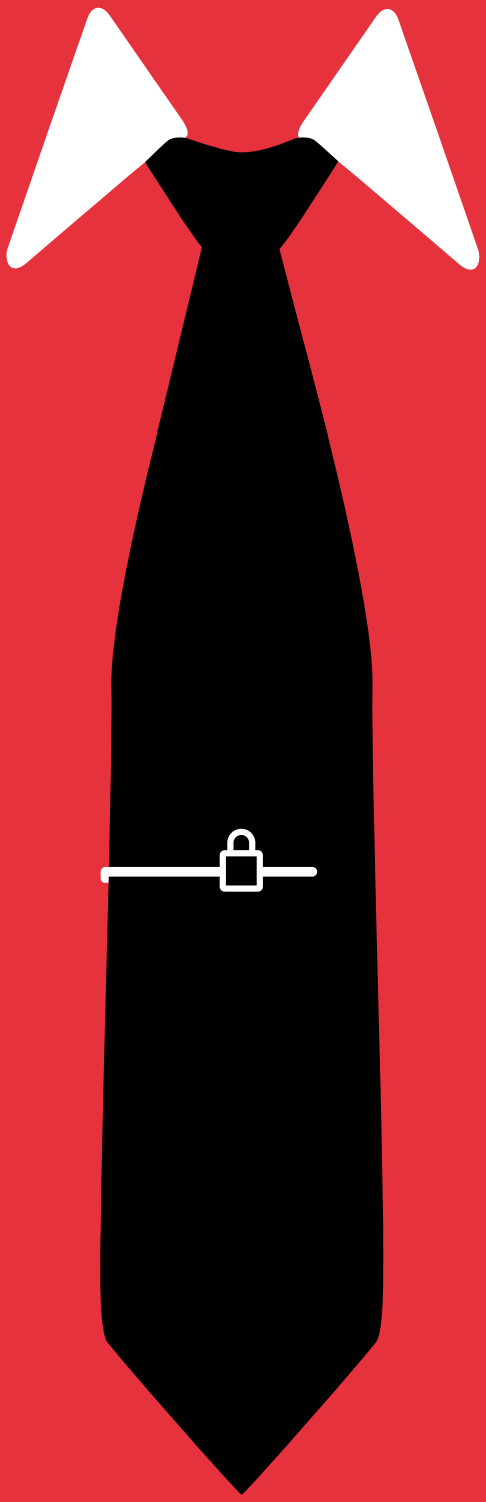


IT-Sicherheit

eine Managementaufgabe

Die digitale Revolution hat nicht nur das Privatleben, sondern auch die Unternehmenswelt auf den Kopf gestellt. Behörden, Institutionen und Organisationen können ohne technische Unterstützung nicht mehr arbeiten oder sind überhaupt nur dank dieser Technologien aktiv. Entsprechend wird die IT-Sicherheit zur zentralen Managementaufgabe avancieren. Denn wenn die Technologie nicht funktioniert, kann das Unternehmen dichtmachen. Schlimmer noch: Es drohen Gefahren, die über das übliche Geschäftsrisiko hinausgehen.

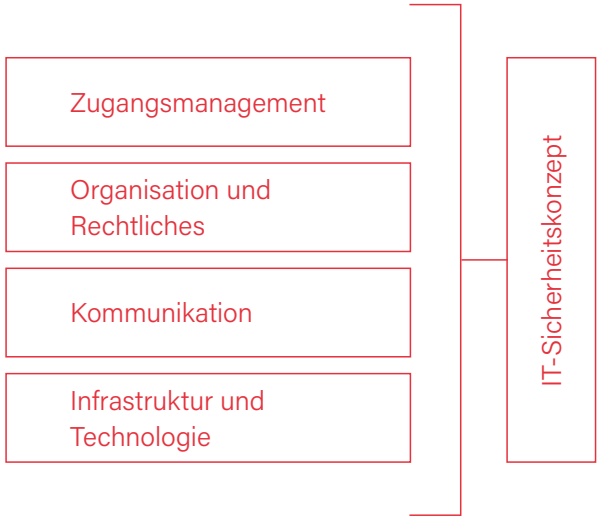
Gemäss einer breit angelegten Studie der FHNW Hochschule für Wirtschaft betrachten 61 % der Schweizer Unternehmen die IT-Sicherheit und den Datenschutz als grösstes Risiko der digitalen Transformation. Ein Drittel der befragten Unternehmen gab sogar an, in den letzten zwei Jahren einen Vorfall wie etwa einen Angriff auf die IT-Infrastruktur und -Daten erlebt zu haben. Die meisten Angriffe auf Unternehmensdaten stammen von kriminellen und staatlich gesponserten Organisationen, wobei auch eine erstaunlich hohe Zahl durch Mitarbeitende (30 %) ausgeführt wird.

Der Website-Betreiber «10 Guards» stellt regelmässig die Preise der im Darknet gehandelten gestohlenen Daten und Dienstleistungen zusammen. Eine Auswahl:
– Kreditkarte mit PIN-Code: USD 15 bis 35
– Online-Banking-Log-in: USD 35 bis 65
– PayPal-Konto: USD 200
– Europäische Identitätskarte: USD 75
– Gehacktes Facebook-Konto: USD 75
– Gehacktes Instagram-Konto: USD 55
– Gehacktes Gmail-Konto: USD 156
– Malware: USD 70 bis 6000
– DDoS-Attacke auf ein beliebiges Ziel: USD 10 bis 800

Die Themenfelder für das eigene IT-Sicherheitskonzept

Zum eigenen IT-Sicherheitskonzept führen die Diskussion, Planung und Implementierung von Massnahmen zu vier zentralen Themenfeldern (vgl. Abbildung):

1. Der Bereich Infrastruktur und Technologie umfasst alle technischen Massnahmen, welche Geräte genutzt werden, wie sie konfiguriert werden sollten und wie sie geschützt werden können.



Die Themenfelder der IT-Sicherheit (N. Mayencourt & M. K. Peter)

2. Die Kommunikation umfasst alle Aspekte der menschlichen Interaktion – mit und über Maschinen. Dabei geht es darum, wie die Sensibilität für Sicherheitsprobleme und sicherheitsrelevantes Verhalten bei den Mitarbeitenden wie auch beim Management erhöht werden können.

3. Organisation und Rechtliches umfasst Regulierungen und Vorschriften, die beschreiben, wie sich die Mitarbeitenden verhalten sollten und wie die Abläufe innerhalb der Organisation gestaltet werden müssen, damit die Sicherheit der IT gewährleistet ist. Die Organisation muss zudem so gestaltet werden, dass sie Gesetzen und internationalen Standards entspricht.

4. Zugangsmanagement: Alle Sicherheitsmassnahmen bauen auf Zugangskontrollen auf. Hier müssen der Zugang zu und der Zugriff auf Systeme geregelt, kontrolliert und protokolliert werden. Zugangskontrollen beinhalten Passwörter, Zutrittskontrollen und die Authentifizierung, Autorisierung und Abrechnung von Anfragen rund um die IT-Systemlandschaft.

Letztlich fügen sich diese Bereiche im IT-Sicherheitskonzept zusammen. Sie definieren für das Unternehmen die notwendigen Vorbereitungen sowie die Umsetzung und überprüfen laufend (vgl. Kapitel IT-Sicherheitsaudit), ob das Konzept dem aktuellen Stand der Angriffstypen, der aktuellen IT-Infrastruktur und der Risikoakzeptanz entspricht.

→

Das Homeoffice

Spätestens seit COVID-19 müssen sich fast alle Unternehmen zusätzlich mit dem Thema Homeoffice und dessen ganz individuellen Herausforderungen befassen. Auch im Homeoffice sind Fragen der IT-Sicherheit wichtig. Prinzipiell sind es dieselben wie am Arbeitsplatz. Wenn jedoch viele Mitarbeitende von zu Hause aus arbeiten, vergrössert sich dadurch die Angriffsfläche der Unternehmung: Die privaten Geräte und Anschlüsse werden Teil des Firmennetzwerks und die privaten Räume Teil der Firmenräume. Ein Einbruch in die privaten Geräte oder das Zuhause der Mitarbeitenden ermöglicht den Zugriff auf Firmendaten und auf die Firmeninfrastruktur. Entsprechend müssen auch die privaten Räume und Geräte sowie das Verhalten der Mitarbeitenden im Homeoffice Gegenstand des IT-Sicherheitskonzepts einer Unternehmung sein. Das ist nicht einfach umzusetzen und zu kontrollieren.

Wichtige erste Tipps sind in der Box aufgeführt. Den Unternehmen wird empfohlen, ihre Mitarbeitenden speziell für die Tätigkeit im Homeoffice (und für das mobile Arbeiten generell) bezüglich der IT-Sicherheit zu sensibilisieren und zu schulen. Als zusätzlicher Schritt wird ein IT-Sicherheitsaudit empfohlen, welches auch die Aspekte des Homeoffice berücksichtigt.

WICHTIGE VERHALTENSREGELN IM HOMEOFFICE

- Nutzen Sie eine VPN-Verbindung, damit die Daten zur Unternehmens-IT verschlüsselt übertragen werden.
- Kommunizieren Sie nur über Unternehmenskonten und nicht über private E-Mail-Konten oder Messenger-Dienste wie WhatsApp.
- Sperren Sie den Computer, auch wenn Sie sich nur kurz vom Arbeitsplatz entfernen.
- Lassen Sie keine vertraulichen Dokumente und Ausdrucke herumliegen.
- Telefonieren Sie nicht auf dem Balkon über Vertrauliches.
- Verschlüsseln Sie IT-Systeme, E-Mails und Datenträger (z.B. USB-Sticks).
- Installieren Sie für Ihre Familie zur Privatnutzung keine Software/Apps.
- Halten Sie Software und Virenschutz auf Ihrem Laptop aktuell.

Das IT-Sicherheitsaudit

Mit dem Begriff «Audit» ist eine unabhängige Untersuchung von Prozessen, Anforderungen und Richtlinien sowie deren Implementierung gemeint. Ein IT-Sicherheitsaudit untersucht also Qualität, Vorhandensein und Einhaltung von IT-Sicherheitsmechanismen in einem Unternehmen. In grossen Unternehmen werden Audits typischerweise von unabhängigen, speziell geschulten Auditoren durchgeführt und sind Teil von oftmals schwerfälligen Qualitätsmanagementprozessen.

Im Rahmen der Vorbereitung eines IT-Sicherheitsaudits ist es wichtig, dessen Ziel klar vor Augen zu behalten. Ein Audit sollte nie zum Selbstzweck verkommen. Stattdessen sollte zu Beginn genau überlegt werden, was erreicht werden soll. Ein typisches Ziel kann sein, die Einhaltung von gesetzlichen oder regulatorischen Vorgaben nachzuweisen, Zertifizierungen zu erlangen oder zu behalten. Man spricht dann häufig von «Compliance». Ist die Entscheidung gefallen, ein IT-Sicherheitsaudit zur Erhöhung der Resilienz und zum Schutz der Wertschöpfungskette durchzuführen, sollte diese Entscheidung festgehalten und kommuniziert werden. Die kommunizierte Zielsetzung des Audits wird somit zum Dreh- und Angelpunkt für alle anstehenden Diskussionen und Entscheidungen. Mit der klaren Zielsetzung geht auch eine realistische Erwartungshaltung einher: Perfekten Schutz vor sämtlichen Gefahren gibt es nicht – nichts passieren kann nur jemandem, der nichts tut. Da Nichtstun aber keine Option ist, gilt es, eine Balance zu finden: Die Wertschöpfungskette sollen bestmöglich geschützt und die Risiken mittels kosteneffizienter Massnahmen minimiert oder idealerweise aus der Welt geschafft werden. Es gilt: So viel wie nötig, so wenig wie möglich.

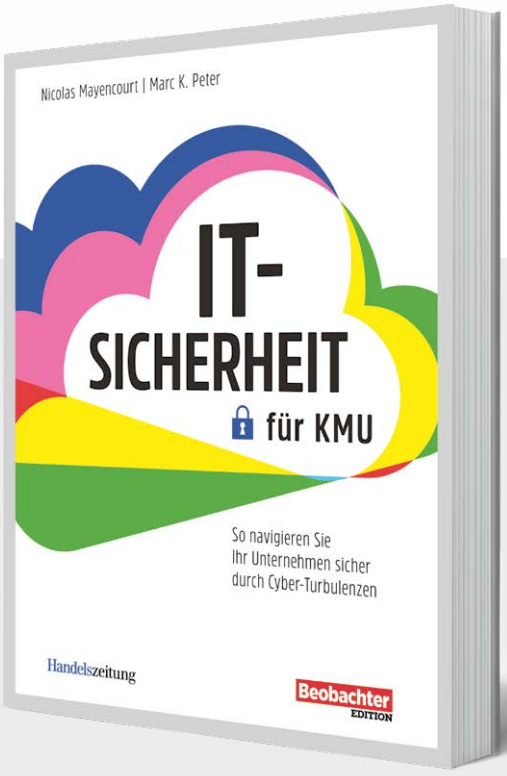
Abgesehen von einigen universellen Sicherheitspraktiken hängt die Auswahl der passenden IT-Sicherheitsmassnahmen stark von der individuellen Ausgangslage eines Unternehmens ab. Die gute Nachricht ist aber, dass der Weg zum Identifizieren dieser Massnahmen für jedes Unternehmen mehr oder weniger gleich aussieht. In einem ersten Schritt geht es darum, sich bewusst zu machen, wie und wo der Umsatz entsteht, was ihn aus IT-Sicht in Gefahr bringen kann und was dagegen zu tun ist. Bei der Risikoanalyse und dem Festlegen von Massnahmen sollten je nach Bedarf Experten beigezogen werden.

IT-Sicherheitsaudits kennen viele Ausprägungen. Unter anderem lassen sich folgende Arten ausmachen:

- Bei einem Penetrationstest nehmen die Sicherheitsexperten die Perspektive eines Einbrechers ein. Sie suchen nach Wegen, in die geschützten Netzwerkbereiche einzudringen, um etwa vertrauliche Daten zu entwenden.
- Bei einem fokussierten Audit wird ein Bereich des Netzwerks, eine einzelne Komponente, eine Software oder App einer Sicherheitsprüfung unterzogen.
- In einem kompletten Audit wird die ganze Infrastruktur auf Verwundbarkeiten und Schwachstellen untersucht oder komplett analysiert.
- In einem Red-/Blue-Teaming greift das rote Team die IT-Infrastruktur eines Unternehmens an. Gleichzeitig versucht das blaue Team, den Angriff abzuwehren. Bei dieser Simulation zeigen sich sowohl die Schwachstellen als auch die Resilienz der IT-Sicherheitsvorkehrungen.

Weitere Informationen finden Sie auf:
www.it-sicherheit-kmu.ch
www.dreamlab.net

Marc K. Peter, Professor an der FHNW Hochschule für Wirtschaft, Olten
Nicolas Mayencourt, Gründer und CEO von Dreamlab Technologies



DAS PRAXISHANDBUCH ZUR IT-SICHERHEIT

Das in der Edition Beobachter & Handelszeitung erschienene Praxishandbuch «IT-Sicherheit für KMU» richtet sich gezielt an kleine und mittelgrosse Schweizer Unternehmen und zeigt, wie sie sich vor IT-Angriffen schützen können. Um technische Inhalte, Konzepte und Anwendungen im Praxishandbuch vereinfacht darzustellen und verständlicher zu erklären, helfen drei fiktive Fallstudien, davon eines von einem Ingenieurbüro.

Nur mit einer aktiven Diskussion und Planung können Unternehmen die IT-Sicherheit als Wettbewerbsvorteil nutzen; die IT-Sicherheit wird so zu einer Managementaufgabe.

«IT-Sicherheit für KMU – So navigieren Sie Ihr Unternehmen sicher durch Cyber-Turbulenzen», Nicolas Mayencourt & Marc K. Peter, ISBN 978-3-03875-343-8, 1. Auflage 2021, 176 Seiten, CHF 48.–