Ein Sicherheitsoffizier für KMU

Ein **Chief Information Security Officer** (CISO) übernimmt Verantwortung für die Informationssicherheit und hat eine ganzheitliche Sicht.

MICHAEL KAUFMANN

SHUTTERSTOCK

Ein Anruf auf dem Smartphone: Die glaubwürdig wirkende Nachfrage nach Kontaktdaten oder ein Anruf der «IT-Abteilung».

Der Schutz vor Cyberangriffen ist komplex, dies beinhaltet selbstverständlich nicht nur die technische Abwehr von Angriffen, sondern fängt viel früher an, und zwar bei der Etablierung einer passenden Security Governance für das Unternehmen. Doch was ist nun explizit zu tun, um eine ganzheitliche Informationssicherheit zu etablieren?

Das Gute ist, dass es verschiedene IT-Security-Frameworks gibt, die herangezogen und adaptiert auf das Unternehmen strategisch implementiert werden können. Das Schlechte ist, dass diese meist sehr umfangreich ausfallen und daher die detaillierte Umsetzung in einem kleineren KMU nicht immer sinnvoll ist. Das richtige Umsetzen ist also eine Gratwanderung, die ein ausgebildeter Chief Information Security Officer (CISO) erfolgreich leiten kann.

Was gilt es zu schützen?

Als erster Schritt gilt es zuerst, sich einen Überblick zu verschaffen über den aktuellen Stand der Informationssicherheit im Unternehmen. Dieses Assessment wird aufzeigen, wie gut das Unternehmen bereits aufgestellt ist und was noch fehlt beziehungsweise verbessert werden muss. Als zweiter Schritt wird der CISO nun eine High-Level-Security-Strategie erarbeiten müssen, die dann für alles Weitere die übergeordneten Rahmenbedingungen vorgibt (siehe Seite 41).

Sicherheit von Anfang an

Um zu wissen, was zu schützen ist, muss unbedingt ein IT-Risikomanagement etabliert werden. Es gilt herauszufinden, wie viel Schutz notwendig ist, um sich bestmöglich gegen die Risiken zu schützen. Es ist wie bei allem im Leben: Ein Schutz gegen alles ist nicht möglich, nicht gewollt und auch nicht bezahlbar. Um zu wissen, was sich zu schützen lohnt, ist schon mal eine erste Dateninventur notwendig mit einer Klassifizierung der Daten in beispielsweise vier Stufen: geheim, vertraulich, intern, öffentlich. Damit leitet es sich später ab, welche dieser Daten speziell schützenswert sind.

Für Projekte, die IT beinhalten, ist es sinnvoll, einfach anwendbare Vorgabedokumente bereitzustellen, um in jedem Projekt gleich zu Beginn eine kleine Schutzbedarfsanalyse durchführen zu können, ein Sicherheitskonzept aufzustellen und die Folgen für den Datenschutz zu klären. Mit diesem Schritt wird Sicherheit gleich zu Beginn im Projekt behandelt und nicht erst nachdem beispielsweise eine Software für die Public Cloud gebaut wurde, um sie dann später wegen Datenschutzanforderungen mühsam umzubauen, damit die in einer geschützten On-prem-Umgebung betrieben werden kann.

Sicherheitsvorgaben als Grundlage

Es ist bekannt, dass die Benutzerinnen und Benutzer oft das schwächste Glied im Sicherheitsdispositiv sind. Dessen will man mit gut verständlichen Richtlinien für Benutzer (Policies) vorbeugen. So etwa mit einem Nutzungsreglement, das definiert, was Mitarbeitende mit der Unternehmens-IT-Infrastruktur und insbesondere mit den zur Verfügung gestellten Notebooks, Mobiles und so weiter geschäftlich und auch privat machen dürfen. Ähnliche Vorgaben braucht es aber auch für den IT-Betrieb und für technische Mindeststandards.

Dies alles hilft aber nichts, wenn dann trotzdem ein Notfall eintrifft und schnell gehandelt werden muss. Um dies im Griff zu haben, empfiehlt es sich, die Konzeption und Umsetzung von Business Continuity Management, sprich Notfallmanagement und Disaster-Recovery-Planung sowie die Durchführung von regelmässigen Übungen vorzubereiten.

Sind all diese Massnahmen erst einmal umgesetzt, müssen sie auch im täglichen Business getestet werden. Dazu gehört auch die Sensibilisierung der Mitarbeitenden, zum Beispiel mittels Benutzerschulungen wie User Awareness Trainings.

Unangemeldeter Test

Das kann auch einmal mit gefakten, kontrollierten Phishing-Mails geschehen. So könnte eine gefälschte Information an die Belegschaft vom angeblichen CEO verschickt werden, um zu sehen, wie viele Mitarbeitende auf den «gefährlichen» Link klicken, und um sie umgehend auf ihr Versehen aufmerksam zu machen. Ebenso sollten ab und zu auch externe und interne Sicherheitsscans durchgeführt werden, um zu erkennen, ob ein IT-System Schwachstellen hat, und um sie dann zu beheben.

Die Cyberrisk-Versicherung

Selbstverständlich gibt es immer Restrisiken, die akzeptiert werden müssen, oder aber teilweise auch mit Cyberrisk-Versicherungen abgedeckt werden können. Wobei die Versicherungen, die solche Policen anbieten, darauf bestehen werden, dass ein guter Grundschutz wie oben skizziert vorhanden sein muss, da sonst möglicherweise keine Versicherung abgeschlossen werden kann.

Erste Anlaufstelle

Wer eine Do-it-yourself-Anleitung sucht, um einen Mindeststandard in einem kleinen KMU zu implementieren, findet einen Best-Practice-Leitfaden auf der unabhängigen Plattform kmuschutz.ch.

Michael Kaufmann, CEO, Atrete IT Consultants, Zürich.
kmuschutz.ch

ANZEIGE