Falsche Wahl

Nicht den Rotstift bei der Sicherheit ansetzen

von Umberto Annino

Herbstzeit ist Budgetzeit. In den Unternehmen werden die Stifte gespitzt und Meetings anberaumt, um die finanziellen Posten und Aufwendungen im kommenden Jahr für die einzelnen Bereiche zu definieren. Es soll in die Mitarbeiter, die Infrastruktur, den Ausbau der Marktstellung, die IT investiert werden. Allenfalls noch ins Marketing und publikumsträchtige Events. Auf der Strecke, bewusst oder unbewusst, bleibt häufig – die Sicherheit. Nicht so effekthaschend wie ein Neubau, nicht so sexy wie ein Anlass mit Starbesetzung. Aber relevant dafür, dass allenfalls beides noch umgesetzt werden kann oder eben nicht mehr.

Bemüssigt man die herzbergsche Motivationstheorie, so würde man bei Sicherheitsthemen wie Informationssicherheit und Cyber Security von Hygienefaktoren sprechen – sie sind notwendig, man nimmt sie aber als gegeben und nicht als sonderlich aufregend hin. Fehlen sie, nimmt man das jedoch als Mangel wahr. Muss im Unternehmen auf die Sparbremse getreten werden, gibt es immer noch gerne Abstriche bei der Sicherheit. Da diese nicht sichtbar im Hintergrund läuft und damit – vermeintlich – keine Lorbeeren zu ernten sind.

Im Hinter- und Untergrund, buchstäblich im Dunkeln lauern jedoch auch die wirklichen Gefahren für Unternehmen. Dennoch fühlen sich kleinere und mittlere Unternehmen (KMU) laut Umfragen von Hackerangriffen, Viren, Schadsoftware und Datenklau kaum übermässig bedroht. Doch sie wiegen sich zu Unrecht in Sicherheit: Gerade weil viele KMU die Risiken mangelnder ICT-Sicherheit unterschätzen und dadurch unzureichend geschützt sind, bilden sie ein attraktives Ziel für Cyberkriminelle.

Wenn die ICT-Systeme eines Unternehmens Lücken aufweisen, kann das nicht nur beim Unternehmen selbst, sondern auch bei den Kunden Schäden verursachen: Daten können durch Manipulation unbrauchbar gemacht oder gar gelöscht werden, Online-Bestellungen verloren gehen, eine Schadsoftware die Systeme anderer kompromittieren. Im schlimmsten Fall droht ein direkter Ertragsausfall mit weitreichenden Konsequenzen.

Datenklau hebelt Unternehmen aus

Insgesamt sind die KMU unzähligen Cyber-Gefahren ausgesetzt. Denn die Möglichkeiten des Internets für die Angreifer sind enorm. Gezielte Spionage-Angriffe oder Advanced Persistent Threats nehmen stündlich zu und führen zu Schäden in Millionenhöhe. Das kann ein Unternehmen durchaus in die Knie zwingen. Die Angreifer passen sich sehr schnell neuen Technologien an. So existieren beispielsweise Trojaner, die mobile Anwendungen wie E-Banking-Apps von Handys angreifen und entsprechend manipulieren. SMS zur Transaktionssignierung lassen sich abfangen und missbräuchlich verwenden. Auch Angriffe und Attacken auf einzelne Unternehmen haben zugenommen: DDoS-Attacken, Spear Phishing, Schadsoftware, Ransomware und E-Mail-Links mit Trojanern sowie gezielte Social-Engineering-Angriffe sind zahlreicher und intensiver geworden. Zudem wird eine starke Zunahme von E-Mails mit einem Link auf eine infizierte Website sowie von Internettelefonie-Missbräuchen beobachtet. Raffiniert getarnte Angriffe nehmen auch über Soziale Medien rasant zu.

Das Unternehmen kommt in Verruf

Was viele Unternehmer nicht wissen: Sie können rechtlich belangt werden, wenn beispielsweise schützenswerte Personendaten von Cyberkriminellen ausspioniert werden. Das gilt als Verstoss gegen das Datenschutzgesetz. Jedes fünfte Unternehmen war schon mindestens einmal Ziel einer Cyber-Attacke. Allerdings kann mehr als die Hälfte der Betroffenen nicht genau angeben, welche Bereiche beziehungsweise Daten angegriffen wurden und welche Folgen dies hatte. Es ist davon auszugehen, dass etliche Attacken von den Unternehmen gar nicht bemerkt werden, weil erforderliche Monitoring- und Kontrollverfahren fehlen. So kann es auch vorkommen, das USPs, Entwicklungs- oder Forschungsdaten, Lizenzen eines Unternehmens einem anderen angeboten werden. Ein Imageverlust sondergleichen. Das zweite Unternehmen macht sich natürlich strafbar, wenn es solche Informationen annehmen würde.

Geradestehen muss der Chef

Cyber Security wird oft als Verantwortung einer Fachabteilung von Informationssicherheits- oder ICT-Experten gesehen. Diese Denkweise kann ein falsches Gefühl von Sicherheit vermitteln. Die eigentliche Herausforderung ist, dass Cyber Security ein Teil der organisationsweiten Vorgaben und Richtlinien wird. Dies bedeutet aber auch, dass Cyber Security als eine zentrale Funktion in der ICT-Strategie und beim Einsatz von ICT-Systemen erhält und nicht wie häufig der Fall, erst am Ende solcher Projekte um ihre Zustimmung angefragt wird. Das Thema Cyber Security muss auf jeder Management-Agenda stehen. Alle Stakeholder, der Verwaltungsrat, die Aktionäre und die Kunden erwarten, dass das Unternehmen dieser Herausforderung genügend Aufmerksamkeit schenkt. Die Unternehmensleitung muss also in der Lage sein, bei der Umsetzung von Cyber Security die richtigen Entscheidungen zu treffen und so die Stakeholder zufriedenzustellen. Ist ein Hackerangriff auf ein KMU erfolgreich, geraten also nicht nur die IT-Verantwortlichen in Erklärungsnot.

Rezepte zur Steigerung der Cyber-Sicherheit

Gelegenheit schafft Diebe gilt auch beim Datenklau bei KMU. Aber resignieren Sie nicht. Zu Ihrem Schutz empfehlen wir Ihnen folgende Massnahmen:

- Aufbau und Definition eines Informationssicherheits-Management-Systems nach ISO 27001 auf der Basis einer entsprechenden Risikobewertung. Informationssicherheit ist nicht nur ICT-Sicherheit. Auch die Menschen und die Prozesse müssen miteinbezogen werden.
- Sensibilisierung: Regelmässige Weiterbildung der Mitarbeiter in Informationssicherheitsfragen und Aufklärung über die neusten Trends im Bereich Cyber Threats, Phishing, Social Engineering und Social-Media-Attacken.
- Limitierung und Kontrolle der Zugriffsrechte: Jeder sollte nur auf die Daten Zugriff haben, die wirklich für seine Funktion notwendig sind. Es geht um eine konsequente Limitierung, Verwaltung und Kontrolle der Zugriffsrechte inklusive zurückhaltender Vergabe von «Privileged Access Rights».
- Implementation von geeigneten technischen Cyber-Security-Massnahmen: ICT-Systeme und Unternehmensdaten müssen technisch ausreichend gesichert sein wie beispielsweise Firewalls, Web- und E-Mail-Sicherheit, Malware-Schutz oder Verschlüsselungssysteme. Stellen Sie aber auch sicher, dass die ICT-Systeme, Software und Applikationen laufend aktualisiert und dass von den Unternehmensdaten täglich Backups erstellt werden.
- Penetration Testing: Mithilfe von Ethical Hackern werden Sicherheitslücken und Schlupflöcher in den ICT-Systemen eines Unternehmens aufgedeckt, bevor ein Hacker es tut.
- Cyber Threat Intelligence: Das Zauberwort der Stunde mit dem durchschlagenden Effekt meint, dass nicht rein reaktiv auf Sicherheitsvorfälle reagiert, sondern präventiv mittels «Intelligence-Methoden» mögliche Angriffe sogar antizipiert und von Vornherein im Keim erstickt werden.
- SIEM und Monitoring: Mithilfe eines Security Information and Event Management (SIEM) werden proaktiv Schwachstellen und Angriffe auf die ICT-Infrastruktur erkannt, sodass diese gezielt und schnell eliminiert werden können. Gleichzeitig wird eine vollständige Transparenz über den Sicherheitszustand im Netzwerk geschaffen und dadurch das Sicherheitsniveau nachhaltig erhöht.
- Und last but not least lassen sich alle Cyber-Sicherheit-fördernden Massnahmen zu weitaus geringeren Kosten an einen Sicherheitsdienstleister auslagern als für den Preis eines internen Chief Information Security Officer (CISO). ■

Die unterschiedlichen Bedrohungsszenarien gilt es im Blick zu haben. DDoS-Attacken, Spear Phishing, Schadsoftware, Ransomware und E-Mail-Links mit Trojanern sowie gezielte Social-Engineering-Angriffe heissten die zentralen Stichworte.

Über InfoGuard

InfoGuard AG ist spezialisiert auf umfassende Informationssicherheits- und innovative Netzwerklösungen. Zu ihren Kompetenzen zählen massgeschneiderte Dienstleistungen nach internationalen Sicherheitsstandards sowie die Entwicklung und Implementierung technischer Sicherheits- und Netzwerklösungen. InfoGuard ist Mitglied der Schweizer «The Crypto Group». InfoGuard ist ISO/IEC-27001:2013-zertifiziert.

ISO/IEC-27001-zertifiziert

Zum Schutz von Unternehmensplattformen, Websites und ICT-Infrastrukturen stellt unser Haus Cloud- oder Managed Security Services zur Verfügung wie beispielsweise ein umfassendes Security Information & Event Management, Cyber-Threat-Analysen, Web Application Firewalls oder gar ein Outsourcing als CISO-as-a-Service. Dadurch stehen dem Kunden die Schweizer Sicherheitsexperten rund um die Uhr aus dem InfoGuard Cyber Defence Center mit ihrer langjährigen Erfahrung und ihrem fundierten Know-how zur Verfügung.

Umberto Annino

ist Senior Security Consultant der InfoGuard AG.

www.infoguard.ch