SOCIAL ENGINEERING – Gemäss sgz-Cyberexperte Chris Eckert gibt es Zeitgenossen, die sagen: «Es gibt zwei Arten von Unternehmen und Institutionen. Die eine Hälfte wurde schon gehackt, die anderen wissen es noch nicht …» Sicher ist: Beim Schutz vor Cyberkriminalität muss noch viel Aufklärungsarbeit geleistet werden.

«Das passiert doch bei uns nicht …»

«Wir haben doch jetzt Firewall, Virenschutz und einen IT-Verantwortlichen eingestellt, reicht das denn noch nicht?» «Das passiert doch nur bei Firmen, die in der Rüstungsindustrie tätig sind …» «Wir haben ja keine Informationen, die andere interessieren!» «Unsere IT-Sicherheit ist 100-prozentig und nicht angreifbar …»

Vorneweg: Solche Aussagen hören wir auch im Jahre 2021 noch oft von Entscheidungsträgern und Verantwortlichen, wenn wir nach dem Auftauchen irgendeines Sicherheitsproblems zur Ursachenerhebung eines Angriffs, der Untersuchung der Umstände und der möglichst schnellen Schadensbehebung angefragt werden.

Weitsichtige Zeitgenossen, manche könnten auch sagen, es seien Pessimisten mit einem ketzerischen Ansatz, sagen heute: «Es gibt zwei Arten von Unternehmen und Institutionen. Die eine Hälfte wurde schon gehackt, die anderen wissen es noch nicht …»

«Passiert mir doch nicht»: Nonchalance ist Wasser auf die Mühlen von Cyberkriminellen. Bild: 123RF

In der Tat, seriöse Unternehmen fokussieren sich heute meist auf die elektronische Absicherung ihrer IT-Systeme gegen Cyberattacken und Datendiebstahl. Für Angreifer etwelcher Art wird es daher immer schwieriger, auf technischem Weg ins Herz des Unternehmens einzudringen und vertrauliche Daten oder Informationen zu stehlen. Und genau aus diesem Grund konzentrieren sich die Angriffe immer häufiger auf das schwächste Glied jedes Sicherheitskonzepts: den Menschen.

Jeder von uns kann somit, meist unbewusst, betroffen sein und damit den Schutz der Unternehmenswerte – den eigentlichen «Kronjuwelen» – gefährden. Solche Angriffe nutzen die Hilfsbereitschaft, die Gutgläubigkeit oder die Unsicherheit von uns Menschen aus. Social Engineering wird also überall dort angewendet, wo Menschen der Schlüssel zu Geld, interessanten Informationen oder vertraulichen Daten sind. Nicht nur Unternehmen vom Kleinst-KMU bis zum Weltkonzern sind davon betroffen. Auch staatliche Einrichtungen und Behörden können ebenso wie Privatpersonen manipuliert und ausspioniert werden. Je unkritischer und gutgläubiger wir Menschen uns in der heutigen Gesellschaft verhalten, desto leichteres Spiel hat die Gegenseite.

Moderne Spione

Social Engineering heisst die Gefahr, und sie ist heute eine der erfolgreichsten Angriffsmethoden. Sie hat das Ziel, Personen zu beeinflussen und bestimmte Verhaltensweisen hervorzurufen. Das Vorgehen basiert auf Lügen, der Vorgabe falscher Identitäten sowie erfundenen Geschichten. Social Engineering ist die gezielte Nutzung psychologischer, taktischer und technischer Manipulationen, um jemanden zu Handlungen zu bewegen, die er nicht möchte oder nie und nimmer vorhatte. Damit werden Mitarbeitende verleitet, Daten, Konzepte, interne Strukturen, Patente, Kundenlisten etc. preiszugeben oder sogar Zugriff auf ihre Systeme zu gewähren.

Social Engineering ist kein neues Phänomen, sondern mit einem englischen Begriff neu versehen worden. Seit es die Menschheit gibt, sind Geheimnisse vorhanden. Und genauso lange gibt es Menschen, die hinter die Geheimnisse der anderen kommen wollen, aus wirtschaftlichen, militärischen, wissenschaftlichen, politischen Gründen oder um die Konkurrenz zu schwächen. Weshalb selbst etwas entwickeln, kaufen oder herstellen, wenn man es billiger und schneller beim Konkurrenten beschaffen kann? Mussten Kriminelle und Spione – man kann sie auch etwas weniger dramatisch als «Ausspäher» bezeichnen – beim Social Engineering früher viel Mut und schauspielerische Begabung mitbringen, sind heute zusätzlich Organisationstalent, Verständnis und Wissen in Elektronik und IT sowie Teamgeist gefragt.

Dieser Bedrohung sind wir nicht einfach schutzlos ausgesetzt! Im Gegenteil: Schutz- und Gegenmassnahmen sind heute nötiger denn je. Das effizienteste und kostengünstigste im Bereich der Schwachstelle Mensch für einen Betrieb oder Institution ist die Sensibilisierung aller Mitarbeitenden. In gezielten Workshops und Trainings wird auf folgende Themenschwerpunkte eingegangen:

- Arten von Angreifern und Erkennen von Schwachpunkten
- Schwachstelle Mensch, Bedrohungen und Angriffsmethoden
- Gefälschte Informationen, Social Engineering und versteckte Absichten erkennen/abwehren
- Sicherheitsbewusster Umgang mit Informationen
- Cyberhygiene und Prävention

Chris Eckert

DER AUTOR

Autor **Chris Eckert** ist Founding Partner der Swiss Business Protection AG und verfügt über mehr als 30 Jahre kriminalistische Erfahrung, erworben bei der Kantonspolizei Zürich und der Bundeskriminalpolizei.

www.fh-hwz.ch
www.swissbp.ch

UNTERNEHMENSCHUTZ

Neuer Lehrgang

Zugeschnitten auf den umfassenden Unternehmensschutz für KMU in der Schweiz wurde ein neuer Lehrgang erschaffen. Der CAS «Business Protection» an der Hochschule für Wirtschaft HWZ in Zürich startet erstmalig am 3. Juni 2021 und dauert berufsbegleitend 18 Tage. Es sind noch Studienplätze frei:

https://fh-hwz.ch/produkt/cas-business-protection/