

PUBLIREPORTAGE

Cyber-Security ist Chefsache

Es ist so eine Sache mit den Verantwortlichkeiten. Cyber-Security klingt erst mal nach IT-Thema und ist somit Sache der IT-Abteilung. Cyber-Security hat aber viel mit Risikomanagement zu tun. Die Risiken in einem Unternehmen zu kennen und einzuschätzen, ist aber definitiv Chefsache.

Die Ausgangslage in der Praxis

Die meisten Firmen setzen in immer grösserem Umfang auf IT-Systeme, um ihre geschäftlichen Abläufe zu optimieren. Der Begriff «Digitalisierung» ist in aller Munde. Wer da nicht mitmacht, droht den Anschluss zu verlieren. Die Digitalisierung ermöglicht es auch, vermehrt mobil zu arbeiten und nicht mehr zwingend im Büro zu sein, um Zugriff auf die Geschäftsunterlagen zu haben. Gerade in Zeiten von Corona hat das Arbeiten im Homeoffice stark an Bedeutung gewonnen.

Zusätzlich setzt sich der Trend zum Cloud Computing fort und immer mehr Lösungen werden (nur noch) in der Cloud angeboten. Die neuen Abmodelle ermöglichen es, IT-Lösungen ohne grosse Investitionen nutzen zu können, die laufenden Kosten sind gut kalkulierbar.

Was bedeutet Digitalisierung?

IT-Systeme werden schon lange eingesetzt, um Dokumente zu bearbeiten und um Informationen auszutauschen, sei es intern oder mit Geschäftspartnern. Auch die Kommunikation wird mehr und mehr digitalisiert. Nebst E-Mail werden heute Kommunikationslösungen eingesetzt, die es erlauben, Videokonferenzen vom Notebook oder Smartphone aus abzuhalten oder einfach in verteilten Teams zusammenzuarbeiten. Zusätzlich zur digitalen Datenhaltung bilden auch vollständig digitale Abläufe wichtige Elemente der Digitalisierung.

Mit der Digitalisierung kommen neue Systeme dazu, die die verschiedenen Insellösungen zusammenführen und auch Produktionssysteme in-



Die Verantwortung für einen sicheren Betrieb der IT und den Schutz der Daten liegt am Ende des Tages beim Management und ist somit Chefsache. Bild: pd

tegrieren. Das Ziel ist es, durchgängig digital zu arbeiten und die dafür notwendigen Daten und Informationen einfach austauschen zu können. Aktenschranke sollen irgendwann der Vergangenheit angehören. Als Folge werden diese IT-Systeme unentbehrlich. Fallen sie aus, hat dies fatale Folgen: Die Firma steht einfach still.

Wo liegen die Risiken?

Die fortschreitende Digitalisierung führt dazu, dass die IT-Umgebung einer Firma immer komplexer wird. Neue Bereiche werden mit neuen Systemen erschlossen und für das Arbeiten im Homeoffice braucht es Fernzugriff. Gewisse Systeme werden in der

eigenen IT betrieben, andere in der Cloud genutzt. Die IT-Landschaft wird heterogener und anspruchsvoller. Eigentlich bräuchte es mehr personelle Ressourcen, um die IT-Systeme sicher zu betreiben. Die Rekrutierung von Fachkräften ist jedoch schwierig. Somit steigt das Risiko, dass die IT-Systeme nicht auf dem aktuellen Sicherheitsstand sind und sich Angriffspunkte für Hacker auftun.

Auf der anderen Seite entwickelt sich die Cyber-Kriminalität immer weiter. Angriffe, die gestern viel Fachwissen und Ressourcen benötigten, können heute automatisiert werden. Dadurch ist kein tiefes technisches Wissen mehr erforderlich und die Anzahl der potenziellen Angreifer wächst stark. Die Digitalisierung findet auch

aufseiten der Cyber-Kriminellen statt. Es entstehen auch neue Geschäftsfelder, viele Hacker sehen sich als Dienstleister. Durch den Einsatz von Ransomware hat sich ein besonders lukratives Geschäftsmodell entwickelt. Die Cyber-Kriminellen «entführen» Daten und geben sie gegen Bezahlung eines Lösegeldes zurück. Das Risiko ist für die Angreifer klein, der Schaden für die betroffenen Firmen kann enorm werden.

Wieso ein Cyber Security Assessment?

In einem IT-Assessment mit Focus auf die Cyber-Security wird die IT-Landschaft des Unternehmens von einer externen Stelle einer Überprüfung unterzogen. Dabei werden verschiedene

Aspekte – von der Gesamtkonzeption bis zu einzelnen Sicherheitsmassnahmen – beleuchtet. Daraus ergibt sich dann eine Gesamtbeurteilung in Form eines auch für das Management verständlichen Berichtes. Falls offensichtliche Mängel erkannt werden, erhalten die Unternehmen auch Vorschläge zu deren Behebung. Um die Resistenz gegen Cyber-Angriffe einschätzen zu können, wird eine Beurteilung der aktuellen Bedrohungslage für die Branche, in der das Unternehmen tätig ist, erstellt. Eine daraus abgeleitete Risikoanalyse zeigt die konkret vorhandenen Risiken auf und bewertet sie. Mit diesen Resultaten ist dann das Management gefordert, in dem es sich über die Risikobereitschaft Gedanken macht: Welche der Risiken sind tragbar, welche müssen reduziert werden? Oft lassen sich die grössten Risiken mit vergleichsweise kleinem Aufwand auf ein tragbares Niveau reduzieren.

Ein IT-Assessment sollte nicht als Misstrauensbekundung gegenüber der IT-Abteilung verstanden werden. Vielmehr geht es darum, eine neutrale, externe Beurteilung zu erhalten, damit das Management und auch die IT-Mitarbeiter ruhig schlafen können. Die Gesamtverantwortung für einen sicheren Betrieb der IT und den Schutz der Daten liegt am Ende des Tages beim Management und ist somit Chefsache. (Anzeige)



Thomas Gusset
Spezialist für Netzwerksicherheit und Geschäftsführer der NetSec.co AG

Kontakt

Netsec.co AG
Im alten Riet 125, Schaan
Telefon: +423 388 27 77
Webseite: www.netsec.co

Verein für Mediation Liechtenstein

Streit mit den Nachbarn

Mediatorin Nina Schwarzkopf liebt an ihrer Arbeit, wenn für ihre Klienten Schritt für Schritt wieder Verständnis füreinander entsteht und plötzlich ein Aufeinander-Zugehen ermöglicht wird. Gerade bei Nachbarschaftsstreitigkeiten beweisen Menschen häufig einen langen Atem. Wenn die Nachbarn zudem noch verwandt oder angeheiratet sind, umso heftiger.

Bleibt es am Anfang vielleicht nur bei unfreundlichen Whatsapp-Nachrichten, sind es später vielleicht Pöbeleien über den Gartenzaun hinweg. Auslösende Faktoren für Konflikte können z. B. über den Zaun des Nachbarn wachsende Pflanzen, Laub abwerfende Bäume, Geruchsbelästigung durch Grillfeste, laute Musik am



Streit mit dem Nachbarn? Auf der Homepage des Vereins Mediation Liechtenstein findet sich eine Liste von Mediatoren mit verschiedenen beruflichen Schwerpunkten. Nina Schwarzkopf ist Gründungs- und Vorstandsmitglied im Verein Mediation Liechtenstein, www.verein-mediation-liechtenstein.li. Bild: iStock



Nina Schwarzkopf
Mediatorin, Verein für Mediation Liechtenstein

Abend oder falsch parkierte Autos sein. Bei allen Konflikten findet sich sehr häufig ein gemeinsames Grundmuster: Fast überall sind es Missverständnisse, persönliche Verletzungen, mangelnde Gesprächsbereitschaft oder einfach fehlende Akzeptanz. Bei scheinbar unlösbaren Konflikten ist oft

nur die Spitze des Eisbergs sichtbar. Die eigentlichen Bedürfnisse und Interessen der streitenden Parteien bleiben im Verborgenen. Halten die Streitigkeiten länger an oder entstehen sogar konkrete Schäden für die eine Seite, sehen die Kontrahenten sich vor Gericht wieder. Hier zählen die

formalen Gesichtspunkte. Es könnte, bedingt durch die teils unübersichtlichen, oft emotionalen Hintergründe, im Ermessen des einzelnen Richters liegen, ob den Parteien alternativ zu einem Zivilverfahren eine Mediation empfohlen wird. Mediation bietet eine freiwillige und selbstbestimmte Möglichkeit einer zeitnahen aussergerichtlichen Streitschlichtung. Sie unterstützt die streitenden Parteien, faire Lösungen zu entwickeln, mit denen die Betroffenen wieder besser miteinander oder nebeneinander leben können. Frühzeitig zu überlegen, ob ein Nachbarschaftsstreit nicht besser ohne Anwalt oder Gericht mittels einer Mediation beigelegt werden könnte, ist eine nerven- und kostensparende Alternative für alle Betroffenen.

Den Blick in die Zukunft und auf eine gute Lösung zu richten, bietet Freiheit und individuelle Win-win-Lösungen. (Anzeige)

Weitere Infos

www.verein-mediation-liechtenstein.li
office@verein-mediation-liechtenstein.li
Tel. +423 791 30 03 oder direkt vor Ort

HUBER

**HERZENSWÜNSCHE
ERFÜLLEN**

**POMELLATO
DAS ORIGINAL**

NUDO

**WIR FREUEN UNS
AUF IHREN BESUCH.**

Weisser Würfel

Städtle 34, FL-9490 Vaduz
T +423 237 14 14
www.huber.li