Adieu Burg

Die IT-Sicherheitsinfrastruktur der kleinen und mittelständischen Unternehmen (KMU) wird oft mit dicken Schutzmauern antiquierter Burgen verglichen. Denn genau wie Burgen waren KMUs früher lokal aufgestellt und konnten sich über diese Hürde vor Angreifern und Eindringlingen schützen. Aufgrund der geänderten Geschäftsanforderungen erfüllen dicke Mauern allein die Sicherheitsanforderungen nicht mehr.

Die alten Schutzmauern von Burgen hatten in der Vergangenheit nur einen Sinn, das eigene Territorium vor Angreifern zu schützen. Diese Analogie ist regelmässig bei Themen der IT-Security anzutreffen. Beim Unternehmen werden, wie bei einer Schutzmauer, Sicherheitszonen mit spezieller Hardware und Software aufgebaut, um so das eigene Netzwerk nach aussen hin abzuschotten. Doch in der heutigen Zeit reicht es nicht mehr aus, einfach nur eine dicke Mauer aufzubauen; es müssen andere Lösungen gefunden werden.

Paradigma Wechsel der Cyberattacken

In der aktuellen Fachpresse wird in letzter Zeit vermehrt von „Cyberspionage" oder „Cyberangriffen", vor allem gegen KMUs berichtet. Unter dem Begriff Cyberangriff versteht man das Eindringen in fremde Computersysteme zum Zweck der Informationsgewinnung. Dabei spielt es keine Rolle, ob es sich um Geheimdienste handelt oder um einen einzelnen Angreifer, der sich einen wirtschaftlichen Vorteil verschaffen will.

Grossangelegte Angriffe, die wir aus der Vergangenheit mittels Viren und Malware kennen, hatten nur einen Zweck: Einen möglichst grossen Personenkreis zu treffen und dadurch einen grossen betriebswirtschaftlichen Schaden erzielen. Die aktuellen Cyberangriffe hingegen werden sehr individuell und konkret durchgeführt. Warum ist das so?

Das Ziel dieser Angriffe hat sich komplett verändert. Früher hatten die Angreifer das Ziel öffentliche Aufmerksamkeit zu erhalten, um auf diese Weise „Ruhm" zu erlangen. Je höher der betriebswirtschaftliche Schaden oder je wirksamer die Medienpräsenz war, desto erfolgreicher war ihr Unterfangen. Heute geht es um den Zugriff auf Informationen, welche sich weiterverkaufen lassen. Informationen wie zum Beispiel Rezepturen, Baupläne, technische Zeichnungen, Finanzzahlen eines Unternehmens, etc.

Gibt es eine Lösung für dieses Problem? Ja, es gibt einen vernünftigen und sinnvollen Lösungsansatz, um diesem Problem entgegenzuwirken.

Das Gesetz als Basis des Handelns

Die erste Frage, die es in diesem Zusammenhang zu beantworten gilt, lautet: Gibt es rechtliche Vorgaben über die zu schützenden Daten durch den Gesetzgeber?

Mit dem Datenschutzgesetz (DSG), dem Obligationenrecht (OR), dem Fernmeldegesetz (FMG) oder der Geschäftsbücherverordnung existieren eine ganze Reihe an rechtlich verbindlichen Vorgaben zum Thema Umgang und Schutz von Informationen. Es werden hier ganz klare Aussagen zum Schutz von Daten, dem Nachweis der Nichtveränderbarkeit, der Vertraulichkeit oder dem Postgeheimnis gemacht, die für alle Unternehmen verbindlich sind. Die rechtlichen Vorschriften nehmen die Verantwortlichen unmissverständlich in die Pflicht. Konkrete Massnahmen fehlen jedoch im Gesetzestext und müssen durch jedes Unternehmen selbst erarbeitet werden.

Wer ist innerhalb eines Unternehmens für die Daten und den Schutz derer verantwortlich?

In Bezug auf die Verantwortlichkeit ist festzuhalten, dass diese im OR ganz klar geregelt ist. Niemand anders als die Geschäftsführung ist für die Daten und dem daraus resultierenden Datenschutz verantwortlich. Diese Aufgabe kann zwar an eine Fachstelle delegiert werden, jedoch bleibt die Geschäftsleitung für die ordnungsgemässe Datenhaltung und den Datenschutz zuständig. Zur Geschäftsleitung gehören laut eines Urteils des Bundesgerichts alle Personen, die eine materiell leitende Position besetzen und auf das Funktionieren des Unternehmens einen massgeblichen Einfluss haben. Damit ist der Personenkreis grundsätzlich sehr weit gefasst und schliesst unter anderem den CIO mit ein.

Die gesetzlichen Anforderungen sind das eine. Diese müssen jedoch innerhalb der Informatik umgesetzt werden können.

Veränderte Anforderungen an die IT

Die Geschäftsanforderungen der KMUs verändern sich. Früher hatten Unternehmen einen Standort, an dem, von der Verwaltung bis hin zur Produktion, alles vorhanden war. In der heutigen Zeit haben mittelständische Unternehmen oftmals mehrere Standorte, produzieren in verschiedenen Ländern und nutzen unterschiedlichste Infrastrukturen.

Mit diesen Geschäftsanforderungen verändern sich auch die Anforderungen an die Informatik. Sie muss die Geschäftsprozesse verstehen, sie mit IT-Mitteln unterstützen, den Betrieb sicherstellen, ihre Kosten im Griff behalten UND dabei den neuen Anforderungen Rechnung tragen. Wie sonst ist zu erklären, warum sich zum Beispiel das Thema „Bring your own device“ seit geraumer Zeit immer in den Medien auftaucht. Der Wunsch, Daten immer und überall zu bearbeiten, ist omnipräsent. Auch andere Themen wie Cloud-Computing oder Unified Communication stellen die Informatik, und vor allem die Informationssicherheit, vor schier unlösbare Aufgaben. Aus den Unternehmen werden aktuell immer wieder die gleichen Forderungen laut:

- flexibles Arbeiten egal wann und wo
- Interne Daten sollen auf beliebigen Endgeräten, auch ausserhalb des Geschäftsnetzwerkes, verfügbar sein
- Anbindung unterschiedlicher Partner an das interne Netzwerk oder
- der Austausch von Daten mit Lieferanten, Kunden oder Dienstleistern

Wie schafft die Informatik den Spagat zwischen den an sie gestellten Anforderungen bezüglich Leistungsfähigkeit, Flexibilität und gleichzeitig die Erfüllung der Informationssicherheits-Richtlinien bzw. den gesetzlichen Anforderungen?

Dies ist ein schwieriger Weg, der bereits in den Köpfen der Geschäftsleitung beginnen sollte. Jedoch fehlt dieser oftmals das Bewusstsein und das Verständnis für die Informatik.

Um den Handlungsbedarf einmal ganz klar aufzuzeigen reicht es, zunächst mit folgender Fragestellung an die Informatik heranzutreten: „Wer hat alles Zugriff auf die wichtigsten Unternehmensdaten?“ In der Regel ist die Antwort so erschreckend wie ausreichend, um das benötigte Verständnis zu wecken. Hier wird meistens festgestellt, dass zu den vom Dateneigner berechtigten Personen noch unzählige andere Personen auf unternehmenskritische Daten Zugriff haben.

Diese Problemstellung kann weiter vertieft werden, indem sich die Unternehmen die Frage nach den Auswirkungen bei Verlust oder Diebstahl ihrer unternehmenskriti-

schen Daten stellen. Hier kommt die Prüfung sehr schnell zum Ergebnis, dass der Verlust wichtiger und geschäftskritischer Informationen ein hohes Risiko mit sehr grossem Schadenspotenzial darstellt.

Hier treffen wir auf „des Pudels Kern": Die Angst, Daten gänzlich oder an Mitbewerber zu verlieren und dadurch nicht mehr wettbewerbsfähig zu sein, ist gross. Daher werden zum Teil technisch aufwendige Infrastrukturen aufgebaut, welche die gesamte Informatik wie eine antiquierte Wehrmauer schützen sollen. Dies erzeugt oftmals nur eines – eine Scheinsicherheit!

Denn: Was passiert in der Realität bei den KMUs? Es werden Daten aus dem internen Netzwerk auf ungeschützte mobile Endgeräte gespeichert, Informationen in der Cloud, wie z. B. DropBox, SkyDrive etc. ungenügend geschützt abgelegt und eine unbestimmte Anzahl an Personen wie Mitarbeiter, Informatiker oder externe IT-Dienstleister dürfen und können auf wichtige Unternehmensdaten zugreifen. Die Devise lautet in der Regel: Bequemlichkeit und Funktionalität vor Sicherheit!

Was kann das Unternehmen konkret dagegen tun?

Die Schutzbedarfsanalyse

Eine geeignete und praktikable Möglichkeit, diese Fragestellung in den Griff zu bekommen ist, die Durchführung einer Schutzbedarfsanalyse.

Hier werden in einer ersten Phase die für das Unternehmen relevanten Business Prozesse herausgearbeitet. Anschliessend wird pro Prozess definiert, wie wichtig und widerstandsfähig dieser innerhalb des Unternehmens sein muss, um einen stabilen Betrieb zu gewährleisten. Die Informationen diesbezüglich kommen nicht von der Informatikabteilung sondern von den Prozessverantwortlichen, die beurteilen können, wie sich Schadenszenarien konkret auf die Prozesse auswirken.

In einer Schutzbedarfsanalyse werden die Fragen nach Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Arbeitsprozessen oder Daten beantwortet. Zudem können die Prozesse nach ihrer Kritikalität priorisiert werden. Diese Informationen sind die Basis für sinnvolle und praktikable Sicherheitskonzepte. Mit diesen Konzepten ist es dann wiederum möglich, die kritischen Prozesse entsprechend der Schutzbedarfsanalyse, mit allen technischen und organisatorischen Möglichkeiten, zu schützen.

Zusätzlich werden alle vorhandenen Daten und kritischen Applikationen identifiziert und anschliessend klassifiziert. So können die unternehmenskritischen Informationen von unwichtigen unterschieden werden.

Diese unternehmenskritischen Daten gilt es, mit allen technischen und organisatorischen Möglichkeiten vor unbefugtem Zugriff zu schützen. Dies kann in letzter Konsequenz auch dazu führen, dass diese Daten das interne Netzwerk nicht verlassen dürfen. Diese dürfen dann weder in einer E-Mail auf mobile Endgeräte repliziert, auf USB-Sticks oder CDs kopiert oder ausgedruckt werden.

Fazit

KMU müssen noch mehr zum Schutz der eigenen Informationen tun. Die Bedrohung durch direkte und unvermittelte Angriffe auf die Netze der Unternehmen durch hochprofessionelle Cyberkriminalität ist real. Die Zeiten, in der man sich von dicken Burgmauern schützen lassen kann, sind vorbei. Deshalb muss die Informationssicherheit einen anderen Stellenwert erhalten und mit Nachdruck angegangen werden. Denn: Hier ist noch ein erheblicher Nachholbedarf festzustellen.

Im Bereich der Informationssicherheit ist auch für die KMU angebracht, externe Unterstützung beizuziehen. Gerade bei den Themen Durchführung einer Schutzbedarfsanalyse oder der Beurteilung IT-rechtlicher Fragen sind die Spezialisten gefragt.

Jetzt gilt es mehr denn je Konzepte zu erarbeiten, um das eigene Know-how vor dem Verlust durch Industriespionage in Form von Cyberangriffen zu schützen. Der Verlust eigener Informationen an einen Mitbewerber, welcher sich dadurch einen „unlauteren" Wettbewerbsvorteil verschaffen kann, stellt ein erhebliches Risiko für das gesamte Unternehmen dar.

Kontakt

Markus Mangiapane

Master in Business
Information Management
Auditor-
Informationssicherheit

BSG UNTERNEHMENSBERATUNG AG
Teufener Strasse 11
CH-9000 St. Gallen

Tel. +41 (0)71 243 57 57
Fax +41 (0)71 243 57 43

Markus.Mangiapane@bsg.ch
www.bsg.ch