CYBER SCHADENFALL

Markel hat sich eine faire Schadensregulierung auf die Fahnen geschrieben. Das beweisen immer wieder Studien und Tests. Zuletzt 2022 im Rahmen der großangelegten FOCUS MONEY Studie – Fairness von Cyberversicherern, welche mehr als 1.200 Fälle untersuchte. Markel erhielt wiederholt die Note „Sehr gut". In Kombination mit direkten Ansprechpartnern kann Markel rasch auf Schadensfälle reagieren. Offene und ehrliche Kommunikation sind dabei Schlüsselelemente, die entscheidend zu einer langfristigen Kunden-/Maklerbeziehung beitragen.

Der lahmgelegte Webservice

DDOS-ATTACKE

Ausgangssituation
Der Versicherungsnehmer ist ein Anbieter von Webservices. Unter Webservices wird in der Informationstechnologie eine Kommunikationskombination zwischen Maschinen und/oder Anwendungen verstanden. Dabei geht es im Kern um den Abruf von Daten, die von einem anderen Rechner oder Applikation zur Verfügung gestellt werden.
Das geschieht über verschiedene Formen an Schnittstellen, die sich einer Sprache (WSDL) bedienen, welche den Dienst näher beschreibt und den Anfrager informiert, welche Funktionen er über den angefragten Webservice ausführen kann. Ein gutes Beispiel sind die Karten von Google. Diese befinden sich nicht direkt auf der website, sondern werden nur über Schnittstellen (z. Bsp. SOAP, RESTful) eingebunden. Das, was angezeigt wird, sind von der website abgefragte und von Google bereitgestellte Informationen. Über die zuvor erwähnte Sprache wird mitgeteilt, dass beispielsweise über die "Plus" und "Minus" Funktion, die Ansicht vergrößert bzw. verkleinert werden kann.

Problembeschreibung
Das durchschnittliche, monatliche Datenvolumen vom Webservice des Versicherungsnehmers liegt bei 5 GByte. Im vorliegenden Schadenfall kommt es zu einem signifikanten Anstieg der Anfragen um den Faktor 10. Stunden später sogar um den Faktor 60. Parallel steigt das Datenvolumen auf bis zu 300 GByte. Doch damit nicht genug: in den nächsten Tagen durchbricht die Anzahl der Anfragen die Millionengrenze. Da der Webservice und dessen Infrastruktur nicht für eine solche Anfragelast ausgelegt waren, führte das in Folge dazu, dass der Webservice aufgrund der Anfragelast für viele Teilnehmer stundenlang nicht erreichbar war.
Zu dem technischen Problem der Nichterreichbarkeit gesellte sich am selben Tage ein per E-Mail eingegangenes Bekennerschreiben mit dem Angebot, die Attacke gegen Zahlung in Höhe von USD 5.000,00 – zahlbar in BitCoin – einzustellen. Der Versicherungsnehmer war somit Opfer einer (mit Erpressung verbundenen) Distributed-Denial-of-Service (DDoS)-Attacke geworden.

Lösungsansatz
Bei einer DDoS-Attacke starten Cyber-Kriminelle von mehreren Rechnern aus ("Distributed") Angriffe gegen den Zielrechner. Der Begriff "mehrere" kann dabei von einigen Dutzend Einzelrechnern bis hin zu Netzwerken aus tausenden Rechnern reichen, welche im Vorfeld mit Schadsoftware infiziert wurden und die dann auf Befehl alle simultan den Zielrechner mit Anfragen überhäufen. Solange bis dieser in die Knie geht und nicht mehr erreichbar ist. Die Folgen für betroffene Unternehmen reichen von Imageschaden bei Bekanntwerden bis zu Umsatzverlusten oder gar Betriebsunterbrechungen. Sich vor solchen Angriffen zu schützen, ist schwer, weil der Zielrechner die Daten erst erhalten muss, um sie zu verarbeiten. Doch dann ist es bereits zu spät.
Dem Versicherungsnehmer wurden – in Zusammenarbeit mit unseren Cyber-Schutzexperten – Maßnahmen auf verschiedenen Ebenen empfohlen. Die DDoS-Abwehr an den Internet Service Provider (ISP) zu verlagern, im eigenen Haus ein Intrusion-Prevention-System (IPS) zu installieren, in Firewall-Technologie und spezielle Hardware investieren und der Einsatz eines Content Delivery Networks (CDN). Nach Ergreifen der Gegenmaßnahmen (einer Kombination aus den zuvor aufgezählten) normalisierte sich die Anzahl der Anfragen wieder und die Serverauslastung pendelte sich wieder auf dem Niveau vor der DDoS-Attacke ein.

Beurteilung durch Markel
DDoS-Attacken nehmen zu. NETSCOUT hat in seinem Threat Intelligence Report berichtet, dass Cyber-Kriminelle 2021 rund 9,75 Millionen DDoSAngriffe gestartet hätten. Ähnlich äußert sich auch der Netzwerk-Anbieter Cloudflare und berichtet, dass in der zweiten Jahreshälfte 2021 Terabit-starke Angriffe massiv zugenommen haben. Einsame Spitze: ein DDoS-Angriff mit knapp zwei Terabit pro Sekunde, der insgesamt lediglich zwei Minuten andauerte aber von 15.000 Bots gestartet wurde.

Welche Kosten wurden übernommen?
Es liegt ein versicherter Schadenfall mit Bezug auf Ziffer A.1 vor. Notwendige und angemessene Kosten zur Schadenabwehr wurden erstattet. Erstattet wurden die Kosten für die Einrichtung des DDoSSchutzes samt erforderlicher Hardware.