„Einen 100%igen Schutz vor Cyberangriffen wird man auch bei Berücksichtigung aller Sicherheitsaspekte nicht erreichen, aber vorbereitet zu sein und im Falle schnell und gezielt handeln zu können, kann die Folgekosten für Datenrettung, Betriebsunterbrechung und Schadenersatzansprüche reduzieren und ein Bußgeld verhindern."

Christoph Hofmann
Datenschutzbeauftragter der WK Tirol

Die Mitarbeiter sind auch für die Sicherheit des Unternehmens verantwortlich, besonders in der digitalen Welt. Daher sollten sie in diese Richtung sensibilisiert werden.

Weise die breite Bevölkerung vor gröberen finanziellen Schäden zu schützen.

Wie in der Natur gilt auch beim Thema Sicherheit – Der Aktive ist dem Passiven überlegen! Daher sollte das Thema Datensicherheit immer aktiv betrachtet werden.

Das Thema Sicherheit steht in einem engen Zusammenhang mit dem Begriff „Routine" – die Routine ist ein zweischneidiges Schwert – Je mehr Informationen der Angreifer über die Routine hat, desto leichter kann er den Schutzwall der technischen und organisatorischen Maßnahmen durchbrechen. Andererseits bietet die Routine die Gewähr, erprobten und als sicher bewerteten Verfahren zu folgen.

Das Thema Sicherheit betrifft nicht nur den Unternehmer! Wichtig ist eine Sensibilisierung der Mitarbeiter, dass auch sie für die Sicherheit des Unternehmens verantwortlich sind! Zu berücksichtigen ist nämlich: Die Schwachstelle bei Cyberangriffen ist im Regelfall der Mensch!

Bei der Entwicklung der Schutzstrategien sollte immer vom „Worst-Case-Szenario" ausgegangen werden. Wenn die entwickelte Sicherheitsstrategie sich auf den größtmöglichen Schaden ausrichtet und konzentriert, sind kleinere Angriffe von der Strategie ebenfalls abgedeckt.

Ein wichtiger Aspekt ist weiters, dass man denkt wie ein Angreifer – simulierte Angriffe zeigen dem Unternehmen die Schwachstellen in der Strategie auf und lenken den Fokus auf wichtige Vorbereitungspunkte für den Ernstfall!

Schützen Sie Ihre Daten und betrachten Sie digitale Entwicklungen immer auch mit einem kritischen Auge!

Die digitale Welt ist eine Errungenschaft unserer Zivilisation, aber auch eine Gefahr für unsere persönliche Integrität.

Der Mitarbeiter als Angriffsziel von Datendiebstahl

Die besten technischen Sicherheitsvorkehrungen nützen nichts, wenn Ihre Mitarbeiterinnen und Mitarbeiter diese nicht unterstützen und auch leben. Jeder im Unternehmen muss wissen, wie mit personenbezogenen Daten umzugehen ist, wie mit unerwünschten Mails vorzugehen ist oder was Passwortsicherheit bedeutet.

Social Engineering klingt eigentlich ganz sympathisch, ist es aber nicht. Durch Vortäuschung falscher Tatsachen wird ein Kontakt mit dem potenziellen Opfer aufgebaut, um so an sensible Daten wie z.B. Passwörter heranzukommen. Man nennt es auch Human Hacking.

Angriffsziel des Social Engineering sind die Menschen selbst. Tugenden wie Kundenfreundlichkeit und Eigeninitiative kann man nicht ernsthaft unterbinden. Trotzdem gibt es Möglichkeiten, auch auf der zwischenmenschlichen Ebene für mehr Sicherheit zu sorgen. Es geht um Sensibilisierung. Die erreicht man, indem man z.B. klarstellt, wo die Grenzen der Hilfsbereitschaft gegenüber Kunden, Kollegen und Vorgesetzten sind. Wichtig ist auch das Bewusstsein, dass selbst eine Handynummer eine vertrauliche Information ist. Man kann weitere Legitimierungsnachweise in sensiblen Bereichen etablieren, um Kunden und Mitarbeiter sicher zu identifizieren. Und über mögliche Angriffsversuche sollten Kollegen sofort informiert werden.

Bekanntlich bestätigen erst Ausnahmen die Regel und man muss dem Mitarbeiter auch eine gewisse Flexibilität zugestehen. Darum ist es außerdem ratsam, eine ständig erreichbare Ansprechperson zu haben, an die sich jeder wenden kann, wenn es einmal notwendig erscheint, die aufgestellten Regeln „großzügig zu interpretieren". Ansonsten kann man davon ausgehen, dass die Sicherheitsmaßnahmen mehr als Schikane angesehen werden, darum nicht gelebt werden und bald in Vergessenheit geraten.

Regelmäßige Schulungen sind unumgänglich. Menschen lernen sehr unterschiedlich und dementsprechend abwechslungsreich sollten auch die angebotenen Schulungsmaßnahmen sein. Es hat sich bewährt, hier eine Kombination aus z.B. Online-Schulungen und interaktiver Schulungssoftware und dgl. zu nutzen. Wichtig sind auch Richtlinien oder Leitfäden.

Sollte tatsächlich ein Hackerangriff erfolgreich sein und ein Datenvorfall vorliegen, muss sichergestellt sein, dass alle wissen, wie damit umzugehen ist, wer zu informieren ist usw.

„Wie man es vom Arbeitnehmerschutz gewohnt ist, müssen Mitarbeiterinnen und Mitarbeiter regelmäßig zu Datenschutz und Informationssicherheit geschult werden."

Mag. Florian Brutter
WK Tirol