publiceren.

NRC downloadde en analyseerde de gehackte bestanden om vast te stellen wat de impact van het lek was.

Rik Wassens