«Viele kennen ihre Kronjuwelen nicht»

Durch Homeoffice erhöht sich die digitale Vulnerabilität. Max Keller von der Funk Gruppe, einem international tätigen Versicherungsbroker, zeigt auf, wie sich Unternehmen wappnen können.

VON THOMAS BERNER

Max Keller leitet das Funk Risk-Lab und ist für die Weiterentwicklung, Ausbildung, Marktforschung und Beratung rund um das Risikomanagement Funk Schweiz und Liechtenstein verantwortlich. Mit dem kürzlich abgeschlossenen MAS Digital Business (Vertiefungsrichtungen: Digital Risk Management und disruptive Technologien) hat er eine solide Grundlage für die Beratung von Unternehmen hinsichtlich digitaler Risiken gelegt.

ORGANISATOR **Herr Keller, geht eine Arbeitsverlagerung ins Homeoffice mit erhöhten Sicherheitsrisiken einher? Warum?**

MAX KELLER Definitiv. Die technischen und organisatorischen Schwachstellen im Homeoffice sind nun auch das Problem der Unternehmen.

Was bedeutet das konkret?

Nutzer und damit auch Mitarbeitende gehen im Privaten noch viel sorgloser mit Daten, Internet und Computer um als im beruflichen Umfeld. Untersuchungen aus Deutschland zeigen, dass immer noch zu viele private Geräte weder passwortgeschützt sind – von Zwei-Faktor-Authentifizierung ganz zu schweigen – noch mit einem Antivirenprogramm gescannt werden. Zugleich wird aber jedes zweite private Gerät für berufliche Zwecke verwendet. In der Schweiz und in Liechtenstein wird es wohl nicht viel anders aussehen. Werden schlecht geschützte private Geräte für berufliche Zwecke gebraucht, können vertrauliche oder schützenswerte personenbezogene Daten kompromittiert werden oder Cyberkriminellen der Zugang zu den Unternehmensnetzwerken eröffnet werden.

Wie äussert sich die erhöhte Gefahrenlage in der Realität?

Zum Beispiel durch die starke Zunahme von Phishing-Angriffen. Diese versuchen insbesondere jetzt, in Zeiten hoher Unsicherheit im Zusammenhang mit Covid-19, die Ängste und Neugierde der Menschen gezielt auszunutzen. Gleichzeitig konnte auch eine enorme Zunahme von Angriffen auf das Remote Desktop Protocol (RPD) beobachtet werden, welches von vielen Unternehmen für den Fernzugriff aus dem Homeoffice auf die Firmennetzwerke genutzt wird. Wir haben also einerseits mehr Schwachstellen und andererseits die Zunahme von Cyberangriffen und deren Versiertheit.

Sind sich die Unternehmen gemäss Ihren Erfahrungen als Spezialist für Digital Risk Management der Situation bewusst?

Ja, das sind sie. Wir merken, dass die Unternehmen verstärkt nach Lösungen für die Sensibilisierung von Mitarbeitenden suchen, um dem Phishing-Angriffen vorzubeugen. Andererseits merken wir auch, dass die Unternehmen die Verlagerung von Geschäftstätigkeiten ins Homeoffice als eine Gefahrerhöhung im Rahmen einer Cyberversicherung anzeigen.

Welche anderen Missstände unterminieren die eigene Cybersicherheit?

Die fehlenden personellen Ressourcen etwa: Die meisten IT-Abteilungen in KMU sind unterbesetzt. Da der IT-Betrieb und der First-Level-Support vorgehen, gibt es oft ungenügende Ressourcen für Sicherheit. Aber auch Kommunikationslücken sind eine Herausforderung.

Kommunikationslücken zwischen wem?

Viele Untersuchungen deuten darauf hin, dass das Sicherheitsgefühl der Geschäftsleitung und das der IT-Verantwortlichen stark voneinander abweichen. So sind signifikant weniger Geschäftsleitungsmitglieder bereit, stärker in Cyber-Security zu investieren als IT-Verantwortliche. Zudem schätzt die Geschäftsleitung die Eintrittswahrscheinlichkeiten von Cyberrisiken viel geringer ein als ihre IT-Mitarbeitenden. Es gibt also eine klare Diskrepanz in der Wahrnehmung von Cyberrisiken, die sich auch auf das IT-Wissen zurückführen lässt. Ma-

© FUNK GRUPPE

Max Keller von der Funk Gruppe: «Generell sollte das Cyber-Security-Budget für den grundlegenden Schutz ca. 15 Prozent des gesamten IT-Budgets ausmachen..»

nagement Attention ist das A und O. Nur wenn das Management die Gefahrenlage versteht, können auch entsprechende Mittel für die Sicherheit gutgesprochen werden.

Die Unternehmen wären also gut beraten, hier mehr Geld in die Hand zu nehmen.

Generell sollte das Cyber-Security-Budget für den grundlegenden Schutz ca. 15 Prozent des gesamten IT-Budgets ausmachen. Wenn wir uns die Realität anschauen, sind wir noch weit davon entfernt. Gerade vor dem Hintergrund der Homeoffice-Schwachstellen sollte das Budget noch ansteigen. Diese lassen sich nur durch zusätzliche Aufwendungen bewältigen. Unternehmen sollten sich fragen, ob sie genügend in die Sicherheit ihres Unternehmens und ihrer Kunden investieren. Zur Kalkulation eines zweckmässigen Cyber-Security-Budgets können unterschiedliche Open-Source-Tools genutzt werden.

Gibt es neben den von Ihnen angesprochenen Kommunikationslücken noch andere Faktoren, welche die Investitionsbereitschaft hemmen?

Sicherheit ist für viele Unternehmen ein Kostentreiber und generiert augenscheinlich keine Umsätze. Kennzahlen wie Return on Security Investment sind dem Grossteil der Unternehmen noch unbekannt. Das Fehlen von Sicherheit führt ja auch nicht gleich zu einem Verlust respektive Schaden. Es ist also ein Wagnis, das viele Unternehmen eingehen.

Ist digitale Sicherheit gerade für kleinere Betriebe überhaupt finanzierbar? Und: Von welchen Beträgen reden wir hier?

Zweckmässigkeit ist wichtig. Ein KMU braucht kein Security Operation Center. Die Basic-Cyber-Security-Hygiene sollte aber mit angemessenen Investitionen zu bewerkstelligen sein. Einen Betrag zu nennen ist schwierig, da die Kosten von vielen Faktoren abhängen: Anzahl Server, Clients, Anzahl Mitarbeitende, Applikationen, Cloud-Services, automatisierte Produktionsanlagen etc.

Wie wichtig ist es, dass Betriebe Expertise über das Operieren der Urheber von Cyberattacken aufbauen?

Sehr wichtig. Unternehmen können ihre IT-Systeme nicht effektiv verteidigen, wenn sie nicht wissen, wie Angreifer vorgehen. Die Angreifer wissen hingegen ganz genau, wo die Schwachstellen liegen könnten. Das ist so ähnlich wie bei einem Fussballspiel. Je besser Sie den Gegner vor dem Spiel analysieren, desto besser sind Sie auf ihn vorbereitet. Die wichtigsten Fragen dabei: Wie schaffen es die Angreifer in die IT-Systeme? Und was, wenn sie es geschafft haben? Wie bewegen sie sich darin? Wie versuchen sie an vertrauliche Informationen zu kommen oder ihre Benutzerrechte zu eskalieren?

Wissen die Unternehmen denn genau, was sie schützen sollen?

Fehlende Risikotransparenz ist in der Tat eine grosse Herausforderung. Viele KMU wissen nicht, was genau ihre Assets sind, beziehungsweise kennen ihre Kronjuwelen nicht. Auf den ersten Moment kann das Unternehmen als nicht sehr interessant für Cyberkriminelle betrachtet werden. Auf den zweiten Blick könnte es aber sein, dass sie es auf Kunden des Unternehmens abgesehen haben. Hier gilt es, über den Tellerrand hinauszudenken. Unternehmen sollten sich vor allem auch überlegen, was sie ein erfolgreicher Cyberangriff kosten könnte, wenn dadurch die Verfügbarkeit der IT-Systeme gestört oder die Vertraulichkeit oder Integrität ihrer Daten verletzt wird.

Wie können Unternehmen Risikotransparenz herstellen?

Unsere Erfahrung hat gezeigt, dass das Schaffen von Risikotransparenz an erster Stelle stehen sollte. Dabei kann das Digital Risk Management eine zentrale Rolle einnehmen. Wir empfehlen, sich die Cyberrisiken aus der klassischen Risikomanagementperspektive anzuschauen. Sprich: Eintrittswahrscheinlichkeit und Schadensausmass. Ersteres ist nur schwer zu beschreiben, geschweige denn zu quantifizieren. Grundsätzlich deuten mehr Schwachstellen – Vulnerabilities –, ein geringer Reifegrad der Cyber-Security-Massnahmen und wertvolle Assets auf eine deutlich erhöhte Eintrittswahrscheinlichkeit hin. Was aber quantifiziert werden kann, ist das Schadensausmass. Unternehmen sollten sich überlegen, inwieweit ihre Geschäftsprozesse von der IT abhängig sind und was ein mehrtägiger IT-Systemausfall für sie bedeuten würde. Andererseits sollten auch die verarbeiteten Daten und die deren Sensibilität betrachtet werden. Stichwort: Datenschutzrisiko.