Auteur: Marijke Stokkel, senior manager cybersecurity, BDO cybersecurity, marijke.stokkel@bdo.nl en Eddie Versluis, dreigingsanalist, BDO cybersecurity, eddie.versluis@bdo.nl

Cybercriminelen gaan publiek: jouw data, hun verhaal

Wat begint als een normale werkdag bij Uber, neemt een onverwachte wending als een melding binnenkomt op de interne chatapp Slack. 'I announce I am a hacker and Uber has suffered a data breach'. Medewerkers nemen het bericht aanvankelijk niet serieus en reacties stromen binnen: emoji's van popcorn en sirenes, de beroemde 'It's happening'-gif. Ubermedewerkers communiceren met de aanvaller in de veronderstelling dat het een grap is.

'Sorry dat ik de pretbederver moet zijn,' schrijft een medewerker, 'maar ik denk dat IT liever minder memes ziet terwijl ze de hack proberen op te lossen.' Het is inderdaad geen grap. De aanvaller probeert, zoals later blijkt een jongen van 18 jaar met op de darkweb-marktplaats gekochte inloggegevens, in te loggen op Uber's netwerk. Als hij wordt geblokkeerd door een extra beveiligingslaag (MFA), doet de aanvaller zich via WhatsApp voor als een medewerker van Uber's beveiligingsteam. Hij vraagt de betreffende medewerker een van de MFA-verzoeken goed te keuren vanwege 'verdachte activiteiten'. Na een vloedgolf aan meldingen geeft de medewerker toe. De aanvaller krijgt toegang tot het interne VPN, vindt de inloggegevens van een beheeraccount en heeft daarmee vrijwel onbeperkte toegang tot meerdere essentiële systemen (1). Naast de chatuitwisseling met Ubermedewerkers, bespreekt de aanvaller zijn acties ook met journalisten en een security-onderzoeker.

Uber heeft geluk dat het de aanvaller alleen om de kick gaat en hij geen systemen vernietigt of versleutelt. Maar een PR-ramp is het wel. De aanval wordt al snel opgemerkt door de media en de besmuikte reacties zijn niet van de lucht. 'It's a big deal, and an embarrassment to the company', schrijft gerenommeerd security-expert Bruce Schneier (2). De aandelen Uber openen de volgende dag flink lager (3).

Negatief framen

Wat opvalt aan deze casus is niet alleen hoe MFA-pushberichten zo hinderlijk kunnen worden dat het doelwit uiteindelijk toegeeft, maar ook dat de aanvaller Ubermedewerkers via Slack benadert en journalisten inschakelt om het nieuws te verspreiden. Het feit dat aanvallers niet alleen hun primaire doelwit aanvallen, maar ook stakeholders en de media erbij betrekken, is een relatief nieuw fenomeen (4).
Voor veel organisaties is dit dan ook een onbekende situatie. Tijdens onze cybercrisisoefeningen zien we geregeld dat crisisteams reageren met: 'We communiceren voorlopig niets' of 'We melden alleen een storing.' Ten onrechte denken ze dat zij bij een aanval controle hebben over de inhoud en timing van communicatie. Dit terwijl in het scenario van de oefening de aanvallers dan al een bericht over de succesvolle inbreuk op het darkweb hebben gezet. In het algemeen geldt dat als aanvallers als eerste berichten en de aanval negatief framen, bijsturen heel moeilijk is. Organisaties moeten beseffen dat hackaanvallers niet alleen hen, maar ook hun stakeholders direct kunnen benaderen en tevens publiekelijk over de aanval kunnen communiceren. Laten we deze strategie verder verkennen.

Nationale schokgolf

Ransomwareaanvallers benaderen vaak klanten, patiënten of medewerkers om extra druk te zetten. Dat gebeurde bijvoorbeeld in oktober 2020 in Finland. Duizenden Finnen kregen de schrik van hun leven toen ze een afpersingsmail ontvingen. Vastaamo, hun psychotherapiekliniek, bleek slachtoffer van een grote cyberaanval waarbij de complete patiëntendatabase werd buitgemaakt. Alle gegevens waren gestolen, waaronder informatie over angstaanvallen, overspel, pedofiele gedachten en zelfmoordpogingen van patiënten. Nadat het bedrijf weigerde losgeld te betalen, richtte de aanvaller zich op de patiënten. Binnen 24 uur moesten ze 200 euro in bitcoin betalen. Wie weigerde, liep het risico dat gegevens gepubliceerd zouden worden. Binnen korte tijd verschenen de eerste dossiers online, waaronder die van politici en andere publieke figuren (5).
De aanval veroorzaakte een nationale schokgolf in Finland vanwege de grootschaligheid van het lek en de ernst van de gestolen informatie. Minstens één zelfdoding werd aan het datalek gekoppeld. Vastaamo ging failliet en de CEO werd strafrechtelijk vervolgd omdat hij een eerder datalek verzweeg en het bedrijf onvoldoende beveiligde tegen cyberaanvallen.

Data leak sites

Ransomwaregroepen gebruiken ook eigen kanalen om een breder publiek te bereiken. Sinds enkele jaren creëren zij data leak sites (DLS) op het darkweb. Op deze platforms publiceren ze gestolen gegevens of dreigen ze daarmee, als onderdeel van hun afpersingsstrategie. Bij uitblijvende betalingen volgen meer bestanden. Veel DLS hebben aftelklokken die aangeven wanneer data vrijkomt of geven korting bij de eerste kopers van gestolen data. Op sommige platforms is de data doorzoekbaar. Andere bevatten persberichten en FAQ's die de informatie zo laagdrempelig mogelijk beschikbaar maken voor derden. Journalisten spelen hier gretig op in. In januari 2025 berichten meerdere media, waaronder techwebsite Tweakers, dat ransomwarebende Cl0p data van IT-dienstverlener Centric op hun DLS heeft geplaatst (6). Dit dwingt Centric vervolgens om publiek te reageren.

Eerlijke pentesters

Ransomwaregroepen begrijpen goed dat hun activiteiten nieuwswaardig zijn en spelen daar handig op in. Door succesvolle aanvallen aan te kondigen, demonstreren ze hun capaciteiten en vergroten ze hun dreiging naar toekomstige slachtoffers.
Ransomwaregroepen gebruiken DLS ook als recruitmentmiddel. Hoge losgeldbedragen op DLS geven ransomwaregroepen een reputatie bij andere cybercriminelen. Door de wereld van ransomware als cool en lucratief voor te spiegelen, proberen ze

Besef dat hackaanvallers niet alleen jou, maar ook jouw stakeholders direct kunnen benaderen en publiekelijk over de aanval kunnen communiceren

meer leden en samenwerkingspartners aan te trekken (7).
Tot slot gebruiken ransomwaregroepen DLS om een bepaald narratief uit te dragen. Ze presenteren zichzelf als 'eerlijke pentesters' die 'cybersecurityonderzoek' uitvoeren. Sommige bieden getroffen organisatie aan om een rapportage op te leveren over hoe ze zijn binnengekomen en hoe dit voortaan voorkomen kan worden (vaak door een update uit te voeren op het kwetsbare systeem). Deze groepen proberen hun acties goed te praten door hun doelwitten af te schilderen als onverantwoordelijk of nalatig. Een FAQ op de leak site van ransomwaregroep 8Base geeft dit treffend weer.

Q: 'I am (was) a client of a company found in your list and became a victim of their irresponsible processing of my personal data and business secrets. What can I do?'
A: 'First of all, we find it necessary to say we are sorry that you were affected by companies 'negligent attitude to the privacy and security of their customers' personal data. But there is a bright side, because it gives you the opportunity to request compensation from such companies' (8).

Je hoeft overigens niet naar het darkweb voor informatie over hackaanvallen. Cybercriminelen promoten hun DLS ook via forums en sociale media op het 'gewone' internet. Daarnaast verzamelen platforms als Ransomware.live via het open source project Ransomwatch gegevens van meerdere DLS en maken die beschikbaar voor een breder publiek.
Hackaanvallers communiceren dus actief over hun aanvallen. Hoe moet je hier als getroffen organisatie mee omgaan? Een aantal tips.

• Wees er snel bij

Als het niet lukt de aanvallers vóór te zijn, zorg dan in elk geval dat je direct op de hoogte bent zodra jouw organisatie op het darkweb verschijnt. Monitor het darkweb in real-time - een logische taak voor het Security Operation Center (SOC). Houd niet alleen je eigen organisatie in de gaten, maar ook leveranciers en samenwerkingspartners met toegang tot jouw data. Zo bleek bij het eerdergenoemde datalek van Centric, data van opdrachtgever gemeente Amersfoort te zijn betrokken.

• Communiceer als eerste

Breng slecht nieuws zelf als eerste naar buiten. Zo houd je controle en bepaal je het narratief, een strategie die bekend staat als stealing thunder. Wacht niet tot er data op een DLS verschijnt. Zodra je weet dat vertrouwelijke gegevens zijn buitgemaakt, is openheid cruciaal. Dit geldt in het bijzonder voor gegevens van derden, zoals klant- of partnerdata. Stakeholders waarderen het wanneer een organisatie verantwoordelijkheid neemt, dat vergroot het vertrouwen. Bovendien vermindert proactieve communicatie de kans dat aanvallers of de pers een ongunstig frame neerzetten, wat moeilijk te corrigeren is.

• Zet de meest getroffenen op de eerste plaats

Sommige organisaties stellen tijdens een crisis hun eigen reputatie boven alles, maar dat werkt vaak averechts. Het oogt egoïstisch en komt onbetrouwbaar over. Richt je in plaats daarvan op de echte getroffenen - zoals mensen van wie gegevens zijn gelekt of medewerkers die niet kunnen werken. Ondersteun hen met concrete acties en transparante communicatie. Een crisis draait om hún belang, niet dat van de betrokken organisatie. Oprechte, empathische communicatie met de meest getroffenen versterkt het vertrouwen en toont verantwoordelijkheid.

Cybercriminelen zoeken steeds vaker de openbaarheid. Weet hoe ze te werk gaan en wees voorbereid.

Referenties

(1) https://www.theverge.com/2022/9/16/23356213/uber-hack-teen-slack-google-cloud-credentials-powershell
(2) https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html
(3) https://investorplace.com/2022/09/uber-stock-falls-5-on-major-cybersecurity-breach/
(4) https://news.sophos.com/en-us/2023/12/13/press-and-pressure-ransomware-gangs-and-the-media/
(5) They Told Their Therapists Everything. Hackers Leaked It All | WIRED
(6) Data van Centric verschijnt op de site van ransomwarebende - Computer - Nieuws - Tweakers
(7) Press and pressure: Ransomware gangs and the media – Sophos News
(8) https://news.sophos.com/en-us/2024/08/06/turning-the-screws-the-pressure-tactics-of-ransomware-gangs/