Michael Kelemen

Informationen zur IT-Sicherheit

Aufgrund der massiv angestiegenen Datendiebstähle durch Hacker und die sog. Cyberkriminalität muss auf das Thema IT-Sicherheit und was jeder dafür tun kann, ein besonderes Augenmerk gesetzt werden.

Die meisten Sicherheitsverletzungen sind nicht auf technische Probleme zurückzuführen, sondern auf menschliches Versagen. Cyberkriminelle sind sich des mangelnden Bewusstseins der User bewusst und suchen gezielt nach Personen, um in die IT-Systeme eines Unternehmens einzudringen oder auf sensible Informationen zuzugreifen. Daher ist eine IT-Sicherheitsinformation ein wichtiger Schritt zur Verteidigung gegen Cyberangriffe.

Solche Sensibilisierungen sind ebenfalls ein wichtiger Bestandteil der Einhaltung der DSGVO. Die Folgen eines Datenklaus sind datenschutzrelevant (Meldung von Datenpannen an die Aufsichtsbehörde und auch an die betroffenen Personen) und auch kriminalpolizeiamtlich zu melden. Oft werden Lösegelder für die Freischaltung von verschlüsselten Daten verlangt.

Die Aufsichtsbehörden und Kriminalbehörden verlangen im Voraus, dass Beschäftigte, die mit personen-bezogenen Daten arbeiten, auf das Thema nachweislich sensibilisiert werden, damit der Betrieb besser geschützt wird. Der bekannteste Verbreitungsweg für Schadsoftware ist die E-Mail. Dabei ist nicht der E-Mail-Text selbst das Schadprogramm, sondern ein Hyperlink (Verknüpfung) in der E-Mail, die durch Anklicken im E-Mail-Text die Schadsoftware herunterlädt. Alternativ befindet sich im E-Mail-Anhang ein Schadprogramm wie .exe-Dateien, Bilddateien, PDF-Dateien oder auch Office-Dateien.

Neben der Verbreitung von Schadsoftware über E-Mails können diese auch auf Webseiten versteckt sein, die über das Internet geöffnet werden, wie Bilddateien, Musikdateien, Videos oder ähnliches. Es kann ausreichen, nur die Website zu öffnen, ohne auf diese beispielhaften Dateien zu klicken, um sich eine Schadsoftware herunterzuladen. Nicht nur unseriöse oder illegale Webinhalte sondern auch unzureichend abgesicherte Webseiten können mit Schadsoftware versehen werden.

Wie erkennt man schadhafte E-Mails? Grundsätzlich gibt es keine Musterlösung. Selbst gut ausgebildete Datensicherheitsexperten können nicht immer eine schadhafte Mail erkennen.

Folgende Anzeichen sind zu prüfen:

- Ist der Absendername bekannt?
- Ist die E-Mail-Absenderadresse plausibel?
- Ist der Betrieb des Absenders plausibel?
- Sind viele Rechtschreibfehler in der E-Mail?
- Sind unübliche Schreibweisen vorhanden?
- Möchte die E-Mail auf weitere Seiten verweisen?

E-Mails die auf andere Seiten verweisen um dort ggf. Kennwörter einzugeben nennt man Phishing-Mails. Ziel ist es, z. B. Kennwörter auf Fake-Webseiten einzugeben, um diese dann zu entwenden. Nutzen Sie nicht die Weiterleitungsfunktion von E-Mails sondern geben die Website direkt in den Browser ein.

Auch der Datenklau über soziale Medien ist nicht unüblich. Oft erfolgt das schleichend. Man stellt einen Kontakt her, befreundet sich mit einer Person und im Laufe der Zeit kommen Fragen über den Betrieb oder über Besonderheiten im Berufsleben. Hierbei sollte immer ein Augenmerk auf die Intension des Fragenden gelegt werden.

Sollten Sie einen Verdacht haben oder bereits eine schadhafte Mail geöffnet haben, kontaktieren Sie unverzüglich die IT-Abteilung. Umso schneller reagiert wird, desto höher die Wahrscheinlichkeit, dass der Schaden geringer ausfällt.

Bei Fragen zu diesem Thema oder zum Datenschutz nutzen Sie bitte unser Formular:

www.bdmv.de/de/beratung