Wow-factor: “We zullen aan cyber-aanvallen moeten wennen”

11-04-2023 07:00

Vertel eens iets over jezelf en wat jij de afgelopen jaren hebt gedaan?

Ik ben inmiddels ruim 20 jaar getrouwd en met 2 fantastische kinderen voel ik me gezegend. Uiteraard mogen de hond en 2 katten daar niet in ontbreken. Privé staat mijn leven met name in het teken van tennis. Ik speel als sinds jaar en dag competitie en in de zomer allerlei toernooien. Dat doe ik niet alleen voor de sportieve prestatie, maar ook voor de gezelligheid. Daarnaast kun je me (zowel zakelijk als privé) altijd wakker maken voor een vliegreis. Zakelijk heb ik voor allerlei bedrijven gewerkt, altijd in de ICT, en de laatste 10 – 15 jaar specifiek in de cybersecurity. In deze jaren heb ik een enorme verscheidenheid aan projecten in binnen- en buitenland kunnen doen met de Talox tools die we hebben ontwikkeld.

Hoe was voor jou de afgelopen Covid-periode?

De periode van Covid was voor mij een periode van nieuwe uitdagingen en een groot persoonlijk verlies. Na de verkoop van mijn bedrijf (Digital Investigation) ben ik, op interim-basis, begin 2020 gestart met een nieuwe uitdaging bij een groot Fins security bedrijf. Als gevolg van reorganisaties ten gevolge van Covid duurde dit avontuur ‘slechts’ ¾ jaar. In deze periode ben ik mijn vader, na een langdurig ziekte bed (ziekte van Alzheimer), verloren.

De combinatie van uitdagingen die het nieuwe thuiswerken met zich meebracht op het gebied van cyber, het feit dat ik voor een derde keer een keuze ‘moest’ maken welke kant ik in professionele zin op wilde en het

besef dat het leven vergankelijk is, heeft me uiteindelijk doen besluiten om mijn hart (en passie) weer te gaan volgen. Het resultaat hiervan is de oprichting van Talox geweest. Talox is mijn huidige cybersecurity-bedrijf dat ik heb opgericht met als doel het MKB weerbaarder te maken tegen aanvallen van cybercriminelen.

Cyber-aanvallen zijn momenteel hot news. Wat is er aan de hand?

Ik ben bang dat we zullen moeten gaan wennen aan cyberaanvallen in het nieuws. Cyberaanvallen zullen nooit meer verdwijnen en zullen de komende jaren alleen maar in aantal toenemen. Dit is een logisch gevolg van de beschikbaarheid van tools op het internet die op zeer eenvoudige wijze, tegen lage kosten en zelfs met gebruikers-ondersteuning te koop zijn. De combinatie met de zeer lage pakkans en de hoge opbrengst zorgt er bovendien voor dat de afgelopen twee decennia een heel ecosysteem is ontstaan van aanbieders van tools, kopers van malware en een enorm aantal individuen en professionele groeperingen die veel geld verdienen aan cybercriminaliteit.

Hoe kunnen bedrijven een cyber-aanval voorkomen?

Cybercrimininaliteit is – ben ik bang – eigenlijk nooit helemaal te voorkomen. Wel kun je veel doen op het gebied van preventie. Heel algemeen gaat het hierbij eigenlijk over bewustzijn, ofwel awareness. Maar dan wel over awareness in het hele bedrijf. Awareness stopt in mijn ogen niet bij het aanbieden van trainingen en informeren van medewerkers, maar vraagt ook awareness bij het management. Bij die laatste groep zouden vooral drie dingen duidelijk moeten zijn. Ten eerste dat er maatregelen nodig zijn om incidenten te voorkomen. Denk hierbij aan MFA (multifactor authentication), inzet van virusscanners en firewalls, maar ook aan beleid (en tooling) voor het gebruik van wachtwoorden. Ten tweede het besef dat het een feit is dat het een keer mis zal gaan. En ten derde dat er nagedacht moet zijn over wat je doet als je daadwerkelijk geconfronteerd wordt met een cyber-incident.

Vertel eens iets over wachtwoorden in het algemeen? Hoe lang en hoeveel tekens moet het minimaal bevatten?

Het antwoord ten aanzien van wachtwoorden is eigenlijk heel simpel. Letterlijk zouden wachtwoorden zo lang mogelijk moeten zijn, minimaal 12 karakters en liever nog 15 (en dan ook nog zonder structuur). Daarbij moeten ze op alle plekken waar je wachtwoorden gebruikt ook nog verschillend zijn. In de praktijk – veel mensen hebben tientallen, zo niet meer dan honderd plekken waar ze wachtwoorden gebruiken – is dit natuurlijk niet te doen. Daarom adviseren wij hiervoor een wachtwoordmanager te gebruiken. Het is goed om dit als organisatie voor je medewerkers te faciliteren. Naast het gebruik van sterke wachtwoorden is een MFA/2FA een heel goed middel om incidenten met misbruik van wachtwoorden te voorkomen.

Wat moet je niet doen met je zakelijk laptop als je extern werkt?

Het belangrijkste om niet te doen, is gebruik maken van openbare wifi. Dit geldt uiteraard voor de trein en bijvoorbeeld de Mc Donalds, maar ook voor hotels of andere (semi) openbare gelegenheden. Het feit dat hierbij soms wel gebruik gemaakt wordt van een wachtwoord is eigenlijk een wassenneus omdat dit wachtwoord nooit veranderd wordt en dus voor iedereen en dus ook voor de cybercrimineel, veelal letterlijk zichtbaar is. Criminelen zijn, als ze zich op datzelfde netwerk bevinden, of nog erger als ze een netwerk hebben opgezet waar jij onbewust gebruik van maakt, in staat om alles mee te lezen dat er over internet gaat. Dit gaat veel verder dan inzicht krijgen in welke websites er op dat moment door personen worden bezocht. Ze zijn namelijk ook in staat om bijvoorbeeld gevoelige informatie als wachtwoorden te onderscheppen. Om dit te voorkomen kun je gebruik maken van een zelf opgezette hotspot (4/5G via je telefoon) of door gebruik te maken van een VPN.

Hoe gaan cybercriminelen te werk? Waar starten ze eerst?

Over het algemeen zoeken cybercriminelen de weg van de minste weerstand. In veel gevallen zijn dat de medewerkers van organisaties die door bijvoorbeeld phishing-campagnes verleid worden gegevens achter te laten of te klikken op een linkje. Hierbij geldt ook heel duidelijk dat het schieten met hagel voor de gemiddelde criminele groepering veel meer oplevert dan een gerichte aanval. Deze laatste zijn duurder en complexer uit te voeren. Het in het wilde weg zoeken naar en schieten op kwetsbare machines levert zonder een grote inspanning heel veel op. Dit is dan ook een grote verandering ten opzichte van een jaar of 10 – 15 geleden waarbij cybercriminelen zich met name richtten op grote organisaties waar 'veel' te halen viel. In de huidige tijd richten veel criminelen zich niet meer specifiek op een doel, maar worden – ook kleinere – ondernemingen 'per ongeluk' slachtoffer.

Als je toch gehackt wordt, wat moet je dan doen?

Primair begint het denk ik met het besef dat het een keer gaat gebeuren. Als je er dan voor hebt gezorgd dat je een aanval (het liefst zo snel mogelijk) hebt ontdekt, zorg er dan voor dat je voorbereid bent. In het ideale geval heb je een plan klaarliggen met contactpersonen en scenario's beschreven op basis waarvan acties ondernemen (moeten) worden. Een ander belangrijk element is de aanwezigheid van, geteste, back-ups van de verschillende systemen.

Welk laatste advies wil je de lezers van MIX meegeven?

Mijn advies aan de lezers zou zijn: realiseer je dat je een keer slachtoffer zal worden. Neem daarom maatregelen om incidenten zo veel mogelijk te voorkomen en zorg er daarnaast voor dat je voorbereid bent. Als laatste zou ik, maar dat is natuurlijk een beetje preken voor eigen parochie, een bedrijf als Talox vragen om je te adviseren en misschien ook te ondersteunen met de implementatie van te treffen maatregelen. Daarbij is het mijn oprechte mening dat er voor elke bedrijf met elk budget maatregelen te treffen zijn om zowel het risico als de gevolgen van een incident aanzienlijk te verkleinen.

WOW-factor

Frank Heus heeft een succesvol track-record in dhz-industrie. Wie hem kent, kent zijn drive en zijn enthousiasme. Voor MIX gaat hij – op strikt persoonlijke titel – op zoek naar de WOW-factor. Heus: "Dion Battermann heeft simpele en effectieve oplossingen voor ons allemaal maar heeft ook bij diverse DHZ-bedrijven dieper gekeken en kwam met grote verrassingen waarbij hij binnen 5 seconde alle wachtwoorden had van alle collega's. Voor mij is hij de WOW-man die mensen kan waarschuwen en bedrijven kan helpen om dit voor te zijn."

Redactie