Cindy Smeulders
Country Manager Belgium
Northwave Cybersecurity

Die ransomware-aanval was een goede, maar dure les

Hoe beleef je als CFO een gesofisticeerde ransomware-aanval die het hele bedrijf platlegt? Welke lessen kun je eruit trekken? En hoe zorg je ervoor dat zoiets nooit meer gebeurt?

Mark Oosterlinck, financieel topman van het bedrijf TVH, wil erover praten, samen met Cindy Smeulders, Country Manager Belgium van cybersecurity-specialist Northwave. “Staan we er vandaag beter voor dan een jaar geleden? Ja. Maar maak ik mij er nog zorgen over? Ook ja.

Het beloofde een fijne, landerige zondagochtend te worden voor Mark Oosterlinck, maar een bende Russische cybercriminelen stuurde 19 mei 2023 een heel andere richting uit. In de nacht daarvoor hadden ze de interne IT-systemen van het bedrijf TVH in Waregem (België), waarvan Oosterlinck CFO is, platgelegd en versleuteld. De impact van die actie was gigantisch, want TVH is bepaald geen kmo’tje. Het bedrijf distribueert onderdelen van industriële machines en boekt een omzet van zo’n 1,6 miljard euro. Het is actief in 90 afdelingen wereldwijd en heeft zo’n 5.000 mensen op de loonlijst.

Neem ons eens terug mee naar die dag. Hoe kreeg u het nieuws te horen?

Mark: “Ik was thuis en kreeg telefoon van onze IT-directeur. Hij vroeg of wij als onderdeel van onze cyberverzekering gebruik konden maken van een first response van een beveiliger. Dat was nodig, zei hij, want we hadden ‘een probleem’. Ik vroeg nog: ziet het er oké uit of niet? En hij antwoordde: het ziet er niet oké uit, het ziet er zelfs slecht uit. Alles lag plat, we konden quasi niks meer doen.”

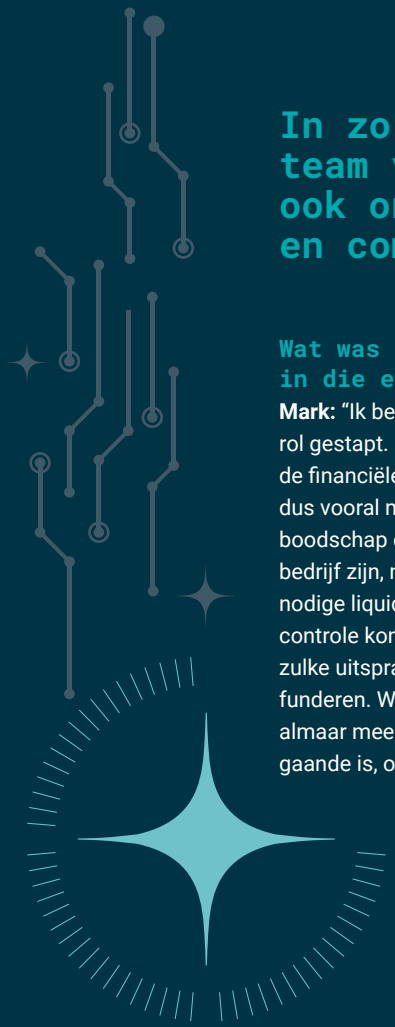
Op dat moment wist nog bijna niemand wat er gaande was?

Mark: “Nee, enkel ik, de CIO en de CEO waren op de hoogte. Voordat we breder gingen communiceren, wilden we eerst goed weten wat er aan de hand was. Een klein team van interne mensen en onze monitoring, die toen extern was, heeft geprobeerd om de aanval in kaart te brengen. En het bredere management is dan gaan kijken wat dit nu betekende. Het was snel duidelijk dat we externe hulp nodig hadden. Op maandagochtend hebben we verschillende cybersecurity-partijen gecontacteerd, waaronder Northwave, en 24 uur later stond Northwave hier met een groot multidisciplinair team.”

Die snelheid is cruciaal, allicht?

Mark: “Absoluut, al hadden we misschien beter op voorhand al wel een soort contingency contract met hen afgesloten. Zodat ze het bedrijf, de procedures en de mensen al kennen op het moment dat zich iets voordoet.”

Cindy: “Wij moesten heel het bedrijf nog leren kennen, inderdaad. Maar we zijn dat gewend en dat is eigenlijk heel vlot verlopen. Als wij in een bedrijf komen in zo’n situatie, is dat niet alleen met technische experts, maar ook met onderhandelaars, crisismanagers en communicatie-experts. Als het nodig is, kunnen wij zelfs een psycholoog meesturen voor de mentale ondersteuning van zowel de klant als onze eigen mensen. Want er heerst soms wel wat paniek en chaos op die momenten.”



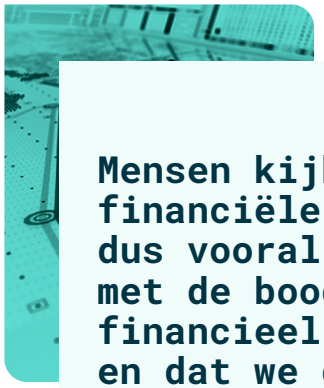
In zo’n crisissituatie komt een team van technische experts, maar ook onderhandelaars, crisismanagers en communicatie-experts.

Wat was uw rol in die eerste dagen?

Mark: “Ik ben wat meer buiten de financiële rol gestapt. Mensen kijken naar de CFO als de financiële guardian, zeg maar. Ik wilde dus vooral mensen geruststellen met de boodschap dat we een financieel gezond bedrijf zijn, met de nodige buffers en de nodige liquiditeiten, en dat we dit onder controle konden krijgen. Pas op, je moet zulke uitspraken natuurlijk wel kunnen funderen. Want uiteindelijk komen ook almaar meer mensen te weten dat er iets gaande is, ook de pers bijvoorbeeld.”

Finaal heeft het bedrijf bijna een maand stilgelegen. Dat is niet niks.

Mark: “Inderdaad, dat is een hele maand zonder omzet, terwijl de kosten gewoon doorlopen. Wat betreft impact en risico is het voor het hele bedrijf dus wel een serieuze eyeopener geweest. Het heeft ook, en dat is wel opmerkelijk, een soort samenhorigheid gecreëerd onder de medewerkers. Veel mensen hebben wel het gevoel dat we hier sterker uitgekomen zijn. We hebben er ook altijd vrij open over gecommuniceerd.”



Mensen kijken naar de CFO als de financiële guardian. Ik wilde dus vooral mensen geruststellen met de boodschap dat we een financieel gezond bedrijf zijn en dat we dit onder controle konden krijgen.

Cindy, nog even over die communicatiespecialisten die jullie meesturen, wat doen die precies?

Cindy: "Zij geven vooral advies over hoe te communiceren, zowel intern als extern. In sommige gevallen kunnen we hen bijvoorbeeld de volledige sociale media van het bedrijf laten overnemen, uiteraard altijd wel in samenspraak met het management."

Mark: "Goede communicatie is een must, maar je moet daar ook mee opletten. Je wilt met wat je communiceert niet de hackers in de kaart spelen. Als wij onthullen hoeveel het ons kost als ons bedrijf een dag niet draait, dan zullen zij extra gemotiveerd zijn. Uiteindelijk hebben we daar pas later over gepraat."

En hoeveel was het, als ik vragen mag?

Mark: "Het totale omzetverlies lag tussen de 85 en 100 miljoen euro, een beetje afhankelijk van hoe je meet en wat je baseline is. Maar in elk geval dus wel een stevig bedrag."

Was dit nu een typisch dossier voor Northwave?

Cindy: "Ja, toch wel. We doen veel kleinere incidenten, maar ook best wel vaak heel grote. We weten hoe we zo'n aanval moeten aanpakken en hoe het bedrijf opnieuw zijn basisdoelstellingen kan bereiken. Die ervaring en expertise is er, want we handelen meer dan 100 serieuze incidenten per jaar af. Mensen schrikken vaak van dat getal."

Kijken jullie nu anders aan tegen cybersecurity, na dit incident?

Mark: "Het is zeker niet zo dat we er voordien totaal geen aandacht voor hadden of dat het iets was dat we minimaliseerden. Maar het heeft er natuurlijk wel voor gezorgd dat we nu een nog grotere en nog snellere inhaalbeweging hebben gemaakt en dat de lat nog hoger ligt. Het was ook makkelijker om die lat hoger te leggen, want niemand moest nog overtuigd worden. Om een idee te geven: we hadden voordien een plan voor multi-factor authentication. We hadden daar een termijn van drie maanden voor uitgetrokken. Uiteindelijk hebben we dat op anderhalve dag ingevoerd. Iedereen wou die inspanning wel doen. We passen nu ook veel regelmatiger wachtwoorden aan, we houden meer phishing-campagnes, er zijn verplichte trainingen, … We leren de reflexen intensiever aan.

Het gaat ook over meer dan het technische aspect. We denken meer na over wat we kunnen doen als er iets gebeurt. Een zeker mate van improvisatie zal er altijd zijn, maar hoe beter de voorbereiding, hoe beperkter de schade. Als ons dit vandaag zou overkomen, denk ik dat de downtime geen maand maar slechts een paar dagen is."

Een zeker mate van improvisatie zal er altijd zijn, maar hoe beter de voorbereiding, hoe beperkter de schade.

Praat u soms met andere CFO's over wat er gebeurd is?

Mark: "Ja, toch wel. En dan pas merk ik hoeveel collega's er zijn die al iets vergelijkbaars hebben meegemaakt. We kunnen bijna een slachtoffervereniging oprichten (lacht). En de meest gestelde vraag is natuurlijk: hebben we de hackers betaald?" (Officieel wil TVH hier niets over kwijt, maar het hackerscollectief Lockbit gaf op zijn website zelf aan dat er niét betaald werd, nvdr.)

Heeft dit binnen het bedrijf nu een cultuuromslag teweeggebracht?

Cindy: "In sommige ondernemingen zie je soms dat mensen bang zijn om te zeggen dat ze op een verdachte link geklikt hebben. Dat is niet de juiste reflex. Er moet een cultuur bestaan waarin mensen mogen falen en toegeven dat ze iets verkeerd gedaan hebben, zonder dat daar gigantische consequenties aan verbonden zijn."

Mark: "Ik denk dat dat voor TVH wel opgaat. We hebben bijvoorbeeld een centraal meldpunt waar medewerkers een verdachte mail naartoe mogen sturen. In plaats van zelf detective te gaan spelen."

Er moet een cultuur bestaan waarin mensen mogen toegeven dat ze iets verkeerd gedaan hebben.

Cindy: "Voor ons als Northwave ligt daar ook een taak. De meeste mensen weten ondertussen wel wat phishing en cybersecurity is, maar vanuit Northwave zorgen we voor een transitie van awareness naar cybersafe behaviour, zoals inderdaad bijvoorbeeld meldingen doen van verdachte zaken zoals phishing."

Mark Oosterlinck
CFO, TVH Parts Holding NV

Hoe betrokken is de board vandaag bij cybersecurity?

Mark: "Zéér betrokken. In de periode van de aanval was de board quasi dagelijks in contact met het management, maar sindsdien is dat ook een topic waarover we heel regelmatig rapporteren. We laten ons benchmarken door twee partijen , waaronder Norhtwave en die scoren ons op NIST (cybersecurity framework, nvdr.) en daar zijn ook zowel relatieve als tijdsgebonden doelen aan verbonden."

Cindy: "Is er binnen de board een specifieke verantwoordelijke voor cybersecurity?"

Mark: "Nee, bij ons wordt dat voornamelijk in het auditcomité bekeken. Daar is een delegatie van de board die er dieper op ingaat. We hebben ook een cybercomité binnen het management met de CEO, CIO en CFO, en onze cyber- en risk directors."

Er is ook de gedeelde verantwoordelijkheid rond business continuity: wat doen we op een moment dat we in een crisis zitten en hoe zorgen we ervoor dat we uit die crisis geraken?

Cindy: "En hoe verloopt de communicatie tussen de cybersecurity-mensen en de board? Ik kan me namelijk voorstellen dat zij twee aparte doelstellingen hebben. De ene focust op cybersecurity, de andere wil het bedrijf draaiende houden."

Mark: "Die communicatie verloopt zeer transparant. Ik zie daar ook geen tegenstelling in. Niemand wil dit nog meemaken en zeker niet op deze schaal. Het enige verschil met de periode voor het incident is misschien dat dit vroeger wat meer ver-van-mijn-bed was. Men bekeek cybersecurity als iets zeer technisch: een muur bouwen om te zorgen dat hackers niet binnenkomen. Maar er is ook de gedeelde verantwoordelijkheid rond business continuity: wat doen we op een moment dat we in een crisis zitten en hoe zorgen we ervoor dat we uit die crisis geraken? Die veerkracht aankweken is goed voor cyberincidenten, maar in principe voor eender welk incident, denk aan een brand of een storm."

Kan of mag je ervan uitgaan dat TVH heel gericht en doelbewust in het vizier werd genomen?

Cindy: “Meestal niet. Het is niet zo dat hackers De Tijd lezen en de lijstjes van grootste bedrijven van België afgaan. Het is meestal willekeurig gekozen. Voor die hackers is dit gewoon een business om geld te verdienen. Vroeger waren dat heel losse groepen of enkelingen, nu zijn die heel georganiseerd en gestructureerd. Er zijn mensen die zich specifiek bezighouden met het zoeken naar toegang, die toegang wordt doorverkocht aan een volgende groep, die gaat dan een aanval ‘inhuren’ bij een ransomware-ontwikkelaar en die voert de aanval uit. Sommige groepen hebben ook een hulplijn: als het niet lukt om de ransomware te installeren, zullen ze je helpen. Het is puur business.”

Gebeurt het eigenlijk dat een bedrijf twee keer wordt aangevallen?

Cindy: “Niet vaak, maar het gebeurt zeker wel. We hebben al klanten gehad die een incident zelf afhandelden door gewoon een backup terug te zetten, maar zonder te weten waar het lek zat. Dan wordt die toegang gewoon doorverkocht aan een andere ransomware-groep en kun je drie maanden later opnieuw worden aangevallen. Het belangrijkste tijdens het afhandelen van een incident is dat we te weten komen waar de hackers zijn binnengeraakt en hoe ze het incident hebben veroorzaakt. En terwijl je het bedrijf weer op de rails helpt, moet je dat gat ook dichten.”

We zijn nu een jaar na het incident. Hoe kijken jullie erop terug?

Mark: “Als een goede, maar zéér dure les. We willen het zelf nooit meer meemaken, maar we willen ook dat andere bedrijven hiervan gespaard blijven. Vandaar dat ik het belangrijk vind om erover te praten. Onze case was een vrij grote aanval die ook de media heeft gehaald, maar er zijn evengoed ongelooflijk veel kleinere dossiers waar niemand over spreekt en die ook enorm veel financiële schade aanrichten. Dat zijn allemaal kleine ondernemers die door onbekende criminelen vaak compleet financieel geruïneerd worden.”

We willen het zelf nooit meer meemaken, maar we willen ook dat andere bedrijven hiervan gespaard blijven. Vandaar dat ik het belangrijk vind om erover te praten.

Cindy: “Dat klopt, voor kleinere bedrijven kunnen de gevolgen echt rampzalig zijn. Als je je data kwijt bent en je hebt de cashflow niet om de gijzelaars te betalen, dan is het vaak boeken dicht.”

Wat raden jullie aan: betalen of niet betalen?

Cindy: “Wij gaan bedrijven niet vertellen of ze wel of niet moeten betalen, maar we leggen het C-level een aantal keuzes voor gebaseerd op de beschikbare herstelcapaciteit en de gevoeligheid van de gestolen data. Dat is geheel afhankelijk van het bedrijf zelf. Als je betaalt, mag je er wel redelijkerwijs van uitgaan dat je je data terugkrijgt. Dat is deel van het businessmodel.”

Mark: “Ik denk dat daar twee aspecten rond zijn: de ethische vraag en de praktische vraag. De ethische vraag is: wil je een crimineel betalen? Dat is een moeilijke afweging, die wij uiteindelijk niet hebben moeten maken. En dan is er natuurlijk ook de praktische vraag. Ik heb die bewuste zondagochtend ook even gedacht: als ik er met een niet al te groot bedrag vanaf kom, dan heb ik de sleutel en kan ik weer verder. Maar zo werkt het niet. Decrypteren duurt sowieso veel langer dan een back-up terugzetten en bovendien: ook al betaal je, je weet nooit zeker wat je terugkrijgt. Dus daar speelt ook weer het belang van die business continuity en ervoor zorgen dat je vanuit je eigen veerkracht weer verder kunt.”

Er zijn twee aspecten: de ethische vraag en de praktische vraag.

Denkt u dat jullie vandaag beter gewapend zijn en een betere grip hebben op IT-security?

Mark: “Ja, dat denk ik wel. We staan er vandaag beter voor dan een jaar geleden. Maak ik mij er nog altijd zorgen over? Dat ook, omdat het zo’n potentiële impact heeft. Het is niet dat ik er slecht van slaap, maar het speelt toch altijd ergens in het achterhoofd mee. Los van de schade aan het bedrijf waren het ook zeer intense weken. Je zit eigenlijk 24/7 op een soort rollercoaster. En niet bepaald de meest prettige.”

Om af te sluiten: welke drie tips zou u uw collega’s willen meegeven?

Mark: “De eerste ligt voor de hand: hou je IT-systeem in topvorm, en zorg dat je beveiliging en back-ups in orde zijn. De tweede is: weet wie je gaat bellen als je gehackt bent. Als je op dat moment nog die keuze moet maken, verlies je kostbare uren, dagen zelfs. En ten derde: maak binnen je team afspraken over wie wat doet als het ondenkbare gebeurt. Er zullen heel veel mensen zijn die op dat moment willen helpen, maar je kunt maar met een beperkt aantal effectief iets doen.”

Cindy: “Dat zijn inderdaad ook de dingen die wij in ons Rapid Response-programma vastleggen en die we elk jaar ook opnieuw trainen. Dus: uitstekende tips (lacht).”

Northwave was partner van de CFO Day 2024 by House of Executives.

Would you like us to assist you on your journey towards cyber resilience and NIS2 readiness? You can reach us at:

NORTHWAVE
CYBER SECURITY

E: info@northwave-cybersecurity.com
T: +31 (0) 30 303 1240
W: www.northwave-cybersecurity.com