SUCCESS STORY

VON DER ZUSAMMENARBEIT

sure[secure]
your security operations center

BIG
direkt gesund

Kurzvorstellung des Partners

Bundesinnungskrankenkasse Gesundheit ist eine deutsche Innungskrankenkasse mit Sitz in Berlin und Verwaltung in Dortmund. Die BIG direkt gesund ist bundesweit geöffnet und verfügt über Geschäftsstellen in Dortmund, Düsseldorf, Köln und Aachen.

Mit 520.000 Versicherten belegt die BIG direkt im Ranking aller gesetzlichen Krankenkassen in Deutschland Platz 29 von 103.

Als Krankenkasse ist die BIG ein wichtiger Baustein für die Bürgerinnen und Bürger und wird deshalb als kritische Infrastruktur für Deutschland betrachtet.

Bundesinnungskrankenkasse Gesundheit

Branche:	Finanzen & Versicherung
Mitarbeitende:	1.000
Gründung:	1996
Versicherte:	520.000

Diese Themen sind Bestandteil der Success Story

- Detection via Managed Detection & Response Service
- Incident Response Management
- Security Operations Center as a Service
- Cyberversicherung

Welche Herausforderungen hatte der Partner?

Die Bundesinnungskrankenkasse Gesundheit (kurz: BIG) ist Opfer eines Cyberangriffs geworden.

Einer Angreifergruppe ist es gelungen, die Systemlandschaft zu kompromittieren. Entdeckt wurde dieser Angriff durch einen Service-Provider, bei dem die BIG einen Managed Detection & Response Vertrag besitzt. Der Dienstleister war in der Lage, den Angreifer zu entdecken, bevor es zu einer Verschlüsselung oder zu Datenabfluss kam, aber es mussten Systeme proaktiv bzw. präventiv heruntergefahren werden.

Denn zu Beginn war es schwierig, das Ausmaß des Angriffs aufgrund mangelnder Visibilität abschätzen zu können. Da zu diesem Zeitpunkt noch kein Security Information and Event Management (SIEM) implementiert war, um die Logs zentral zu analysieren, hat die Analyse des Vorfalls viel Zeit in Anspruch genommen.

Parallel dazu wurde die bestehende Cyberversicherung vom Versicherungsgeber im Preis massiv angehoben und nach dem Sicherheitsvorfall sogar gekündigt. Diese Situation verdeutlicht einen Widerspruch: Trotz erhöhter Sicherheitsmaßnahmen reagieren Versicherer oft mit Preiserhöhungen oder Kündigungen, da sie ein gesteigertes Risiko sehen.

Denn aus einem Cyberangriff resultiert in der Regel eine deutlich stärkere Cybersecurity. Die gewonnenen Erkenntnisse führen dazu, dass wichtige Maßnahmen umgesetzt werden, was die Cyberresilienz verbessert.

Wird dieser Hintergrund im Detail mit dem Versicherer besprochen, kann das sogar zu einer besseren Versicherbarkeit und zu optimierten Konditionen führen. Mit einer fundierten Analyse und einer klaren Roadmap kann ein spezialisierter Makler erfolgreich mit den Versicherern verhandeln. Gute Beziehungen zu den Versicherern und eine detaillierte Darstellung der Sicherheitsmaßnahmen erhöhen die Chancen auf einen passenden Versicherungsschutz.

Wie haben wir die Herausforderung gelöst?

Uns war sehr schnell klar, was wir in diesem Fall brauchen würden:

- Incident Response Team
- Transparenz & Visibilität
- Effiziente Prozesse und intensive Begleitung

Incident Response

Nachdem die Analysten der suresecure in der Nacht erste Anomalien feststellten, wurde der Partner informiert, dass vermutlich ein Angreifer Zugriff auf die Umgebung hat. Gemeinsam mit den IT-Technikern der BIG wurden weiterführende Untersuchungen durchgeführt und letztlich die These bestätigt. Um weiteren Schaden zu verhindern, wurden die Server erst mal proaktiv vom Netz genommen und die Internetverbindung unterbunden.

Unsere Forensik-Teams haben alle Systeme durchleuchtet und diese insbesondere auf die identifizierten Indicators of Compromise (IOCs) geprüft. Jedes infizierte System musste infolgedessen proaktiv neu aufgesetzt werden. Zur Erhöhung der Visibilität innerhalb der Infrastruktur wurde zusätzlich unser Security Operations Center Service (SOC-Service) ausgerollt. So konnten wir sicherstellen, dass alle Logs von allen Assets zentral gesammelt und ausgewertet werden. Sollte es dem Angreifer trotz unserer Bemühungen gelingen, persistent in der Umgebung zu bleiben, so haben wir zumindest eine totale Visibilität und damit die Möglichkeit, sehr schnell auf die Ereignisse zu reagieren. Gleichzeitig unterstützten wir den Partner bei der Krisenkommunikation und den Gesprächen mit Behörden und Versicherungen.

Cyberversicherung

Noch im Prozess wurde die Cyberversicherung durch den Versicherungsgeber gekündigt und die Prämie massiv erhöht. Dies wurde vorerst akzeptiert, damit die Zahlung der monetären Schäden nicht gefährdet wird. Zwölf Monate später kam es dann erneut zu einer Kündigung durch den Versicherer und einer Umstellung der Konditionen. Dadurch war die Fortführung der Versicherung nicht mehr wirtschaftlich sinnvoll. Ebenfalls wurden klare Signale gesetzt, dass die Versicherung kein Interesse hat, für den Schaden zu zahlen.

Die BIG hatte durch die kurzfristige Kündigung der Versicherung sehr wenig Zeit, nach Alternativen zu suchen, und bat uns daher um Unterstützung. Hinzu kommt, dass es für KRITIS-Unternehmen nicht so einfach ist, eine Versicherung zu erhalten, da das Schadenspotenzial höher ist. Außerdem ist es auch nicht so einfach, eine Versicherung zu erhalten, nachdem ein Schaden eingetreten ist. Es ist notwendig, den Versicherern glaubhaft zu machen, dass adäquate Maßnahmen getroffen wurden.

Ich habe schon viele Sicherheitsvorfälle begleitet, aber dieser war besonders. Vor allem, weil der Impact auf die Versicherten so groß war und es einfach darum ging, schnellstmöglich wieder Leistungen erbringen zu können.

Besonders aber auch wegen einer spürbar partnerschaftlichen Zusammenarbeit mit allen Ansprechpartnern bei der BIG. Das war wirklich ganz großes Kino.

Baran Kamaci
Enterprise Account Executive
suresecure GmbH

Heutiges Setup

Heute laufen alle Logs in das Security Operations Center von suresecure, und wir sind in der Lage, sollte es erneut zu einem Angriff kommen, wesentlich früher einzugreifen, da wir gegenüber einem MDR-Service nun alle Logs erhalten. Der SOC-Service ist auch ein strategisches Instrument mit Blick auf das Umsetzungsgesetz der NIS2-Richtlinie. Hier werden insbesondere für KRITIS Unternehmen wie die BIG neue Anforderungen gestellt, die bei der BIG nun bereits erfüllt sind.

Reports aus dem SOC werden monatlich der Versicherung zur Verfügung gestellt. Diese werden aber nicht einfach versendet, sondern auch mit der Versicherung durchgesprochen.

Dabei gehen wir auf Quantität und Qualität der Alerts ein, sprechen über mögliche Eskalationen sowie die aktuelle Bedrohungslage und geben einen transparenten Überblick zum Schwachstellen-Management. Dadurch bekommt der Versicherer ein sehr gutes Gefühl für die Risikobewertung.

Denn unter anderem werden auch Verbesserungsmaßnahmen abgebildet, die dann wiederum zu besseren Prämien und Konditionen führen können. Außerdem erhöht die Transparenz die Zahlungsbereitschaft der Versicherung im Schadensfall. Denn durch die Reports kann der Versicherer hinterher nicht sagen: „Das war uns so nicht bewusst".

Ich liebe es Rätsel zu lösen. Dieses war besonders knifflig und hat von uns allen viel abverlangt. An diesem Projekt sind alle Beteiligten gewachsen und ich bin sehr dankbar für die Erfahrungen, die ich in diesem Projekt sammeln durfte.

André Ditzel
Senior IR-Analyst
suresecure GmbH

Andreas Faltin, IT-Leiter BIG Direkt

Gemeinsam arbeiten wir mit suresecure an der Steigerung unseres Sicherheitsniveaus auf strategischer und konzeptioneller Ebene sowie bei der operativen Umsetzung von Sicherheitsthemen. Wir sind begeistert von der hohen Einsatzbereitschaft, Professionalität und das hohe Verantwortungsgefühl des Teams von suresecure. Dies ermöglicht eine sehr angenehme, zielgerichtete Zusammenarbeit auf hoher Vertrauensbasis, auch in schwierigen Situationen.

Key Take-Aways:

- Frühzeitige Detection ist enorm wichtig, um Folgeschäden zu minimieren
- Visibilität und Transparenz in der eigenen Infrastruktur schaffen volle Handlungsfähigkeit
- Cyberversicherungen können auch trotz Cyberangriff und KRITIS-Zugehörigkeit geschlossen werden

suresecure Gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de