Tipps für KMU

Unternehmensnetzwerke sind in der Regel schwieriger vor cyberkriminellen Angriffen zu schützen als private. Grund dafür sind die höhere Komplexität und die gravierenderen wirtschaftlichen Folgen von Störungen oder Ausfällen. Griffige Massnahmen zur Risikominderung sind daher unumgänglich.

Wichtigste Merkpunkte:

- Stützen Sie sich für die Abwägung der Risiken und der Umsetzung von Massnahmen auf **Leitfäden und Merkblätter** etablierter Institutionen ab.
- Identifizieren Sie, welche **Prozesse, Systeme und Daten** für Ihr Unternehmen am wertvollsten sind und gehen Sie diese zuerst an.
- Fassen Sie zur Erhöhung der Informationssicherheit im Unternehmensnetzwerk geeignete sowohl **technische** wie auch **organisatorische Massnahmen** ins Auge.
- Definieren Sie **Verantwortlichkeiten, Zuständigkeiten und Ansprechstellen** für sicherheitstechnische Belange.

Unternehmensnetzwerke sind in der Regel komplexe, oft über längere Zeit gewachsene Strukturen mit zahlreichen Schnittstellen und Datenflüssen zu Kunden und Geschäftspartnern. Bereits kurzzeitige Störungen oder gar Ausfälle dieser Infrastruktur zeitigen oft gravierende wirtschaftliche Auswirkungen für das Unternehmen. Damit sind KMU im Allgemeinen grösseren Risiken durch Cyberkriminalität ausgesetzt als Private.

Um die Widerstandskraft von KMU vor solchen Gefahren – die sogenannte IKT-Resilienz – zu erhöhen und die damit verbundenen Risiken zu minimieren, sind geeignete Schutzmassnahmen vorzusehen. Infolge der Komplexität und des Umfangs sind solche jedoch meist kosten- und ressourcenintensiv. Eine sorgfältige Abwägung ist hier deshalb eminent wichtig.

Leitfäden und Merkblätter nutzen

Wie soll ein KMU diese grosse Aufgabe anpacken? Und wie stellt es sicher, dass nichts übersehen wird?

Viele etablierte Institutionen haben sich dieser Fragen angenommen und sich eingehend mit der Umsetzung von IKT-Schutzmassnahmen speziell für KMU befasst. Im Laufe der Zeit sind so zahlreiche Leitfäden und Merkblätter entstanden, die ein gleichzeitig effizientes wie effektives Vorgehen ermöglichen. Die Anlehnung an solche Hilfsmittel ist deshalb sehr zu empfehlen.

Als Einstieg in die Thematik wäre einmal das «Merkblatt Informationssicherheit für KMUs» (https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html) vom NCSC zu erwähnen. Das sehr kompakte Merkblatt richtet sich explizit an Schweizer KMU und soll diesen dabei helfen, die Informationssicherheit in ihrer Systemlandschaft und im Unternehmensnetzwerk zu erhöhen.

Prozesse, Systeme und Daten identifizieren

Wo und womit soll man beginnen? Welche Prozesse, Systeme oder Daten soll ein KMU zuerst angehen?

Die Basis zur Beantwortung dieser Frage bildet eine (vereinfachte) Risikoanalyse. Dazu sind die, für die Wert-

schöpfungskette des Unternehmens besonders wichtigen Prozesse, Systeme und Daten zu identifizieren und deren Anfälligkeit hinsichtlich IKT-Gefahren zu beurteilen.

Technische Massnahmen ergreifen

Technische Schutzmassnahmen bilden die erste Abwehrkette, wenn es darum geht cyberkriminellen Gefahren zu begegnen. Der Katalog möglicher Massnahmen ist lang. Doch welche Massnahmen sind die richtigen?

Diese Frage hängt stark von der spezifischen Bedrohungslage des KMU ab. Einige technische Massnahmen können aber als allgemeingültig angesehen werden und gehören damit zum Grundschutz jedes KMU. Zu diesen Massnahmen gehören sicherlich:

- Regelmässiges Durchführen von Datensicherungen (Backups) (https://www.ebas.ch/datensicherung-im-kmu-umfeld/)
- Installation und Betrieb eines aktualisierten Virenschutzes (https://www.ebas.ch/virenschutz-im-kmu-umfeld/)
- Einspielen regelmässiger Sicherheitsupdates (https://www.ebas.ch/patchmanagement-im-kmu-umfeld/)

Organisatorische Massnahmen ergreifen

Technische Massnahmen alleine können keinen umfassenden Schutz gewährleisten. Es sind deshalb immer auch ergänzende organisatorische Massnahmen vorzusehen.

Die Liste ist auch bei den organisatorischen Massnahmen umfangreich. Speziell hervorgehoben sollen hier folgende Punkte werden:

- Regelmässige Sensibilisierung und Schulung der Mitarbeitenden
- Etablierung einer strengen Passwort-Policy
- Sichere Abläufe bei kritischen Anwendungen (z.B. Mehr-Augen-Prinzip bei E-Banking-Applikationen)

Verantwortlichkeiten, Zuständigkeiten und Ansprechstellen definieren

Wer verantwortet die Datensicherung? Wer ist zuständig für das Einspielen von Sicherheitsupdates? An wen wenden sich Mitarbeitende, die beispielsweise einen Malware-Befall vermuten?

Für einen reibungslosen Betrieb müssen innerhalb des KMU Verantwortlichkeiten, Zuständigkeiten und Ansprechstellen mit Bezug zu IKT-Sicherheit nicht nur definiert, sondern den Mitarbeitenden auch bekannt sein.

Mittels einer geeigneten Informationsplattform kann ein niederschwelliger Zugang zu den richtigen Stellen gefördert werden. Damit lassen sich die Antwortzeiten auf Vorfälle reduzieren und die Meldequote erhöhen.

Schweizer KMU sind vermehrt Ziel von cyberkriminellen Angriffen mit teils gravierenden Folgen für das betroffene Unternehmen. Deshalb sind Massnahmen zur Risikominderung unumgänglich.