Sortierzentrum: Dank digitalem Scan jedes Paketes erfahren auf dem Postportal www.post.ch registrierte Empfänger per SMS oder E-Mail, wie gross und schwer die Sendung ist und und an welchem Tag sie zugestellt wird. ZVG

Für KMU kein Thema?

Cyber-Kriminalität KMU stellen ein leichtes Ziel dar, da sie der Sicherheit oft nicht genug Aufmerksamkeit widmen.

ROMAN HALTINNER

Cyber-Kriminalität ist ein globales Milliardengeschäft. Auch mit Opfern in der Schweiz. Erpressung mit der Hilfe von Verschlüsselungstrojanern und Manipulation von Zahlungsflüssen unter Verwendung von Trojanern ist derzeit eine beliebte Masche der Cyber-Kriminellen, die auf einen schnellen finanziellen Gewinn aus sind. Anfang dieses Jahres beispielsweise wurde publik, dass ein KMU Opfer eines Cyber-Angriffes geworden war. Cyber-Kriminelle waren mittels Schadsoftware in das Netzwerk der Firma eingedrungen. Sie gaben im Namen des Unternehmens Zahlungen in der Höhe von 423 000 Franken über diverse Banken in Auftrag. Nur verschieden nachgelagerte Sicherheitsmechanismen bei den involvierten Banken verhinderten einen Totalverlust und hohen finanziellen Schaden.

Dieses Ereignis zeigt, welche Gefahren für KMU durch Cyber-Angriffe entstehen, verursacht durch einzelne Hacker oder professionelle kriminelle Organisationen. Das Management eines KMU steht vor der Herausforderung, sicherzustellen, dass die Bedrohung für das Unternehmen verstanden wird, die richtigen Massnahmen getroffen und die richtigen Prioritäten gesetzt werden. Dies ist, angesichts der Komplexität der Technologie und des Tempos der Veränderung, der sie unterworfen ist, keine leichte Aufgabe. Für Nichtspezialisten in diesem Gebiet ist es oft schwierig, zu verstehen, wie sie mit der Thematik umgehen sollen und sich auf die wesentlichen Massnahmen konzentrieren können. Das Verständnis der Bedrohung sowie die Art des Angriffes sind jedoch zentral, um eine essenzielle Voraussetzung zur Beurteilung zu schaffen und Aussagen darüber zu treffen, inwieweit die Organisationen ein Ziel für solche kriminellen Handlungen sind.

Verantwortung den Experten zu überlassen, gilt nicht als Entschuldigung.

Wer sind die Täter?

Unter Cyber-Kriminalität versteht man Straftaten unter Ausnutzung elektronischer Infrastruktur, die bei Unternehmen materielle oder auch immaterielle Schäden verursachen. Der Begriff deckt ein breites Spektrum von Zielen und Angriffsmethoden ab. Das Verstehen von Tätern, also deren Motivation, Organisation und Auftraggeber sowie die Art der Durchführung solcher Angriffe, ist unerlässlich für effektive Massnahmen gegen Cyber-Kriminalität.

Ein wesentlicher Teil analoger Straftaten, die einen direkten Vermögensvorteil zum Ziel haben, verschiebt sich in die digitale Welt – das heisst, dass sie sich im Internet abspielen. Verbrechen geschehen nicht mehr nur im Rahmen krimineller Strukturen, sondern jederzeit und überall. Genaue Zahlen zu Meldungen und Verurteilungen von Cyber-Delikten gibt es aufgrund einer hohen Dunkelziffer zwar nicht, doch – ausgehend von aktuellen Entwicklungen – wird die Bedeutung von Cyber-Kriminalität weiter zunehmen. Dass das Ziel solcher Aktivitäten sich nicht nur auf grosse Unternehmen beschränkt, sondern auch kleinere Unternehmen betroffen sind, zeigt das eingangs erwähnte Beispiel.

Cyber-Risiken sind eine grosse und vielfältige Herausforderung für die Führung von Unternehmen. Die Entschuldigung, die Verantwortung den Experten zu überlassen, soll dabei nicht gelten. Es ist wichtig und unerlässlich, dass die Unternehmensführung das Unternehmen in den folgenden Bereichen lenkt und verantwortet:

– Zuteilung von Ressourcen, um Cyber-Security betreiben zu können.
– Eine unternehmensweite Governance, die eine risikobasierte Entscheidungsfindung erlaubt.
– Eine Unternehmenskultur, in der jeder um seine Verantwortung weiss.

Unternehmen können die Risiken für ihr Geschäft durch den Aufbau von Kapazitäten in den folgenden drei kritischen Bereichen reduzieren: Prävention, Erkennung und Reaktion.

- **Prävention:** Beginnt mit der Governance und Organisation des Unternehmens. Es geht neben strategischen und taktischen auch um technische Massnahmen, einschliesslich der Verantwortung für den Umgang mit Cyber-Security innerhalb der Unternehmung, sowie Sensibilisierungsmassnahmen für die Schlüsselmitarbeiter.
- **Erkennung:** Durch die Überwachung von kritischen Ereignissen und Sicherheitsvorfällen kann ein Unternehmen seine Erkennungsmassnahmen stärken. Überwachung und Aufzeichnung von Daten bilden zusammen ein ausgezeichnetes Instrument, um auffällige Muster im Datenverkehr zu erfassen und den Ort der Angriffe zu lokalisieren.
- **Reaktion:** Bezieht sich auf die Aktivierung eines Plans, sobald ein Angriff stattfindet. Bei einem Angriff sollte die Unternehmung in der Lage sein, die betroffene Technologie sofort zu deaktivieren. Bei der Entwicklung einer Reaktion und dem Wiederherstellungsplan sollte eine Unternehmung Informationssicherheit als kontinuierlichen Prozess etablieren und nicht als eine einmalige Aktivität ansehen.

Vertrauen der Stakeholder gewinnen

Das Thema Cyber-Security muss auf jeder Managementagenda eines KMU stehen. Alle Stakeholder – der Verwaltungsrat, die Aktionäre und die Kunden – erwarten, dass das Unternehmen dieser Herausforderung genügend Aufmerksamkeit schenkt. Die Unternehmensleitung muss also in der Lage sein, bei der Umsetzung von Cyber-Security die richtigen Fragen zu stellen, um so durch die Komplexität des Themas zu navigieren und damit das Vertrauen aller Beteiligten zu gewinnen.

Roman Haltinner, Director Cyber Security Services, KPMG, Zürich.

Cyber-Sicherheit: Die fünf grössten Irrtümer

Irrtum 1: «100 Prozent Sicherheit»
Die Entwicklung eines Bewusstseins, dass es 100 Prozent Schutz vor Cyber-Kriminalität gibt. Dies ist weder machbar noch ein geeignetes Ziel. Es ist aber ein wichtiger Schritt auf dem Weg zu einer effektiven Sicherheitspolitik, die es dem Unternehmen erlaubt, Entscheidungen über sein Abwehrdispositiv zu treffen. Wirksame Abwehrmassnahmen setzen beim Verständnis der Bedrohung (der Täter und ihrer Tathandlungen) an. Diese enthalten Massnahmen in Bezug auf organisatorische Schwachstellen (Prävention), die Implementierung von Mechanismen, um drohende oder tatsächliche Vorfälle (Erkennung) zu erfassen, sowie die Fähigkeit, auf Vorfälle (Reaktion) sofort zu reagieren, um Verluste zu minimieren.

Irrtum 2: «Wir investieren in die Sicherheit, indem wir die besten erhältlichen Sicherheits-Tools implementieren»
Das Thema Cyber-Security wird auf dem Markt durch spezialisierte Anbieter von technischen Sicherheitsprodukten geprägt. Diese Werkzeuge sind für die Basissicherheit unerlässlich und müssen in die IT-Architektur integriert werden. Sie sind aber nur ein Teil und nicht die Grundlage einer ganzheitlichen und robusten Cyber-Security-Politik. Die Investition in technische Hilfsmittel sollte eine Massnahme und nicht der Treiber der Cyber-Security-Strategie sein. Es ist wichtig, dass Führungskräfte Verantwortung für den Umgang mit dieser Herausforderung übernehmen. Die Technologie allein kann in dieser Hinsicht nicht helfen. Sie müssen auch bereit sein, Mitarbeiter zu schulen, um das Bewusstsein für die Bedrohung durch Cyber-Angriffe zu fördern.

Cyber-Sicherheit wird oft als Verantwortung einer Abteilung gesehen.

Irrtum 3: «Unsere Abwehrmassnahmen reichen gegen Angriffe der Hacker aus»
Die Bekämpfung von Cyber-Kriminalität ist ein markantes Beispiel für einen nicht zu gewinnenden Wettlauf. Die Angreifer sind bei der Entwicklung neuer Methoden und Technologien gegenüber den Verteidigern immer einen Schritt voraus. Aber ist es wirklich sinnvoll, in Abwehrmassnahmen zu investieren, um mit den immer raffinierter werdenden Werkzeugen der Angreifer Schritt zu halten?

Ja, es ist wichtig, den präventiven Ansatz und die damit verbundenen Abwehrmassnahmen auf dem neuesten Stand zu halten, um so einen Einblick in die Absichten der Angreifer und deren Methoden zu erhalten. Das Management muss den Wert der Informationen im Unternehmen und die Implikation auf das Kerngeschäft bei einem Verlust dieser Informationen verstehen. Die Cyber-Security-Strategie und -Politik braucht es, um Investitionen in diesem Bereich zu priorisieren, anstatt zu versuchen, alle Risiken abzudecken. Kurz gesagt sollte das Management sich der neuesten Techniken bewusst sein, sie aber risikobasiert und gezielt gegen ihre Bedrohungen einsetzen.

Irrtum 4: «Überwachung ist alles»
Nur Unternehmen, die in der Lage sind, externe Entwicklungen und Trends zu verstehen, und diese Erkenntnis nutzen, um die Sicherheitspolitik und -strategie anzupassen, sind auf lange Sicht in der Prävention erfolgreich. Die Praxis zeigt, dass Cyber-Security stark von der Compliance getrieben wird. Dies ist verständlich, denn viele Unternehmen müssen eine Reihe von Gesetzen und Vorschriften erfüllen. Allerdings ist es kontraproduktiv, die Compliance alleine als das ultimative Ziel der Cyber-Security-Politik zu betrachten.

Irrtum 5: «Wir stellen die besten Experten an, um uns gegen Cyber-Kriminalität zu schützen»
Cyber-Sicherheit wird oft als Verantwortung einer Fachabteilung von Informationssicherheitsexperten gesehen. Diese Denkweise kann ein falsches Gefühl von Sicherheit hervorrufen. Die eigentliche Herausforderung ist, Cyber-Sicherheit zu einem Mainstream-Ansatz zu machen. Dies bedeutet, dass Cyber-Sicherheit zu einem Teil der organisationsweiten Vorgaben und Richtlinien wird.

Dies bedeutet aber auch, dass Cyber-Sicherheit als eine zentrale Funktion in die Entwicklung neuer IT-Systeme einbezogen wird und dass nicht – wie häufig – erst am Ende solcher Projekte um ihre Zustimmung angefragt wird. (rh)