Kennen Sie die anderen Welten in Ihrem Unternehmen?

Im Wandel der Zeit

Die Veränderungen der Bedrohungsszenarien

von Georg Lutz

Das Thema IT Sicherheit hat in den letzten Jahren immer wieder neue Dimensionen erreicht. Dazu brauchen wir immer neue Sicherheitskonzepte. Vielleicht sollten wir aber auch aus diesem sich immer schneller drehenden Hamsterrad aussteigen und nach neuen Ansätzen suchen. Dabei hilft ein Blick in die Forschungslabors.

Neben der Dotcom- und der Immobilienblase, Harry Potter und dem iPhone haben die Nullerjahre des 21. Jahrhunderts vor allem eines gebracht: Eine rasant zunehmende globale Verflechtung der Datennetze und Informationen und damit einhergehend eine zunehmende Bedrohung von Daten. Hand in Hand mit dem technologischen Fortschritt geht die Weiterentwicklung von geeigneten Angriffen, um an fremde, aber interessante Daten zu gelangen. Alte Verfahren werden stetig weiterentwickelt und automatisiert und auch laufend der neuesten Technik angepasst.

Es lohnt sich darum für die KMU, der IT-Security die gebührende Sorgfalt zukommen zu lassen. Sicherheitslücken können schnell in ein teures Fiasko münden oder gar rechtliche Schritte nach sich ziehen. Aufgrund des Drucks durch das Daily Business vernachlässigen heute noch viele KMU das IT-Compliance-Management und dort insbesondere die Informationssicherheit. Diese Hürde kann jedoch umgangen werden, indem die damit zusammenhängenden Aufgaben an entsprechende Fachkräfte aus- respektive eingelagert werden.

Angreifer schärfen ihre Waffen

Gerade von menschlicher Seite droht heute die grösste Gefahr. Angreifer rüsten laufend auf und nützen jedes Loch, jede bekannte Schwachstelle aus, welche bei einer Webapplikation unbeachtet und ungepatched bleibt. Seit Mitte letzten Jahres zieht zudem das Phänomen weite Kreise, dass Angreifer scheinbar vertrauenswürdige Beziehungen via Soziale Netzwerke ausnutzen, indem sie bösartige Links vom Absender eines Freundes aus verschicken. Geradezu perfid sind die Waterhole-Angriffe, in Analogie zum Tierreich: Die Eindringlinge fokussieren auf ein zentrales Ziel wie beispielsweise eine Special Interest-Website, welche von vielen Menschen frequentiert wird und nicht unbedingt über einen als genügend zu bezeichnenden Schutz verfügen. Computer werden befallen, wenn Mitarbeiter eine infizierte Website (Drive-by-Infektion) besuchen. Die Opfer kommen selbst aus verschiedenen Richtungen zu den Angreifern.

Informationssicherheit als strategische Erfolgsposition

Absicht oder Nachlässigkeit, Systemfehler oder menschliches «Versagen» welcher Natur auch immer: Die Wahrung der Informationssicherheit liegt nicht nur im Ermessen einer Unternehmung oder Behörde, sondern bildet einen relevanten strategischen Erfolgsfaktor. Vertraulichkeit, Integrität und Verfügbarkeit von Informationen also sind nicht nur «nice to have». Sie sind Bestandteil des Pflichtenheftes der obersten Unternehmensführung. So liegt gemäss Sarbanes Oxley Act und Basel III das

Der Chief Information Security Officer CISO ist die Vermitlungsebene zwischen den IT- und Businesswelten.

Handling der operationellen Risiken und die sicherheitsmässige Überprüfung eines Unternehmens implizit im Verantwortungsbereich des Verwaltungsrates. Der Schutz der Kundendaten ist sogar explizit geregelt. Immer mehr Unternehmen wollen sich deshalb auch keine sicherheitsmässige Blösse geben und organisieren ihr Informationssicherheits-Managementsystem nach dem ISO-Standard 27001:2013, welcher weltweit seine Gültigkeit hat. Dieses beinhaltet nicht nur die Zertifizierung von Geschäftsprozessen, sondern auch die Massnahmen zur Sicherstellung der Informationssicherheit.

Sicherheitsmässige Schlüsselposition

Zu diesem Zweck beschäftigen viele Unternehmen einen Chief Information Security Officer. Zu deren Aufgaben zählen namentlich, den Bereich «Informationssicherheit» des Unternehmens zu führen und basierend auf Risikoanalysen für das Unternehmen geeignete Sicherheitsstrategien zu erarbeiten. Zudem sollen sie unternehmensintern eine breit abgestützte Aufmerksamkeit für das Thema schaffen und eine entsprechende Kultur implementieren. CISO werden an vorderster Front eingesetzt, wenn es um die Erarbeitung und Definition der sicherheitsrelevanten Objekte geht und die Definition der Bedrohungen und den daraus abgeleiteten Sicherheitszielen. Weiter zählen zu ihren Aufgaben die Ausarbeitung von Sicherheitsvorschriften und deren Auditierung. Kurz, sie sind die oberste moralische Instanz in Sachen Risikoanalyse im Informationssicherheitsbereich und Umsetzung entsprechender griffiger Massnahmen.

Eingekauftes Know-how

Für KMU lohnt sich die Besetzung eines CISO in langjähriger Vollbeschäftigung nicht immer. Hier setzt das Angebot des Zuger Informationssicherheitsspezialisten InfoGuard AG ein. Wir übernehmen für ein Unternehmen die Aufgabe des Information Security Officers im Rahmen eines Outsourcing-Verhältnisses. Dabei profitieren die Unternehmen von der Erfahrung und dem umfassenden Know-how unserer Sicherheitsexperten auf den Ebenen Organisation/Prozesse, Compliance, Audit und Technik. Und das einkaufende Unternehmen gewinnt gleich doppelt – nicht nur vom CISO selbst, sondern vom ganzen dahinter stehenden und steckenden InfoGuard Know-how-Team: Buy one – get a whole team.

Der Chief Information Security Officer CISO agiert als Bindeglied zwischen der IT-Abteilung und dem Management und hilft diesem, die rechtlichen und regulatorischen Anforderungen in punkto Informationssicherheit einzuhalten. In der Regel rapportiert er direkt an den CEO. Beim Insourcing von Informationssicherheits-Spezialisten sind verschiedene Kooperationsformen denkbar: Entweder wird der unternehmenseigene CISO im Rahmen eines Langzeitmandats durch eine externe Fachperson im Teilzeitpensum unterstützt oder ein KMU nimmt einen externen Informationssicherheitsexperte hinzu, um den Aufbau der Sicherheitskultur voranzutreiben und ein entsprechendes Bewusstsein unter den Mitarbeitern zu implementieren. Der CISO agiert dann wie ein unternehmenseigener Mitarbeiter und ist Teil des dortigen Systems. Nur so kann er allfällige Schwachstellen in der Organisation gleich aufdecken, Zugriffsberechtigungen überprüfen und das Verhalten der Mitarbeiter einer kritischen Betrachtung unterziehen: Denn jedes Unternehmen ist sicherheitsmässig nur so gut, wie sein schwächstes Glied in der Kette – der Mensch. ■

Die wichtigsten Aufgaben des Chief Information Security Officers

- Risikoanalysen
- Beratungsdienstleistungen punkto Informationssicherheit
- Die Definition von Sicherheitsstrategien und -policies, die Schaffung entsprechender Vorschriften und die die Überprüfung deren Einhaltung
- Erarbeitung und Durchführung von Awareness-Kampagnen sowie entsprechendes Training der Mitarbeiter
- Portfolio Management der Security Prozesse
- Auditierung der Funktionseinheiten zum Stand der Umsetzung und der Weiterentwicklung der Sicherheitsvorschriften.

Franco Cerminara

ist Head of Consulting bei der InfoGurad AG.

www.infoguard.ch