Bei Cyberattacken hilft Vorbereitung

Salzburg: Expertentalk zu Cyberangriffen und Krisenkommunikation

Digitale Angriffe beschäftigen Unternehmen: Die Attacken von Cyberkriminellen führen zu massiven Unterbrechungen des Geschäftsbetriebs und möglicherweise zu wirtschaftlichen Folgen und Image-Schäden. Beim Expertentalk von ikp Salzburg, Industriellenvereinigung und Marketingclub Salzburg ging es darum, wie sich Unternehmen und Organisationen auf Angriffe vorbereiten können und wie in einer Cyberkrise kommuniziert wird, um längerfristige Imageschäden zu vermeiden.

Die richtige Vorbereitung ist der Schlüssel, um im Ernstfall schnell und adäquat reagieren zu können und das eigene Unternehmen möglichst unbeschadet durch die Krise zu manövrieren. Das ist der Tenor der vier Vortragenden, Florian Schwap, Kommunikationsverantwortlicher der SalzburgMilch, die im Sommer Opfer einer Cyberattacke war, Gottfried Tonweber und Bernhard Zacherl, Cybersecurity-Spezialisten bei EY Österreich und Andreas Windischbauer, Krisenspezialist der Kommunikationsagentur ikp Salzburg.

Die Erfahrung von Florian Schwap zeigt: „Eine 100%ige Sicherheit vor Cyberangriffen gibt es nicht. In der Krise sind ein ruhiger Kopf, unkonventionelle Ideen, flexible und motivierte Mitarbeiter*innen sowie extreme Ausdauer gefragt. Spielen Sie das Szenario Cyberangriff im eigenen Unternehmen durch und nutzen Sie die Zeit vor der Krise, Sie könnten schon morgen das nächste Ziel sein!"

Aufklärung und interne Kommunikation
Cyberkriminelle zielen nicht mehr nur auf die technischen Sicherheitslücken eines Unternehmens ab, sondern zusätzlich auch auf Mitarbeiter*innen als Einfallstor. „Die richtige Vorbereitung ist essenziell, denn sieben von zehn Unternehmen haben ihre Mitarbeiter*innen während der Pandemie ins Homeoffice geschickt. Jedes Unternehmen in Österreich kann Opfer eines Cyberangriffs werden und muss sich besser gestern als heute vorbereiten. Wenn man auf einen Angriff wartet, ist es schon zu spät", so Gottfried Tonweber, Leiter Cybersecurity und Data Privacy bei EY Österreich. Bernhard Zacherl, Director Cybersecurity und Data Privacy bei EY Österreich ergänzt: „Um sich besser zu schützen, haben mehr als die Hälfte der Unternehmen ihre Mitarbeiter*innen für die Thematik Cybersecurity und Datendiebstahl sensibilisiert sowie neue organisatorische Regelungen aufgesetzt. Die Vermittlung des nötigen Know-hows an die eigene Belegschaft ist für eine erfolgreiche Cyberabwehr von elementarer Bedeutung. Mithilfe von regelmäßigen Schulungen, praktischen Trainings und geplanten Phishing-Kampagnen wird das Gefahrenbewusstsein der Angestellten geschärft, um im Berufsalltag richtig agieren zu können".

Content und Kanäle der Krisenkommunikation
In der Krisenkommunikation werden zur Vorbereitung konkrete Szenarien durchgespielt. Das gilt auch für die Kommunikation bei Cyberattacken. Wichtig ist die Diskussion der Kommunikationsstrategie bereits im Vorfeld. In der Vorbereitung wird definiert, wer in der Krise spricht und konkrete Inhalte und Textbausteine werden formuliert. Kanäle, die kurzfristig bespielbar sind, wie eine App für Mitarbeitende, die Website und Social Media sind essentielle Werkzeuge für die Cyberkrisenkommunikation. Andreas Windischbauer, Geschäftsführer von ikp Salzburg: „Strategisch geleitete Kommunikation ist eine wichtige Voraussetzung um Krisen erfolgreich zu bewältigen. Im Ernstfall ist es wichtig, dass die Mitglieder des Krisenstabs und externe Expert*innen gut abgestimmt arbeiten und auf mögliche Szenarien vorbereitet sind." Daher bietet die Kommunikationsagentur ikp Salzburg in Zusammenarbeit mit Spezialist*innen aus den Bereichen IT, Recht und Cybersecurity Workshops zum Thema Cyberkrisenkommunikation an.

Industriellenvereinigung Salzburg empfiehlt Notfallpläne
„Die kriminellen Aktivitäten treten in unterschiedlichsten Spielarten in Erscheinung: von der CFO-Fraud, also fingierten Zahlungsanweisungen durch einen Vorgesetzten bis hin zum klassischen Hackerangriff, der den Betrieb lahmlegt und Lösegeldforderungen beinhaltet", erklärt Irene Schulte, Geschäftsführerin der IV-Salzburg, und betont weiter: „Die Unternehmen widmen erhöhte Aufmerksamkeit dem Thema Cybersecurity. Es gilt, das Bewusstsein der Mitarbeitenden zu schärfen, den IT-Bereich entsprechend gut aufzustellen und die Prozesse im Background anzupassen. Die Industriellenvereinigung will ihre Mitgliedsbetriebe mit Erfahrungsaustausch stärken und empfiehlt Notfallpläne für das Krisenmanagement und die Krisenkommunikation zu erstellen. Von den Betroffenen können wir lernen, wo rasch Hilfe zu bekommen ist und wie Reputationsschäden abgewendet werden können."

www.ikp.at