Herr der Lage:
Effektive Kommunikation navigiert Unternehmen durch eine Cyberattacke

Cyberkriminalität und Datendiebstahl sind ein Supergau und können Unternehmen ins Straucheln bringen. Ein Notfallplan hilft allen Beteiligten, die Nerven und vor allem die Kontrolle zu behalten.

Die finanziellen und operativen Auswirkungen einer Cyberattacke können eine Organisation an den Rand ihrer Existenz bringen. Durchschnittlich 4,3 Millionen Euro betrugen 2023 die Kosten eines Datendiebstahls. Für kleine und mittlere Unternehmen (KMUs), die oftmals im Fokus der Angriffe stehen, eine bedrohliche Summe. Denn immerhin zielen laut Statistik von Sophos X-Ops 43 Prozent aller Cyberangriffe im letzten Jahr auf diese Organisationsgrade ab. Daneben leiden Ansehen und Vertrauen, zwei in hart umkämpften Märkten entscheidende Erfolgsfaktoren. Eine klare, schnelle Kommunikation ist der Schlüssel, um die Kontrolle über die Situation zu behalten und um die Folgen zu mildern.

Krisenmanagement im Falle einer Cyberattacke bedeutet, dass bereits vor einem Vorfall die möglichen Szenarien durchdacht sind und klare Marschruten für die echte Attacke aufgestellt werden. Sophos hat die wichtigsten Punkte zusammengestellt und in seinem Leitfaden für die Erstellung eines Incident-Response-Plans detailliert beschrieben.

Prävention: Aspekte, die vor einem Cybervorfall bedacht werden müssen:

- Gibt es im Unternehmen einen Notfallplan und beinhaltet dieser auch die Krisenkommunikation im Falle eines Datendiebstahls? Hilfe hierbei bieten Experten aus IT, Recht und Kommunikation.
- Die Ernennung eines Sprechers sorgt für konsistente Botschaften an Geschäftspartner und die Öffentlichkeit.
- Der Notfallplan sollte griffbereit und von überallher abrufbereit sein, selbst wenn die Systeme kompromittiert sind.

Reaktion: Aspekte, die nach einem Cybervorfall aktiv gestartet werden müssen:
Antworten nach einer Cyberattacke variieren nach Eskalation und Botschaften. Daher muss der Notfallplan individuell an das Unternehmen angepasst sein. Allerdings sind folgende Schritte nahezu immer unerlässlich und die Organisation muss diese für sich priorisieren:

- **Informieren der Strafverfolgung**: üblicherweise durch den ausgewählten Sprecher des Unternehmens.
- **Beratung mit Experten**: in Deutschland regeln die Bundes- und jeweiligen Landesbehörden den Datenschutz. Die Ansprechpartner sollten ebenfalls im Notfallplan notiert sein.
- **Erklärungen abgeben**: Aktualität ist entscheidend, um die öffentliche Wahrnehmung zu steuern und das Narrativ zu kontrollieren. Am besten gibt es bereits eine Vorlage, die sich akut vervollständigen lässt mit klarer Aussage zu folgenden Fragen: wie kam es zu dem Diebstahl, welche Daten sind betroffen und welche Maßnahmen werden zum Beheben unternommen, auch für die Zukunft.
- **Kommunikation mit Stakeholdern**: Ob Verkäufer, Kunden oder Investoren, Unternehmen sollten zügig ihre wichtigsten Partner über die Cyberattacke und gegebenenfalls den Datendiebstahl in Kenntnis setzen. Idealerweise ist diese Kommunikation bereits im Notfallplan hinterlegt. Auch der Kommunikationsweg sollte bedacht sein – ist E-Mail-Verkehr

nicht möglich, müssen andere, sichere Kanäle genutzt werden und diese vorab implementiert und getestet sein.
- **Kommunikation mit betroffenen Personen**: Transparent, empathisch, rechtzeitig – so sollten Organisationen im Idealfall mit den Menschen umgehen, deren Daten gestohlen wurden. Auch hier ist eine Vorlage sinnvoll.

Schnelle und effektive Krisenantwort
„Das Aufsetzen eines Cybervorfall-Kommunikations-Plans ist von entscheidender Bedeutung für jede Organisation zur Vorbereitung für eine Cyberattacke“, so Michael Veit, Cybersecurity-Experte bei Sophos. „Damit haben Unternehmen eine klare Navigationsanleitung und Kontrolle auch bei rauer See. Zudem helfen Simulationen der Krisenszenarien, potenzielle Fallstricke zu erkennen und den Plan kontinuierlich an neue Bedrohungen anzupassen.“

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de