Collective Intelligence

Risikomanagement und Kommunikation in Cyberkrisen

Neue Anforderungen und wie Unternehmen sich vorbereiten können

Von **Suntka von Halen**

Brunswick Group

14. März 2023

BRUNSWICK

Risikomanagement und Kommunikation in Cyberkrisen

Die Bedrohungslage globaler Unternehmen durch Cyberangriffe hat sich in den vergangenen Jahren kontinuierlich verschärft. Experten rechnen damit, dass sich weltweit allein die wirtschaftlichen Schäden bis 2025 auf rund 10,5 Billionen Euro belaufen werden.[1] Der deutschen Wirtschaft entsteht ein jährlicher Schaden von rund 203 Milliarden Euro allein durch Diebstahl von Daten, Spionage und Sabotage[2] - knapp eine Vervierfachung gegenüber den Jahren 2016/2017 (55 Milliarden Euro)[3].

Die Gründe liegen auf der Hand: Die globale Gesellschaft nutzt die exponentiell wachsenden Möglichkeiten der Digitalisierung in immer mehr, immer vernetzteren und immer sensibleren Anwendungsbereichen. Forschung und Entwicklung, Gesundheit, Verwaltung, Politik, globale Lieferketten und Produktionsnetzwerke sind durch die zunehmende Datenverfügbarkeit attraktive Angriffsziele für Cyberkriminalität.

Die Risikolandschaft verschärft sich exponentiell im aktuellen Umfeld

Industriespionage, Geopolitik, finanzieller Anreiz – die Motive der Angriffe sind so vielfältig wie die Angriffe selbst. Cyberkrisen zählen heute zu den größten operativen Risiken von Unternehmen und Organisationen, und Unternehmen sind sich der Bedrohung aus dem Netz bewusst: Im Allianz Risk Barometer 2022 stehen Cyberattacken mittlerweile auf Platz 1, nachdem sie im Vorjahr nur unter den Top 3-Risiken liefen. Die Awareness steigt also, die Erfahrung zeigt dagegen, dass vor allem das dynamische Wachstum des Cyber-Risikos im Risikomanagement vieler Unternehmen nicht durchgehend abgebildet wird. Während das Schadenspotenzial von Cyberrisiken schon aus sich selbst heraus exponentiell wächst, setzen die Verwerfungen im makroökonomischen Umfeld noch einmal einen Turbo auf, denn Corona-Pandemie, Ukraine-Krieg und Energiekrise verändern die Risikolandschaft in atemberaubenden Tempo. Verfügbarkeit und Bezahlbarkeit von Rohstoffen und Energie, Supply Chain-Risiken und exponentiell höhere Vulnerabilität von Netzwerken durch remote Zugriffe sind nur einige Beispiele. Wie so oft sind die Risiken auch interdependent und können sich so schnell zu einem perfect storm verknüpfen. Diese Dynamik muss im Risikomanagement von Unternehmen angemessen berücksichtigt werden.

Risikomanagement und Kommunikation integriert betrachten

Ein Cyberangriff verursacht nicht nur Kosten zur Wiederherstellung der betroffenen Systeme, sondern zusätzlichen hohen Ressourcenaufwand für Krisenmanagement sowie indirekte Kosten wie den Vertrauensverlust einer breiten Masse von Endkunden im B2C-Geschäft, Stichwort Übermittlung von Gesundheitsdaten, private Finanztransaktionen oder Nutzung von Online-Verwaltungsservices, oder Konventionalstrafen in einem hochintegrierten B2B-Geschäft. In allen diesen Situationen steht vor allem aber die unternehmerische Reputation auf dem Spiel, und an dieser Reputation hängt ein Preisschild: Bewertung und Kurs, Auftragsvolumina oder der Wettbewerb um Partner und Talente. Schnelle, konsistente und den Zielgruppen gegenüber hilfreiche Kommunikation ist daher eine unternehmerische Priorität und muss integriert mit dem Risikomanagement aufgesetzt werden. Die gute Nachricht ist: Sie lässt sich vorbereiten.

---

[1] Vgl. Cybercrime Magazine, unter: https://cybersecurityventures.com/cybersecurity-almanac-2022/

[2] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

[3] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr

Erfolgreiches Krisenmanagement ist eine Funktion von guter Vorbereitung

In jeder Krise eines Unternehmens ist es Aufgabe der Unternehmenskommunikation, einen synchronisierten Informationsfluss und gegebenenfalls Dialog mit den verschiedenen internen und externe Zielgruppen des Unternehmens zu organisieren. Die besondere Herausforderung bei Cyberkrisen liegt darin, dass wenn der Angriff erkennbar wird, z.B. im Moment der Verschlüsselung bei Ransomangriffen, das Ausmaß des Schadens in den allermeisten Fällen völlig unklar ist. Dwell times – also der Zeitraum zwischen Eindringen der Angreifer und tatsächlicher Verschlüsselung – von mehreren Wochen sind nicht unüblich und ermöglichen Ausspähen, Diebstahl, Manipulation oder eben die Vorbereitung der Verschlüsselung von Daten. Die Forensik benötigt dagegen üblicherweise mehrere Wochen, um einen vollständigen Überblick zu bekommen. Die Unternehmenskommunikation muss also einen längeren Zeitraum der Unsicherheit moderieren und koordinieren als in fast jeder anderen Krise.

Der (nachvollziehbare) erste Impuls ist oft, so umfassend und transparent wie möglich zu informieren. Dennoch zeigt die Erfahrung, dass sich im Laufe der Forensik fast immer neue Sachstände ergeben, die zu aufwendigen Korrekturen führen, wenn zu früh zu viel veröffentlicht wird.

In einer Cyberkrise muss die Kommunikation im Krisenteam das Spiel mit Gas und Bremse beherrschen. Eine erste kurze Information über den Vorfall muss die wichtigsten Zielgruppen schnell erreichen – Behörden, Mitarbeiter, Kunden, Investoren, Partner. Diese Information muss vor allem Hilfestellung bieten (persönliche Ansprechpartner, Support-Hotline und -Emailadresse), verständlich sein und angemessen empathisch angesichts der Auswirkungen des Vorfalls auf die Zielgruppen. Hier transportiert die Tonalität der Kommunikation immer auch eine unternehmerische Haltung. Entsprechend müssen Kommunikationsmaterialien wie Holding Statement, Talking Points oder top level FAQ gut vorbereitet sein.

Ebenfalls sollten grundsätzliche unternehmerische Entscheidungen für die wahrscheinlichsten Angriffsszenarien Teil der Krisenvorbereitung sein. Hier müssen die Teams von Unternehmens-kommunikation und Risikomanagement ihre Arbeit für eine effiziente Vorbereitung auf gegebene Szenarien oftmals noch stärker vernetzen. Teil des integrierten Risikomanagements sind auch regelmäßige Trainings und Simulationen. Sie sind zwar im ersten Schritt aufwändig, beispielsweise in der Aufbereitung veränderter Risikoszenarien für Cyberangriffe und Anpassung der Kommunikationsprozesse. Dafür sind integriert trainierte Teams im Ernstfall aber den entscheidenden Schritt schneller in einem unternehmensweit koordinierten effizienten Krisenmanagement und schützen so die Geschäftsfähigkeit, die unternehmerische Reputation und damit den unternehmerischen Gesamtwert.

Kommunikation muss sich im Übrigen nicht nur mit der eigenen Risikoumgebung beschäftigen – Industry Round Tables, nationale oder globale Initiativen wie z.B. die Allianz für Cybersicherheit des BSI oder die Charter of Trust bieten wertvollen Austausch und hilfreiche Vernetzung unter Experten und Peers, um sich angesichts des steigenden Risikos von Cyberangriffen im Risikomanagement und der Kommunikation bestmöglich aufzustellen.

Um das Gespräch fortzuführen:

Suntka von Halen

Co-Lead Cybersecurity Germany

E-Mail: svonhalen@brunswickgroup.com

