BILD: ZEPHYR_P/ ADOBESTOCK.COM

Die sieben Todsünden für den Weg in die Cyberkrise

Wer unvorbereitet in einen Cybervorfall gerät, kommt wohl zunächst ins Schleudern. Unüberlegtes Handeln könnte aus einem Vorfall aber eine echte Krise machen. Insbesondere folgende sieben Todsünden gilt es unbedingt zu vermeiden.

Alles steht still, und eine Lösegeldzahlung steht auch noch zur Debatte. Wenn sich ein Cyber-Incident zu einer Cyberkrise entwickelt, können die Folgen für Organisationen jeder Grösse verheerend sein. Kosten für Betriebsausfall, Reputationsschäden, Lösegeldzahlungen und andere Folgen können schnell durch die Decke schiessen. Keine Organisation möchte sich in solch einer Situation wiederfinden. Daher sollte man bereit sein, wenn es darauf ankommt. Idealerweise gelangt man erst gar nicht in solch eine Situation. Aber was, wenn doch?

Im Buch «Cyber Crisis Management» von Holger Kaschner ist die Rede von sieben Todsünden, welche die erfolgreiche Bewältigung einer Cyberkrise verhindern. Rein inhaltlich lässt es sich als ein Referenzwerk empfehlen, das viele unserer Erfahrungen und Best Practices mit Kunden bestätigt. Die sieben Todsünden sind:

1. Interne und externe Stakeholder werden zur Nebensache.
2. Man lässt sich zu öffentlichen Schuldzuweisungen hinreissen.
3. Man ist nicht transparent genug und gibt Fakten nur peu à peu preis.
4. Man vergisst die Mitarbeitenden, kommuniziert intern nicht offen und nur verzögert.
5. Man kann Versprechen nicht einhalten und lässt diesen keine Taten folgen.
6. Man überschätzt die Krisenstandhaftigkeit der Organisation. Gleichzeitig unterschätzt man die Risiken und deren Folgen.
7. Man vergisst die Prävention und ist nicht vorbereitet.

Wir haben 23 CISOs befragt, welche Relevanz die Bereitschaft für Cyberkrisen in ihrem Unternehmen spielt. Etwa 60 Prozent der Befragten gaben an, dass diese eine hohe beziehungsweise sehr hohe Relevanz in ihrem Unternehmen habe. Man möchte glauben, dass dem Üben und Simulieren von Cyberkrisenszenarien daher die entsprechende Aufmerksamkeit geschenkt werden. Nicht zuletzt ist es eine effizient und effektiv agierende Krisenorganisation, die im Extremfall den Verlust minimieren kann, sofern Handlungsroutinen simuliert und blinde Flecken durch solche Simulationen aufgedeckt wurden. In der Realität sehen die Befragten jedoch einen expliziten Ausbildungsbedarf für Fachstäbe auf taktischer Ebene sowie für die Krisenorganisation und Entscheidungsträger auf strategischer Ebene, um die Cyberkrisenstandhaftigkeit zu steigern. Mit 68 Prozent der Antworten wurde mangelnde Unterstützung durch die Geschäftsleitung als die grösste Herausforderung für die effektive Durchführung von Cyberkrisenausbildungen von den Befragten genannt. Es folgten mit jeweils 14 Prozent Budget-Restriktionen, die implizit mit der Unterstützung durch die Führungsebene zusammenhängen, sowie die Integration von Cyberkrisenausbildungen im hektischen Tagesgeschäft als weitere Antworten.

Wie kann es also sein, dass der Cyberkrisenstandhaftigkeit seitens Führungsebene in Zeiten der mitunter täglichen Berichterstattung von Cybervorfällen anscheinend ungenügende Relevanz zugeschrieben wird? Diese Frage lässt sich auch in dieser Kolumne nicht abschliessend klären und die Antwort hierauf ist sicherlich mehrdimensional. Möglicherweise hängt es mit der Risikowahrnehmung zusammen. Siegrist und Árvi unterscheiden drei dominante Faktoren, welche die Risikowahrnehmung beeinflussen: die Eigenschaften der Gefahren, die Eigenschaften der wahrnehmenden Person und Heuristiken zur Risikobewertung. Je greifbarer und unmittelbarer die Eigenschaften von Risiken, desto eher werden diese auch ihrem Risiko entsprechend wahrgenommen. Je sachkundiger und persönlich betroffen eine Person ist, desto eher nimmt diese das Risiko als ein solches wahr und bewertet es anhand von Fakten, statt nach Entscheidungsabkürzungen zu suchen. Wenn man also Betroffenheit generiert oder der Führungsebene in einer für sie verständlichen Sprache Cyberrisiken und deren Gefahren für die Organisation näherbringt, dann schafft man eine Grundlage, um sich die Unterstützung der Führungsebene für Investments in Cyberresilienz zu sichern.

Was sind Ihre Erfahrungen? Fordern Sie uns heraus!

Die Autoren
Fabian Muhly, Partner, Leo & Muhly Cyber Advisory
Philipp Leo, Partner, Leo & Muhly Cyber Advisory

Die vollständige Kolumne finden Sie online
www.swisscybersecurity.net