22

VERLIES DE CONTROLE NIET

BUSINESS CONTINUÏTEITSPLAN HELPT IN VOORBEREIDING OP CYBERAANVAL

Recentelijk werd het webinar met de titel ‘Gehackt? Een effectief stappenplan van paniek naar productie’ georganiseerd door ACA IT-Solutions, een dochteronderneming van Crowe Foederer accountants & advies. De aanwezigen vernamen dat het verstandig is om proactief in de strijd tegen cybercriminelen een business continuïteitsplan op te stellen. Net zoals ondernemingen dat doen voor brand, waterschade of andere calamiteiten.

GEERT RADEMAKERS

Stel in de strijd tegen cybercriminelen een business continuïteitsplan op.

“Als je de kansen op een rij zet, dan is de kans om slachtoffer te worden van cybercriminaliteit veel hoger dan andere risico’s voor de bedrijfscontinuïteit”, stelde Geert Rademakers, directeur van ACA IT-Solutions. “Feit is dat twee op de vijf bedrijven tegenwoordig te maken krijgen met enige vorm van cybercriminaliteit. Als u niets voorbereidt, dan bent u tijdens en na een hack aan de cybercriminelen overgeleverd. Betalen en hopen op teruggaaf van bestanden is dan nog de enige remedie.” Een goede voorbereiding voorkomt paniek, concludeert Rademakers. Dat voorbereiden zit dan vooral in het vooraf opstellen van een business continuïteitsplan. Net zoals dat gebeurt voor andere calamiteiten. “Wij zien vaak dat er chaos en paniek uitbreekt bij ondernemingen die worden geraakt en die niet zijn voorbereid. Dan verlies je de controle.”

HOE DENK JE TE HERSTELLEN?

Met een goede voorbereiding is veel te ondervangen. Rademakers: “Maak van tevoren een plan over hoe je denkt te herstellen, wat de prioriteiten zijn, welke processen beslist door moeten draaien en welke applicaties snel up and running moeten zijn.” Rademakers legde vervolgens uit hoe het kan dat cybercriminaliteit zo’n opmars maakt. “De digitale transformatie maakt ons afhankelijk van ICT. De cloud, de moderne werkplek en het feit dat we altijd online zijn, vergroten het aanvalsvlak. Daarbij komt dat misdadigers buiten schot kunnen blijven van autoriteiten en op afstand via crypto’s hun geld kunnen verdienen. Waren tien jaar geleden alleen corporates interessant voor hackers, ze richten hun pijlen nu op het mkb. Ook omdat ze bijvoorbeeld geautomatiseerd aanvallen kunnen uitvoeren op veel bedrijven naar aanleiding van een kwetsbaarheid. Om zo te kijken of ze beet kunnen krijgen bij bedrijven die niets tegen die kwetsbaarheid hebben gedaan.”

WAT IS ER AAN DE HAND?

“Iets of iemand constateert dat er iets niet goed is”, vertelt Rademakers over het begin van een hack. “Maar wat is dat? Als eerste moet je proberen vast te stellen wat er aan de hand is. Is het al gebeurd of is het nog steeds gaande? Is er een hacker bij betrokken of vond de aanval volledig automatisch plaats? En: wat is eigenlijk precies de impact? Belangrijk is om, als niets meer werkt, een uitwijkmogelijkheid te hebben. Want hoe draait je bedrijf anders verder? Daarnaast is interne en externe communicatie belangrijk, om geruchten onder controle te houden en realistische verwachtingen te managen. Denk aan communicatie naar medewerkers, klanten, leveranciers, partners en de pers. Dat soort zaken kun je niet oppakken zonder voorbereiding en een plan waarmee je ook geoefend hebt. Je zult dus een crisisteam en ook externe hulp in moeten schakelen. Die externe hulp kan lopen via je cybersecurityverzekering waar die hulp soms al meeverzekerd is. Daarnaast horen je sleutelfunctionarissen in het crisisteam 24 uur, 7 dagen in de week bereikbaar te zijn. En eigenlijk is er niet één crisisteam, maar een driehoek van drie teams.”

UITWIJKEN OF NIET?

Daar ging cybersecurityspecialist Maarten de Rooij op verder. De aanpak van cybersecurity kent drie teams. Eén voor crisisregie, één voor communicatie en één voor het oplossen van het probleem. “Vanuit de crisisregie maak je als organisatie je bedrijfsnoodplan en weeg je af hoe ernstig de situatie is. Moet je naar een volgende fase opschalen? Hier wordt ook de afweging gemaakt of je wel of niet moet uitwijken met de ICT-infrastructuur. Bij het team voor de probleemoplossing schatten de leden in wat de impact is op de organisatie, schatten ze de hersteltijd in, zoeken ze naar oplossingen voor de hack en realiseren ze daadwerkelijk het uitwijken naar een andere ICT-infrastructuur. Het team communicatie houdt zich bezig met informatieverstrekking over de situatie naar alle belanghebbenden. Denk aan informatie over de verwachte hersteltijd en over tijdelijke oplossingen. Hier vindt ook, als dat nodig is, communicatie met de pers plaats die wellicht lucht heeft gekregen van de precaire situatie.”

UIT EEN DIEP DAL KOMEN

“Je weet pas wat je moet doen als je ook weet wat er heeft plaatsgevonden”, reageert Rademakers. “Dat gaat over forensisch onderzoek. Onderzoekers bepalen daarbij hoe de hack heeft plaatsgevonden, welke systemen zijn geraakt en of er data zijn ontvreemd die gepubliceerd kunnen worden. Daarnaast is het de kunst om te bepalen in hoeverre je als organisatie afhankelijk bent van de cybercriminelen. Is het antwoord ‘ja, helemaal afhankelijk’ dan moet er contact worden opgenomen met de hackers. Voor de onderhandeling over losgeld voor dataherstel of onderhandeling voor het voorkomen van exposure van je data.” Na de vaststellingsfase moet de organisatie uit een diep dal komen. De Rooij: “Als je weet hoe ze zijn binnengekomen en wat is geraakt, kun je ook kijken wat er aan ICT-infrastructuur is gecompromitteerd. En kun je kijken van welk punt je waar nog een back-up hebt, of deze bruikbaar is en of je moet uitwijken met delen van of je gehele ICT-infrastructuur. Alles wat je hebt voorbereid, levert op dit punt tijdswinst op.”

BEDRIJFSKRITISCHE PROCESSEN

“Kunnen je systemen en data hersteld worden? Kunnen data worden gewassen?” vervolgt De Rooij. “Let wel op, vaak zorgen hackers ervoor dat ze de back-up ook infecteren. Daarnaast is het opbouwen van een ICT-infrastructuur op een uitwijkmogelijkheid een flinke klus. Denk aan het opbouwen van nieuwe rechten, profielen en user databases. Het uitfaseren van oude systemen en overstappen duurt al snel één of twee weken.” Rademakers: “Medewerkers hebben de neiging om de stekker van servers eruit te trekken als zo’n hack bezig is, maar daardoor ben je niet geholpen. Het hindert zelfs het forensisch onderzoek.” De Rooij raadt ook aan in een business continuïteitsplan vast te leggen wat bedrijfskritische processen zijn en welke niet of minder essentieel. “Dat doe je in een business impact analyse, oftewel BIA. Als bijvoorbeeld een HR-systeem eruit ligt, is dat vervelend, maar het kan zijn dat je twee weken zonder kunt. Maar je kunt niet zonder software die je productie aanstuurt. Zonder productie zou je failliet kunnen gaan.”

RPO EN RTO

Ook kan een organisatie in het business continuïteitsplan aangeven wat de RPO en RTO zijn. De Rooij: “RPO staat voor Recovery Point Objective. Dit houdt in dat je een bepaalde mate van dataverlies accepteert bij een grootschalige storing. RTO staat voor Recovery Time Objective. Dit betreft de tijd dat het systeem na de storing weer beschikbaar moet zijn. 24 uur of 48 uur of meer? In het plan zitten ook de bedreigingen en kwetsbaarheden die een gevaar vormen voor je organisatie. Dit zit in een BKA: Bedreigingen Kwetsbaarheden Analyse. Ook ga je na welke gevolgschade kan ontstaan na een hack, kijkend naar de resultaten van de BIA en de BKA. Daar maak je scenario’s voor, waarbij je ook kijkt of je die scenario’s kunt voorkomen of stoppen. Aansluitend bezie je of je een bepaald risico moet accepteren of wellicht onderbrengen bij een cyber security-verzekering.”

VAN PLAN NAAR PRAKTIJK

Nadat de plannen zijn gemaakt en de randvoorwaarden zijn vastgesteld, is het zaak om het plan in praktijk te brengen. Worden back-ups gemaakt zoals in het plan is bepaald? Verloopt een uitwijktest zoals het is bedacht? Is de IT-omgeving dusdanig ingericht dat de gewenste RPO en RTO ook daadwerkelijk gehaald kunnen worden? Het is de taak van de beleidsmakers en het IT-management om samen het plan in praktijk te brengen en te houden.

PLAN UP TO DATE HOUDEN

Rademakers hamert op het feit dat het business continuïteitsplan up-to-date moet worden gehouden. “Niets is vervelender dan er pas bij een crisis achter-

MAARTEN DE ROOIJ

Kunnen je systemen en data hersteld worden?

MICHAEL WATERMAN

Je bent zelf verantwoordelijk voor jouw data.

komen dat de ICT-infrastructuur toch anders is dan in het plan staat vermeld. Daarnaast moet je regelmatig met het plan oefenen om verbeteringen te kunnen aanbrengen." De Rooij: "Inderdaad, je moet dit aandacht blijven geven." Rademakers: "Feitelijk komt het erop neer dat je telkens drempels opwerpt voor hackers. Zie het als een escape room. Hoe meer kamers er in de ICT-infrastructuur zitten, hoe moeilijker het is eruit te komen. Zo is het voor de hackers ook. Dat maakt het moeilijker om schade te berokkenen." Rademakers noemt immutable storage en storage snaphots als technische mogelijkheden. Een immutabele back-up of opslag betekent dat de gegevens vastliggen, onveranderlijk zijn en nooit kunnen worden gewist. Storage snaphots zijn een momentopname die de toestand van een systeem op een bepaald tijdstip weergeven. "Dit soort oplossingen helpt."

CLOUD MINDER GEVOELIG

Rademakers en De Rooij, maar ook Michael Waterman, Manager Cybersecurity Team, behandelden achteraf vragen van de deelnemers. De eerste vraag: zijn cloudapplicaties minder gevoelig voor een hack? Rademakers: "Ja, in principe wel, maar het blijven applicaties. Een cloudleverancier kan ook getroffen worden." Waterman: "Let wel, de cloudleverancier is niet verantwoordelijk voor jouw data, dat ben je altijd nog zelf. Bijvoorbeeld of je je tweewegauthenticatie niet hebt aanstaan. Ga in gesprek met je leverancier over hoe de cybersecurity is geregeld en wie waarvoor verantwoordelijk is. Laat ze aantonen wat ze eraan doen." Rademakers wijst op de kosten voor forensisch onderzoek. Waterman: "Het zijn echte specialisten die jarenlang ervaring hebben. Daarbij moet je denken aan tarieven die je ook hebt in de advocatuur."

Wat heeft Waterman van hacks geleerd, wil een deelnemer weten. "De intensiteit van zo'n periode is enorm. Niet alleen je reguliere medewerkers, maar ook ICT'ers komen zwaar onder druk te staan. Daarbij komt dat medewerkers goed geïnformeerd moeten worden omdat ze tal van vragen hebben. Gaat het bedrijf wel door? Heb ik nog wel een baan? Enzovoorts. Die paniek en chaos moet je zien te voorkomen. Door je goed voor te bereiden."

Dit artikel is tot stand gekomen met medewerking van Crowe Foederer.

SRA helpt u graag

ENKELE PRAKTISCHE TIPS

Naast het hebben van een business continuïteitsplan is er een aantal zaken die continu aandacht behoeven.

AWARENESS

Zorg ervoor dat medewerkers bewust worden en blijven van de risico's van cybercriminaliteit. Doe dit ten minste vier keer per jaar. Denk hierbij aan (online) trainingen, workshops en phishingsimulatie.

WACHTWOORDEN

Zorg voor goede wachtwoorden en stel multifactorauthenticatie verplicht, tenzij dit niet mogelijk is. Doe dit ook voor socialmedia-accounts.

BACK-UP EN RECOVERY

Zorg voor een goede back-up strategie en test periodiek de werking van de back-up (recoverytest).

SRA helpt u graag. Op www.sra.nl/it-diensten vindt u meer informatie.