Informationsdienst Datenschutz & Datensicherheit

Schwerpunktthema: Social Engineering

Liebe Kolleginnen und Kollegen,

in dieser Ausgabe unseres Informationsdienstes widmen wir uns einem Thema, das jeden von uns betrifft: Social Engineering - oder einfacher ausgedrückt, die Kunst der Manipulation.

In der Praxis erleben wir leider immer wieder, dass selbst die beste technische Sicherheitsinfrastruktur durch einen unbedachten Klick umgangen werden kann. Denken Sie daran: Cyberkriminelle setzen nicht immer auf komplizierte Hackerangriffe - oft ist es einfacher, einen gutgläubigen Mitarbeitenden zu täuschen.

Die gute Nachricht: Mit dem richtigen Wissen können Sie sich und unser Unternehmen effektiv schützen. Diese Ausgabe gibt Ihnen praktische Tipps, wie Sie Manipulationsversuche erkennen und richtig reagieren.

Ich wünsche Ihnen eine aufschlussreiche Lektüre.

Mit besten Grüßen

Ihr Team vom

Informationsdienst Datenschutz & Datensicherheit

Das Wichtigste in Kürze

- *Social Engineering nutzt menschliche Schwächen statt technischer Lücken*
- *91% aller erfolgreichen Cyberangriffe beginnen mit Social Engineering*
- *Wichtigste Warnsignale: Zeitdruck, ungewöhnliche Anfragen, Vertraulichkeit*
- *Bei Verdacht: Stoppen, nachfragen, IT-Support informieren*

Social Engineering: Was ist das?

Social Engineering ist eine der erfolgreichsten Angriffsmethoden auf Unternehmen. Dabei nutzen Kriminelle nicht technische Schwachstellen, sondern manipulieren Menschen durch psychologische Tricks. Laut aktueller BSI-Statistik beginnen 91% aller erfolgreichen Cyberangriffe mit Social Engineering. Für Unternehmen ist es daher essentiell, dass alle Mitarbeitenden die typischen Angriffsszenarien kennen und wissen, wie sie diese erkennen und abwehren können.

Aktueller Trend: KI „klont" Stimmen

Seit 2024 nutzen Angreifer verstärkt KI-generierte Stimmen für telefonische Social Engineering Angriffe. Dabei werden öffentlich verfügbare Aufnahmen von Führungskräften genutzt, um täuschend echte Sprachnachrichten oder Telefonanrufe zu erstellen.

Fallbeispiel: Der „falsche" Chef

Ein Mitarbeiter der Buchhaltung erhielt eine dringende E-Mail, vermeintlich vom Geschäftsführer. Dieser bat um die sofortige Überweisung von 45.000 EUR für einen wichtigen Geschäftsabschluss.

Die E-Mail-Adresse sah auf den ersten Blick echt aus, enthielt aber einen kleinen Tippfehler. Der Absender drängte auf absolute Vertraulichkeit und schnelles Handeln. Glücklicherweise hatte der Mitarbeiter kürzlich eine Security-Awareness-Schulung besucht und erkannte die typischen Warnsignale der Cyberattacke, die allgemein als „Chef-Masche oder „CEO-Fraud" bekannt ist.

Warnbeispiele im Fallbeispiel

- *Ungewöhnlich dringende Anfrage*
- *Forderung nach Vertraulichkeit*
- *Kleine Abweichung in der E-Mail-Adresse*
- *Umgehen üblicher Prozesse*

Social Engineering: „Erfolgs"-Faktoren

Social Engineering basiert auf grundlegenden menschlichen Verhaltensweisen und Emotionen:

- Häufig genutzte psychologische Hebel:
- Autorität (z.B. Vorgesetzter, IT-Support)
- Zeitdruck ("Muss sofort erledigt werden!")
- Hilfsbereitschaft ("Könnten Sie mir kurz helfen?")
- Angst ("Ihr Account wird gesperrt, wenn...")
- Neugier ("Schauen Sie sich diese Fotos an!")