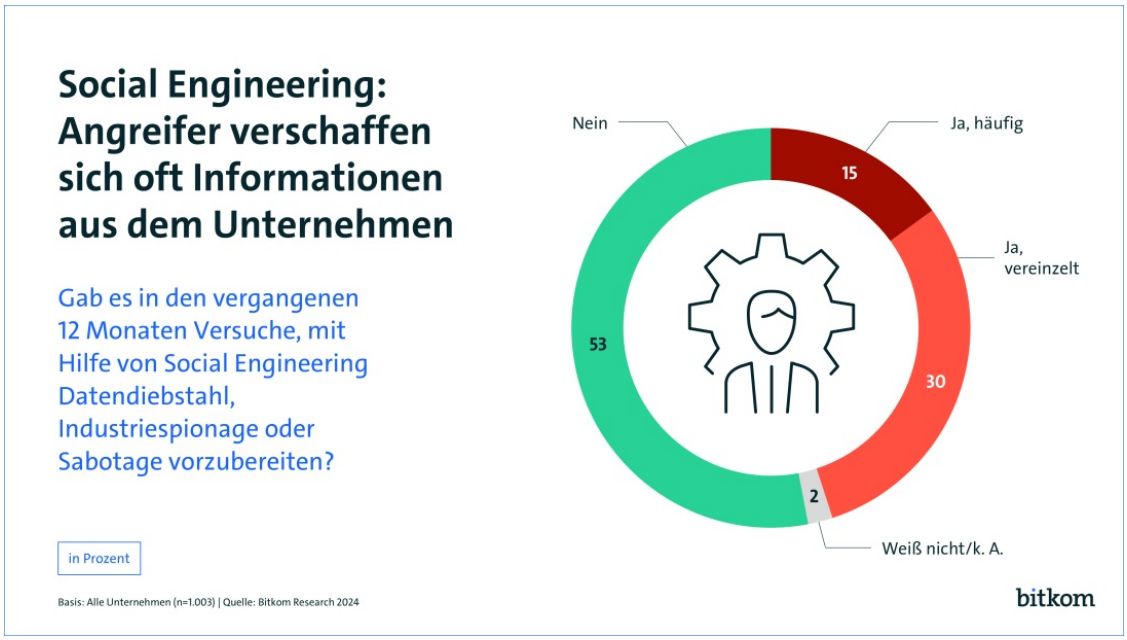
Bitkom e.V. | Presseinformation

Social Engineering: Wenn der Hacker sich als Kollege ausgibt

- **In jedem zweiten Unternehmen wird versucht, Cyberangriffe durch Social Engineering vorzubereiten**
- **Bitkom gibt 4 Tipps, die jedes Unternehmen beherzigen sollte**



Berlin, 11. Oktober 2024 – Ein Anrufer aus der IT-Abteilung, der das Passwort für ein PC-Update braucht, eine E-Mail aus der Vorstandsetage mit Link zu einer Website oder eine verzweifelte SMS der Kollegin, die nicht auf ihren Rechner zugreifen kann – dahinter können Cyberkriminelle stecken, die Informationen für einen Angriff sammeln. Social Engineering nennt sich die Methode, bei der Mitarbeiterinnen und Mitarbeiter manipuliert werden, damit sie vertrauliche Daten preisgeben. In fast jedem zweiten deutschen Unternehmen (45 Prozent) kam es innerhalb eines Jahres zu solchen Vorfällen. 30 Prozent berichten von vereinzelten Versuchen, 15 Prozent sogar von häufigen. Das sind Ergebnisse eine Befragung von 1.003 Unternehmen ab 10 Beschäftigten im Auftrag des Digitalverbands Bitkom. „Durch Social Engineering versuchen Cyberkriminelle zum einen, sich Zugangsdaten zu IT-Systemen zu verschaffen. Zum anderen kann es zunächst einmal nur darum gehen, wichtige Informationen zu sammeln, etwa zu Namen der direkten Vorgesetzten oder eingesetzter Software. Auch solche Angaben können dabei helfen, einen weiteren Social-Engineering-Angriff vorzubereiten oder eine Cyberattacke durchzuführen“, sagt Felix Kuhlenkamp, IT-Sicherheitsexperte beim Digitalverband Bitkom.

Bitkom gibt vier Tipps, wie sich Unternehmen besser vor Social Engineering schützen können:

1. Regelmäßige Schulungen durchführen: Unternehmen sollten regelmäßige Schulungen durchführen, um Mitarbeiterinnen und Mitarbeiter für die Gefahren von Social Engineering zu sensibilisieren. Dabei können sie lernen, verdächtige Nachrichten oder Anfragen zu erkennen und zu melden.

2. Prozesse klar definieren und sicher gestalten: Unternehmen sollten Richtlinien festlegen, welche Informationen auf welchem Weg – etwa telefonisch oder per Mail – weitergegeben werden dürfen und welche zum Beispiel nie, etwa Passwörter. Zudem sollten doppelte Sicherheitsmechanismen, wie das Prüfen und Bestätigen von Überweisungen oder sensiblen Entscheidungen durch mindestens zwei oder mehr Personen in verschiedenen

Unternehmensbereichen implementiert werden. So lassen sich die Risiken durch Manipulationen von Einzelpersonen oder unbefugte Zugriffe stark minimieren.

3. Multi-Faktor-Authentifizierung verwenden: Eine Multi-Faktor-Authentifizierung, bei der neben dem Passwort zum Beispiel auch ein Code auf dem Smartphone oder eine Keycard benötigt wird, erschwert die Nutzung von Informationen, die durch Social Engineering erbeutet wurden. Angreifer können dadurch nicht so leicht in die IT-Systeme eindringen.

4. Moderne IT-Sicherheitssoftware einsetzen: Grundsätzlich sollten Unternehmen Sicherheitssoftware wie Spam-Filter oder Anti-Phishing-Software nutzen, um zumindest einfache Angriffe herauszufiltern. Daneben können spezielle softwarebasierte Systeme eingesetzt werden, um ungewöhnliche Aktivitäten im eigenen Netzwerk zu entdecken, die auf Social-Engineering-Angriffe hindeuten. Künstliche Intelligenz und Anomalie-Erkennung bemerken in vielen Fällen verdächtiges Verhalten und lösen rechtzeitig Alarm aus.

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org
Download Pressefoto

Felix Kuhlenkamp
Leiter Sicherheit
Download Pressefoto
Nachricht senden

Hinweis zur Methodik

Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.003 Unternehmen ab 10 Beschäftigten und einem Jahresumsatz von mindestens 1 Mio. Euro in Deutschland telefonisch befragt. Die Befragung fand im Zeitraum von KW 16 bis KW 24 2024 statt. Die Umfrage ist repräsentativ. Die Fragestellungen lauteten: „Gab es in den vergangenen 12 Monaten Versuche, mit Hilfe von Social Engineering Datendiebstahl, Industriespionage oder Sabotage vorzubereiten?“

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/Social-Engineering-Hacker-als-Kollege