6.2. Online Betrügereien: Warnungen und Tipps

„Dear Google user", so beginnt die verheißungsvolle Mail, in der mir aufs Herzlichste gratuliert wird, im Anhang befindet sich selbst ein vom CEO Larry Page signierter Mitteilungsbrief, in dem mir ein Gewinn von sage und schreibe 1,5 Millionen Britische Pfund angekündigt wird. Ich brauche nur noch einige Kontaktdaten mitzuteilen und schon sage ich dem Alltag für ein Weilchen „Ade", da ich mir mit dieser stolzen Summe sicherlich ein paar Tage Urlaub verdient habe.

Doch ich zögere, weil ich einerseits nicht weiß, wie viel 1,5 Millionen Pfund in richtigem Geld (also Euro) wert sind und mich andererseits frage: Woher hat Google eigentlich meine Adresse und geht das mit datenschutzrechtlichen Dingen zu? Doch die eigentliche Frage ist: wer fällt noch auf diese plumpen Gaunermethoden rein? Als Antwort ist leider zu sagen: Es fallen noch viel zu viele auf diese Methoden rein. Andererseits werden die Methoden immer ausgefeilter und raffinierter.

MIT WELCHEN METHODEN SIND DIE UNTERNEHMEN KONFRONTIERT?

- Phishing: darunter versteht man den Versuch, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetbenutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den angegriffenen Unternehmen zu schaden.

- Trojaner (Spionage- /Ausspäh-Software): bezeichnet ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt und zum Beispiel Daten ausspioniert und an den Betrüger leitet (Passwörter und Bankdaten, ...). Trojaner zählen zu den unerwünschten bzw. schädlichen Programmen, der sogenannten Malware.

- Computerviren: sich selbst verbreitende Computerprogramme, die sich in andere Computerprogramme einschleusen.

- Hacking oder Hacken: das illegale Eingreifen in Computersysteme oder Kontenaktivitäten durch das unautorisierte Ausspähen oder Erschleichen von Passwörtern.

Diese Vorgehensweisen sind nicht so selten wie man denkt. Mittlerweile sind die Methoden, diese Programme zu verbreiten immer ausgefeilter. Die plumpe Phishing E-Mail, in der Millionengewinne suggeriert werden, sind dabei nur die Spitze des Eisberges. Eine andere Form sind die Bank E-Mails, in der eine Bank den Kunden warnt, dass sein Zugang nur dann freigeschaltet wird oder bestehen bleibt, wenn er sofort seine Kontaktdaten, möglicherweise sogar sein Passwort, an den Absender zurücksendet. Dann gibt es auch noch die Online-Betrüger, die als „Retter" daherkommen. Sie rufen in englischer Sprache an und stellen sich als den Kundendienst eines großen Softwareunternehmens dar („Hier ist Microsoft"). Das ahnungslose Opfer wird dann genötigt, dem „Helfer" über TeamViewer Zugang zum Computersystem zu geben. Dieser kann dann alles Mögliche an Programmen installieren oder aber den Zugang von außen zum gesamten System freischalten.

Eine immer wieder auftauchende Masche ist der Einbruch in ein Computersystem (egal auf welchem Wege: Computervirus, Maleware, Hacking,...), wobei alle Daten auf dem betroffenen Server sofort verschlüsselt werden. Der Nutzer wird danach aufgefordert, ein Lösegeld zur Entschlüsselung der Daten zu zahlen (meist in Kryptowährung). Um sich gegen solche Angriffe zu wehren ist es ratsam, besondere Schutzmaßnahmen mit dem Informatiker vorzusehen. Generell sollte geprüft werden, ob die Sicherheitskopien täglich gemacht werden und ob sie sicher aufbewahrt werden. Wer merkt, dass eine Verschlüsselung im Gange ist, sollte das betroffene System sofort abschalten und vom Internet trennen. Die Polizei rät, auf keinen Fall ein Lösegeld zu zahlen. Dieser Rat ist doppelt richtig, da einerseits nicht sicher ist, ob danach die Daten tatsächlich wieder entschlüsselt werden und andererseits so die kriminellen Machenschaften auch noch belohnt werden.

ZWEI TIPPS:

Keine unbekannten oder verdächtigen Mails oder Anhänge öffnen!

Eine beliebte Angriffsmethode ist es, den Mailserver eines Betriebs zu hacken und über das Adressbuch an alle dortigen Einträge eine „Rechnung" in Form einer PDF zu versenden. Die PDF ist ein mit einem Virus oder Maleware verseuchte Datei, die Schaden beim Öffnen der Datei anrichten.

TIPP: immer wachsam bleiben und verdächtige Mails nicht öffnen und im Zweifelsfall beim Versender nachfragen, ob die Mail auch von ihm stammt.

Den eigenen Schutz penibel beachten:

- Virenschutzprogramme immer auf dem neuesten Stand halten;
- Sicherheitskopien anfertigen und sicher aufbewahren;
- Nicht auf dubiose oder teils auch kuriose „Angebote" antworten.

WAS MACHEN, WENN EINE DROH E-MAIL EINTRUDELT?

Beispiele:

- Eine Masche der Kriminellen ist es, eine Mail zu senden, die aussieht, als wäre sie von der eigenen E-Mail-Adresse aus versandt. Der Inhalt suggeriert, dass das Konto gehackt wurde und der Angreifer verlangt ein Lösegeld.

- Eine Mail suggeriert, dass eine hohe Geldsumme durch einfache Mittel zu erlangen ist. In diese Kategorie fallen auch die sogenannten „Nigeria-Connections".

Die Geschichte wird erzählt, dass ein Familienmitglied viele Millionen auf einem Konto hat, aber nicht dran kommt und Hilfe beim Empfänger der E-Mail sucht. Oder eine Person ist sterbenskrank und möchte über den Empfänger noch ein gutes Werk tun. Der beste Rat ist, nicht auf solche Nachrichten zu antworten und sie als unerwünschte Maus (Spam) zu markieren. Eventuell kann die E-Mail der Polizei weitergeleitet werden, obwohl diese auch nichts dagegen ausrichten kann, höchstens vor der Betrugsmasche zu warnen.

Leider ist es immer wichtiger, sich jede Nachricht genau anzusehen und nicht aus Routine jeden Anhang zu öffnen. Letztendlich gibt es keine Garantie, dass man nicht gehackt wird. Aber man kann seine Passwörter regelmäßig ändern und so auswählen, dass sie komplex und nicht einfach zu erraten sind. Eine tägliche Sicherheitskopie ist ein Grundschutz, der garantiert, dass im Falle eines Verlustes nur Daten eines einzigen Arbeitstages verloren gehen. Das ist schlimm genug, aber nicht zu vergleichen mit dem Super-GAU eines Totalverlustes aller Daten. Die hier angesprochenen Themen sind ein kleiner Bestandteil einer Weiterbildung im Bereich Datenschutzmanagement, die beim ZAWM Eupen angeboten wird. Der nächste Schulungstermin ist im Herbst 2019 vorgesehen.

Rainer PALM, Rechtsanwalt
MITTELSTÄNDLER – Das Magazin der ostbelgischen Mittelstandsvereinigung – Mai/Juni 2019