Auteurs: Tom Bakker is redactielid van iB-Magazine. Tom is bereikbaar via tombakker@pvib.nl Sandra Kagie is freelance tekstschrijver (Sanscript tekstproducties). Sandra is bereikbaar via info@sanscriptproducties.nl.

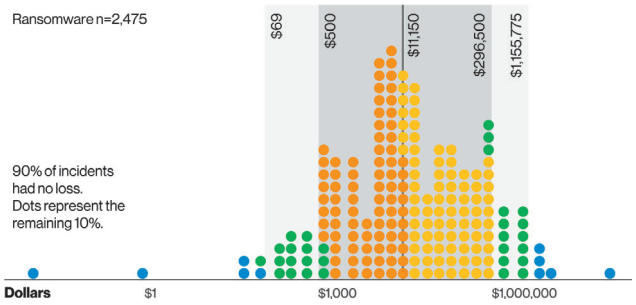
INTERVIEW

Co-auteur Data Breach Investigations Report pleit voor holistische aanpak cybercrime

Op het moment dat we Gabriel Bassett, hoofd data-analist en co-auteur van het in mei gepresenteerde 2021 Data Breach Investigations Report (DBIR) spreken, is ransomware volop in het nieuws. Door een ransomware-aanval op de Amerikaanse software-leverancier Kaseya lagen wereldwijd honderden bedrijven stil. Ook in Nederland werden slachtoffers gemaakt. Termen als 'grootste cyberaanval ooit' domineerden het nieuws. Het geëiste losgeld: 70 miljoen dollar.

Wanneer we Bassett vragen naar het meest positieve nieuws uit het jongste Data Breach Investigations Report (DBIR) verwijst hij direct naar de impact-sectie van het rapport. Daaruit blijkt dat de financiële impact van een ransomware-aanval in veruit de meeste gevallen 'niet exorbitant hoog is', zoals hij het verwoordt.

Hij wijst vervolgens in het rapport op de mediaan van meer dan 11.000 dollar die bedrijven verloren na een ransomeware-aanval. In negentig procent van de gevallen verloren slachtoffers van een ransomware-aanval zelfs helemaal geen geld. "Heel anders dan dat wat we in het nieuws zien", concludeert hij.



Figuur 1 – Verlies per incidenttype. Elke stip vertegenwoordigt 0,5% van de incidenten.

De les die bedrijven uit dit, in zijn ogen, 'goede nieuws' zouden moeten trekken, is dat je als bedrijf kunt dealen met de gevolgen van een ransomware-aanval. "De gevolgen

ervan zijn niet onoverkomelijk. Dit in tegenstelling tot het gevoel dat je zou kunnen krijgen wanneer je berichtgeving over dit type aanvallen in het nieuws volgt."

'Geen Italian job'

"Je kunt als organisatie een fout maken en deze te boven komen", stelt Bassett geruststellend. Aan de andere kant noemt hij het feit dat cybercrime een constante dreiging blijft voor organisaties het slechtste nieuws dat dit keer uit het rapport naar voren komt. "Cybercrime is geen Italian job, maar een business that is here to stay", waarschuwt hij. "Aanvallers hoeven geen experts te zijn, want alles is te koop. Neem ransomware as-a-service. Iedereen die wil, kan ermee aan de slag." Dit maakt volgens Bassett dat elk bedrijf en elke organisatie een potentieel slachtoffer blijft. Ook al denk je 'bij mij valt toch niks te halen'. "Een realiteit waarmee zowel grote als kleine organisaties rekening moeten blijven houden."

"Voor aanvallers is cybercrime nu eenmaal een heel efficiënt businessmodel", waarschuwt Bassett. "Het vergt niet veel investeringen en ze lopen weinig risico. Verdachten slaan immers bij voorkeur toe buiten hun eigen landsgrenzen, wat de opsporing heel moeilijk maakt. Digitaal doen grenzen van landen er niet toe , maar juridisch gezien, als het aankomt op opsporing, is dit een heel ander verhaal. Een tegenstelling die aanvallers in de kaart speelt."

Holistische aanpak

Bassett hoopt dat deze constatering regeringen en bedrijven ertoe aanzet echt na te denken over manieren om dit gunstige businessmodel om zeep te helpen. Vragen die we hiertoe volgens hem gezamenlijk moeten beantwoorden zijn: hoe maken we het businessmodel achter cybercrime minder efficiënt? Hoe verhogen we de drempel zodat het moeilijker is voor aanvallers om zich op het cybercrimepad te begeven? En hoe vergroten we het risico voor aanvallers dat ze gepakt worden? In het verlengde hiervan hoopt Bassett dat het belangrijkste nieuws uit het rapport van volgend jaar zal zijn dat de securitygemeenschap erin is geslaagd cybercriminelen op een 'holistische manier' aan te pakken. "Dat zou ik heel graag opschrijven in het DBIR 2022", geeft hij aan wanneer we hem naar de door hem gewenste headline van dat volgende rapport vragen.
"Dat het ons gezamenlijk is gelukt meer bedrijven en organisaties weerbaar te maken tegen cybercrime aan de ene kant en dat we er aan de andere kant voor hebben weten te zorgen dat cybercrime voor aanvallers minder economisch interessant is geworden en méér risicovol."

Kat-en-muisspel

Wat deze gewenste aanpak betreft zou de securitygemeenschap volgens hem een voorbeeld moeten nemen aan fraudebestrijders. "Die denken niet: wanneer komt er nu eens een eind aan fraude. Het is een kat-en-muisspel en dat

2021 DBIR: de achtergrond

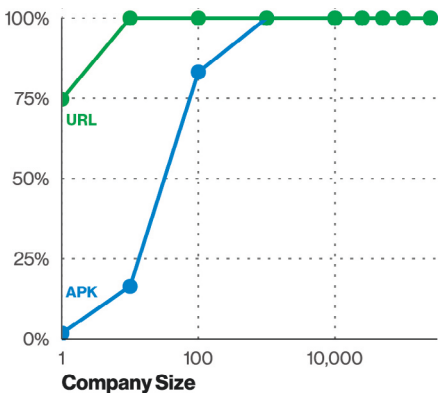
Om te komen tot het 2021 DBIR, alweer de 14e editie van het jaarlijkse onderzoek, heeft een team van analisten, onder wie Gabriel Bassett, 79.635 aan security gelinkte incidenten bekeken. Hiervan bleek het in 29.207 gevallen te gaan om veiligheidsincidenten, waarvan 5.258 bevestigde datalekken. Ter vergelijking: vorig jaar analyseerden ze 3.950 datalekken.
Wie zijn de slachtoffers? Wie zit er achter de cyberaanvallen? Welke tactieken gebruiken cybercriminelen? Slechts een aantal van de vragen die de onderzoekers ook dit jaar in het rapport beantwoorden. Want, zo stellen zij: 'The more you know about the threats you face, the better your chances of keeping your data secure and your name out of the headlines.'
Dit keer is het DBIR gebaseerd op het onderzoek van incidenten afkomstig van 83 bijdragers uit 88 landen. En in het rapport wordt een uitsplitsing gemaakt in elf sectoren, waaronder: de financiële sector, de gezondheidszorg, het onderwijs, de retail en de maakindustrie. Ook wordt een grove regionale analyse gemaakt. Hierbij worden Europa, het Midden-Oosten en Afrika als één regio beschouwd (EMEA).

Benieuwd wat de bevindingen zijn van de onderzoekers over bijvoorbeeld de sector waarin jij werkt?
Het volledige 2021 Data Breach Investigations Report is beschikbaar via Verizon:
https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

accepteren ze. En dat spel spelen ze goed. Iets wat de securitygemeenschap ook moet doen. Perfectie is niet het doel. Nee, het minimaliseren van de dreiging tot deze behapbaar is, moet vooropstaan." Het delen van incidenten is en blijft hierbij volgens Bassett cruciaal. "Help anderen begrijpen wat er is gebeurd in het geval van een cyberaanval, zodat iedereen het beter kan doen", roept hij op. "En stop met het stigmatiseren van slachtoffers, want daarmee bereik je juist het tegenovergestelde."

Menselijke fouten

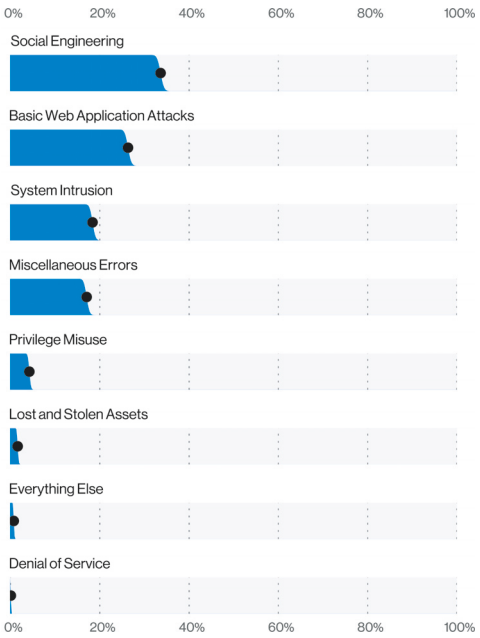
Hij trekt vervolgens de parallel met hoe bedrijven in zijn ogen zouden moeten omgaan met menselijke fouten die gemaakt worden door medewerkers. Nog altijd een belangrijke oorzaak van beveiligingsincidenten en datalekken, zo blijkt uit het rapport. "Why not cultivate your employees to be your early warning system when it can have a great return on investment?", is de opmerking uit het 2021 DBIR die hij in dit kader aanhaalt. "Wanneer iemand binnen je organisatie denkt dat hij bijvoorbeeld heeft geklikt op een verkeerde link dan moet hij of zij zich vrij voelen dit meteen te melden. Zonder dat dit vervelende gevolgen voor diegene heeft", legt hij uit. "Je schamen voor iets wat je verkeerd hebt gedaan, is heel normaal. En het is precies die schaamte waarvan aanvallers profiteren. Een gang van zaken die we kunnen veranderen door de cultuur van angst om fouten toe te geven, te doorbreken. Dat medewerkers fouten maken, zal niet veranderen", stelt hij. "Wat de gevolgen zijn van zo'n fout, hangt echter af van hoe je hier als bedrijf of organisatie mee omgaat. Wat we als security-specialisten nooit moeten vergeten is dat we niet een computer of een systeem beveiligen, maar een organisatie.



Figuur 2 - De kans dat iemand in een bedrijf een foute link ontvangt of een fout APK-bestand (Android app) installeert afgezet tegen de grootte van een bedrijf.

Dat betekent dat je medewerkers altijd moet meenemen in je verhaal."

Terug naar het rapport van dit jaar. In totaal analyseerden Bassett en zijn collega's 29.207 incidenten, waarvan 5.258 bevestigde datalekken vanuit heel de wereld. De belangrijkste conclusies: phishing-aanvallen stegen met 11 procent, aanvallen met ransomware met 6 procent en bij 85 procent van de inbreuken speelde de factor 'mens' een rol. De belangrijkste drijfveer van cybercriminelen is en blijft financieel gewin en daders moeten we zoeken in de wereld van de georganiseerde misdaad.



Figuur 3 – Datalek patronen (n=5275).

Niet veel nieuws onder de zon, zou je kunnen zeggen. En juist dat biedt volgens Bassett voordelen, want voor een belangrijk deel weet je als bedrijf of organisatie dus waar je je op moet voorbereiden. "Engineer for the expected and use operations for the exceptional", adviseert hij daarom. "Je wilt niet dat de afdeling operations binnen je organisatie achter elke phishing-email aan moet die je ontvangt omdat je geen phishing filter service hebt", geeft hij een voorbeeld. "Zorg er daarom voor dat qua workload alles in de juiste emmer terechtkomt. Bewaar met andere woorden de balans tussen engineering en operations, zodat de laatste oog voor de uitzonderingen kan houden", besluit hij.