Social Engineering

Haben Sie das schon gewußt? **Die Vorgehensweise bei Cyber-Attacken hat sich verschoben.** Angreifer versuchen nicht mehr, sich mit Hilfe ihrer hoch entwickelten Tools und Techniken in Ihren Computer reinzuhacken. Sie haben gelernt, dass es einfachere Methoden gibt, Ihren Ihre vertraulichen Informationen zu entlocken. **Stichwort Social Engineering.**

Ein Social Engineering-Angriff findet auf der psychologischen Ebene statt. Der Angreifer versucht, Sie zu einer Aktion zu verleiten, die Sie besser nicht tun sollten. Denken Sie an Trickbetrüger. So funktioniert auch ein Social Engineering-Angriff. Aber mit einem wichtigen Unterschied: der Angriff erfolgt aus dem Internet, er kommt von irgendwo her und kann jeden treffen, auch Sie.

Z.B. Beispiel das sogenannte Phishing. Sie erhalten eine Nachricht, z.B. eine Email, die Sie auffordert, etwas ganz bestimmtes zu tun. Z.B. einem Link zu folgen, oder einen Anhang zu öffnen. Viele Phishing-Versuche sind leicht zu erkennen, weil die Nachricht ziemlich plump daherkommt. Aber es gibt auch Beispiele, die weitaus gefährlicher sind, weil sie gut recherchiert und perfekt formuliert sind und deshalb sehr authentisch wirken.

Beispiele:

- die Email von Ihrem Kollegen, mit der Bitte sich das Dokument noch einmal anzuschauen,
- die Message von Ihrem Chef mit einem Link auf die Quartalszahlen,
- die Email von Ihrem IT-Dienstleister mit der Rechnung im Anhang,
- der Anrufer aus dem IT-Support, der Sie auffordert, eine Fernwartung zu starten,
- die WhatsApp aus der Kantine mit dem Speiseplan der nächsten Woche,
- Ihre Lieblingswebseite mit dem Link zu den Börsenkursen.

Die Angreifer haben viel dazu gelernt. Darum ist Vorsicht geboten. Hier sind einige Regeln, die Ihnen helfen werden:

- Vorsicht, wenn eine Nachricht außergewöhnlich dringlich gemacht wird oder bei angeblicher Gefahr in Verzug. Ein Angreifer könnte versuchen Stress zu erzeugen und Sie zu einer unvorsichtigen Aktion verleiten wollen.
- Geben Sie nie streng vertrauliche Informationen über eine Email oder einen Messenger oder am Telefon weiter.
- Verlassen Sie nicht den gewohnten Weg, der durch die Sicherheitsrichtlinien in Ihrem Unternehmen vorgegeben ist, auch wenn Sie dazu aufgefordert werden.
- Prüfen Sie bei jeder Email, die Sie öffnen, den Absender, den Adressaten und die Domain im Header: Kein Schreibfehler? Kein Buchstabendreher? Kein Zeichen vergessen oder zuviel?
- Öffnen Sie keine Anhänge, außer Sie sind absolut sicher, dass sie authentisch sind.

Viele Unternehmen haben in den letzten Monaten verstärkt auf Homeoffice gesetzt. Das macht die Gefährdungen durch Social Engineering noch brisanter. Denn im Homeoffice wird private IT und Firmen-IT parallel genutzt. Die Geräte laufen im gleichen lokalen Netzwerk zu Hause, im vielleicht unsicheren

WLAN. Private soziale Kontakte und Firmenkontakte laufen im Homeoffice zusammen. Der Arbeitsplatz wird oft im Wohnzimmer oder einem anderen leicht zugänglichen Raum eingerichtet.
Das sind Faktoren, die einem Social Engineering-Angreifer stark entgegenkommen.

Die bereits existierenden Sicherheitskonzepte sollten überdacht und ggf. an die neuen Gefährdungslagen angepasst werden.
Dabei kann ich Sie sehr gut unterstützen.

Rufen Sie mich an: 05254 9369 420, oder nutzen Sie mein Kontaktformular.