Social Engineering – die neue Gefahr!

Kürzlich berichtete Radio SRF1, dass mehrere Schweizer Universitäten Opfer von Hackerangriffen geworden sind. Unbekannte hatten Lohnzahlungen der Unis in insgesamt sechsstelliger Höhe auf dunkle Konten abgezweigt. Wer nun meint, es war ein genialer Code-Knacker, der die Sicherheitsvorkehrungen durch intime Kenntnisse der Systemschwachstellen umging, liegt völlig falsch. Der Angreifer nutzte vermutlich ganz einfach die Hilfsbereitschaft, Gutgläubigkeit, Unkenntnis oder die Unsicherheit von Angestellten aus, um an vertrauliche Zugangsdaten zu gelangen. Damit war es dann ein Leichtes, Empfängerkonten für Lohnzahlungen abzuändern.

Diese Angriffsmethode, auch bekannt als «Social Engineering», hat in den letzten Monaten einen enormen Aufschwung erlebt. Die Methoden sind zahlreich, perfide und werden immer professioneller. In einem ersten Schritt nutzen die Angreifer öffentliche Informationen aus Firmenwebseiten, die meist auch Organigramme mit Namen und Funktion der Kader offenlegen. Damit gerüstet, wird die betroffene Firma telefonisch oder per Mail kontaktiert, um die zunächst allgemeine Recherche zu verfeinern. Hilfsbereite Mitarbeiter werden manipuliert, vertrauliche Informationen weiterzugeben oder Dinge zu tun, die zu grossem Schaden führen. Oft werden Informationen eines ersten telefonischen Kontaktes für einen weiteren, massgeschneiderten Anruf genutzt. Die Betrüger verwenden dazu ein breites Spektrum an psychologischen Manipulationsmethoden. Es sind typischerweise die folgenden sechs Schlüsselprinzipien zur Beeinflussung von Menschen:

- Reziprozität – Menschen neigen dazu, sich für einen Gefallen zu revanchieren.
- Autorität – Menschen lassen sich von glaubwürdigen, sachkundigen Experten leiten.
- Konsistenz – Menschen mögen es, mit dem, was sie zuvor gesagt oder getan haben, im Einklang zu sein.
- Sympathie – Menschen sagen lieber Ja zu denen, die sie mögen.
- Konsens – Besonders wenn Menschen unsicher sind, übernehmen sie die Handlungen und Verhaltensweisen von anderen.
- Knappheit (an Ressourcen oder Zeit) – Einfach gesagt, Menschen wollen mehr von den Dingen, die rar sind. Oder sie weichen von vorgeschriebenen Prozessen ab, wenn plötzlich etwas ganz dringend wird.

Eine Krisenzeit, wie die aktuelle Pandemie, vergrössert die Angriffsfläche und Wirksamkeit der oben genannten Methoden. Mitarbeiter im Homeoffice erhalten Mails und Anrufe von Betrügern, die sich als Supportpersonal von Microsoft ausgeben und auf Fehler im Firmennetz hinweisen, die mit hoher Dringlichkeit behoben werden müssen. Angst und Pflichtbewusstsein bewegt ahnungslose Mitarbeiter dazu, «Hilfs- oder Reparaturprogramme» der Betrüger runterzuladen und damit die vollständige Kontrolle über ihren Computer den Eindringlingen zu überlassen.

Besonders dramatisch wird es, wenn Kriminelle die Ängste und Sorgen der Bevölkerung auszunützen. Die Täter verschicken E-Mails, die angeblich von der WHO stammen oder rufen im Namen des BAG an, um an vertrauliche Informationen zu gelangen. Es geht sogar so weit, dass Hacker mit Spyware herausfinden, auf welchen, nicht ganz jugendfreien Internetseiten Familienväter surfen und in der Folge damit drohen, bei Nichtbezahlung eines Lösegeldes, die Familie mit dem Coronavirus zu infizieren.

Die neue Gefahr «Social Engineering» bedroht zunehmend Firmen und Privatpersonen in gleicher Weise. Es wird höchste Zeit, dass wir uns dagegen rüsten! ■

Felix Gassmann

Felix Gassmann ist seit März 2017 Executive Vice President & CTO/CIO der Sauter-Gruppe und seit Dezember 2010 Präsident der Gruppe der Schweizerischen Gebäudetechnik-Industrie (GSGI). Die Gruppe will für die Gebäudetechnikbranche wegweisend sein und unterstützt die Realisierung umweltfreundlicher und energieeffizienter Gesamtsysteme. In seiner Funktion als Präsident der GSGI setzt sich Felix Gassmann für die gemeinsamen Anliegen der Branche ein und vertritt diese in Wirtschaft und Politik.