Hand aufs Herz, nehmen Sie Cyberrisiken ernst?

Immer mehr Initiativen weisen auf die Bedeutung von Cyberrisiken hin. Kleine und mittlere Unternehmen (KMU) sind für Cyberangriffen ebenso anfällig wie Grossunternehmen. Das bedeutet, dass ein KMU, dass seine Mitarbeitenden nicht auf mögliche Cybergefahren hinweist und in dieser Hinsicht schult, Gefahr läuft, unternehmenskritischen Daten zu verlieren.

>> Interview von Ursula Moonen | moonen communications GmbH

Phishing-Nachrichten per E-Mail oder SMS, Ransomware-Bedrohungen, Identitätsdiebstahl – die Liste der möglichen IT-Schwachstellen, die Unternehmen das Leben schwer und teuer machen können, ist lang.

«Zwei Drittel aller Schweizer KMU stufen IT-Sicherheit als wichtig ein. Aber nur 18 Prozent befürchten, selbst angegriffen zu werden. Denn KMU sind durchaus lohnende Ziele für Attacken von Cyberkriminellen», laut gfs.Zürich Studie: «Homeoffice und Cybercrime in KMU 2022»

Am Markt gibt es viele technischen Lösungen, Schulungen und Expertentum. Trotzdem setzen sich KMU immer noch dem Risiko aus, von einem Cyberangriff getroffen zu werden. Was tun, wenn die Handlungsfähigkeit ausser Kraft gesetzt wird? Warum sind KMU so zaghaft darin, sich vor Cyberrisiken zu schützen?

Im Interview mit einem KMU stellen wir Hardy Ruoss, Mitinhaber der beiden mittelständischen Unternehmen Diag AG und UCSP Schweiz AG, diese Frage. Er hat sich eingehend mit der Frage befasst, wie er seinen KMU-Kunden eine auf deren Anforderungen zugeschnittenen Lösung anbieten kann.

Ursula Moonen: Herr Ruoss, Sie stellen kleine und mittlere Unternehmen eine funktionierende IT-Infrastruktur zur Verfügung. Unter dem Dach der UCSP Schweiz bündeln Sie Partner, mit denen Sie gemeinsam die Kundenanforderungen abdecken. Warum nehmen Sie jetzt das Thema Cyberrisiken mit in Ihr Partner-Angebot auf?

Hardy Ruoss: Das Thema selbst brennt unseren Kunden unter den Nägeln. Die fast täglichen Informationen in den Medien verunsichern viele KMU. Ausserdem werden an KMU- Veranstaltungen und im Web vielfältige Produkte, Lösungen und Beraterkompetenzen angeboten. Langsam wird es den Geschäftsinhabern bewusst, dass die ganze Security-Thematik mittlerweile real ist und es jeden treffen kann – mit mittleren bis schweren finanziellen Folgen.

Die zunehmende Digitalisierung von Geschäftsprozessen, die Home-Office Pflicht während der Pandemie und die generell schnelle technische Entwicklung tun ihr Übriges.

Stellen Sie sich ein Unternehmen in der Grössenordnung von 1 bis 49 Mitarbeitenden vor. Wann und wie soll der oder die Verantwortliche neben der Haupttätigkeit noch die Zeit finden, sich mit der komplexen Thematik der Cyberrisiken auseinanderzusetzen? Fragen wie beispielsweise hinsichtlich des richtigen IT-Sicherheitstools und dessen Handhabung sowie das Monitoring der Angriffsfläche oder des Dienstleisters und das kontinuierliche Verfolgen von Entwicklungen am Markt sind dann nur schwer zu bewältigen.

Hinzu kommt, dass auch unsere KMU-Kunden und Kundinnen gezwungen sind, sich auf ihrem Fachgebiet mit erweiterten Kundenanforderungen und Neuerungen auseinanderzusetzen.

Braucht es für solche Unternehmen speziell aufbereitete Dienstleistungen?

Ja, unbedingt. Aus eigener Erfahrung – wir sind selbst ein kleines Unternehmen im Sinne von KMU – ist es unsere Intention, Partner im Angebot der UCSP Schweiz aufzunehmen, die Unterstützung bieten und kein «Overkill» für ein KMU sind. Diese Partner verfügen über eine ausgewiesene Expertise auf ihrem Gebiet. Es ist für ein KMU wichtig, genau das zu bekommen, was für ihre Grösse auch notwendig ist, und zwar einfach und pragmatisch.

Hardy Ruoss

«Langsam wird es den Geschäftsinhabern bewusst, dass die ganze Security-Thematik mittlerweile real ist und es jeden treffen kann – mit mittleren bis schweren finanziellen Folgen.»

Unter dem Label «SecurityToday by UCSP» haben wir 3 Schwerpunkte aufgegriffen:

1. **Der Faktor Mensch – Bewusstsein für Sicherheit schaffen**
   Vielen KMU ist bewusst, dass mit versehentlichem Klicken auf einen Link oder dem Öffnen eines Anhangs einer Mail die Gefahr besteht, dass Hacker sich Zugang zum Unternehmen verschaffen. Für unabsehbare Zeit kann dann nicht mehr auf unternehmenskritische Daten zugegriffen werden. Alles steht still. Gezielte Aufklärung und Schulung für Mitarbeitende tut Not. re4ming bietet eine passgenaue Lebenshilfe online und on Site an.

2. **Ein webbasierter Dateien-Bereiniger, der die Datenintegrität sicherstellt**
   Damit sichergestellt ist, dass in einem E-Mail-Anhang keine schädliche Software eingebaut wurde, scannt der Dateien-Bereiniger nicht nur, sondern entfernt gegebenenfalls Schadsoftware und versteckte Textnachrichten. Die im Alltag anfallenden Verträge, Lebensläufe, Rechnungen und vieles mehr können anschliessend geöffnet und bearbeitet werden. Virotron, ein Produkt von basics4net, ist weitere effiziente Lebenshilfe.

3. **Der «Security-Checker»,** der alle potenziell sicherheitsrelevanten IT-Schwachstellen unter die Lupe nimmt und die IT oder Prozesse des Unternehmens unter dem Aspekt der Sicherheit betrachtet.

Die individuellen Unternehmensprozesse eines KMU aus der Sicht eines imaginären Cyberkriminellen zu analysieren, ist das dritte Thema, das wir unter dem Blickpunkt der Lebenshilfe in das Partnerportfolio aufgenommen haben. freudiger IT services schaut genau, sehr genau dorthin, wo gerne weggeschaut wird, sei es aus Bequemlichkeit oder Unwissen.

Herr Ruoss, welchen Rat möchten Sie Ihren Kunden mit auf den Weg geben?

Um Ängste und Vorbehalte zu minimieren, empfehle ich, den Ernstfall gedanklich durchzuspielen. Stellen Sie anschliessend die Themen zusammen, die Ihnen Kopfschmerzen bereiten oder Fragen aufwerfen. Welche Gefahrenquellen und Lösungen sind Ihnen bekannt, aber noch nicht gelöst? Diese erste Risikoabschätzung verschafft Ihnen die Klarheit, den ersten Schritt zur Sicherung Ihrer unternehmenskritischen Daten.

Vielen Dank für Ihre Erläuterungen, Herr Ruoss.

UCSP Schweiz AG, Lachen, ist ein mittelständisches, unabhängiges, inhabergeführtes Unternehmen. Seit 2012 arbeiten es mit einer Vielzahl von Resellern erfolgreich zusammen.
www.ucsp-schweiz.ch
www.securitytoday.ch

Diag AG, Lachen, stellt state-of-the-art IT-Infrastruktur zur Verfügung, vor Ort, im Mietmodell oder als Kaufvariante. Aus zwei Schweizer Datacenter greifen Kunden auf die individuellen Cloud Lösungen zu.
www.diag.ch

Die Autorin

Ursula Moonen bietet als Inhaberin der moonen communications GmbH Kommunikations-Unterstützung in Transformationsprozessen an. Die gebürtige Niederländerin und Schweizerin verfügt über eine mehr als 25-jährige Berufserfahrung in der IT-Industrie.
www.moonen-communications.ch

Dieser Beitrag wurde ermöglicht durch moonen communications GmbH. Basierend auf einer ganzheitlichen Sicht auf die Kundenbeziehungen eines Unternehmens und deren kontinuierliche Entwicklung erarbeitet moonen communications eine passgenaue und differenzierte Zielgruppenansprache.