Presseinformation

27. April 2017

Unternehmen als Zielscheibe für Cyberkriminelle

„Streng vertraulich“ steht in der Mail des „Chefs“ an den Mitarbeiter aus der Buchhaltung. Er solle einen fünfstelligen Betrag auf das Konto XY für eine anstehende Firmenübernahme überweisen. Der arglose Mitarbeiter folgt den Anweisungen und schon ist der finanzielle Schaden entstanden.

So schnell könnte es gehen. Unternehmen stehen zunehmend im Visier von Cyberkriminellen. Die Strategien sind vielfältig, aber bevor ein Mitarbeiter ins Blickfeld der Kriminellen rückt, wird die Firma über das Internet auf allen denkbaren Kanälen ausspioniert. Im Anschluss wird ein Mitarbeiter derart geschickt manipuliert, dass er entweder arglos vertrauliche Daten des Unternehmens preisgibt oder Zahlungen an Fremdkonten anweist. Diese neuen Betrugsmaschen werden auch „CEO-Fraud“, „Fake President“ oder „Mandate-Fraud“ genannt.

Grundsätzlich gilt auch hier als beste Schutzmaßnahme – wie bei den meisten Betrugsangriffen über das Internet: „Firewall und Menschenverstand“. Sichern Sie Ihre Systeme: Implementieren Sie Firewalls, Antivirensoftware, Updates und ändern Sie Startpasswörter, auch auf der

Kontakt

Tanja Beller
Bundesverband deutscher Banken e.V.
Director, Pressesprecherin
Tel. +49 30 1663-1220
tanja.beller@bdb.de

Schlagworte

Cyberattacken
Unternehmen
Cyberkriminalität
Social Engineering
Cybersicherheit

Presseinformation

Telefonanlage sowie auf allen mit dem Internet verbundenen Systemen. Appellieren Sie an die Aufmerksamkeit Ihrer Mitarbeiter: Jeder ungewöhnliche Sachverhalt sollte mit gesundem Menschenverstand betrachtet werden. Neben der erhöhten Aufmerksamkeit ist eine offene Unternehmenskultur der beste Schutz für Ihr Unternehmen. Lassen Sie bei ungewöhnlichen Geschäftsvorfällen Rückfragen bis in die Führungsebene zu.

Mit diesen weiteren Tipps schützen Sie Ihr Unternehmen:

- **Prüfen Sie risikobehaftete Prozesse wie Zahlungseingaben und -freigaben oder Stammdatenänderungen etwa bei Kontoverbindungen oder Versandadressen.**
- **Schulen Sie Ihre Mitarbeiter im bewussten Umgang mit den Social-Media-Netzwerken. Kontaktanfragen von Unbekannten sollten nicht leichtfertig akzeptiert werden. Veröffentlichte Daten müssen darauf geprüft werden, ob sie nicht gegen den Mitarbeiter selbst verwendet werden können.**
- **Besondere Vorsicht gilt für den E-Mail-Verkehr: Passen Absender und E-Mail-Adresse zusammen? Ist der Inhalt der E-Mail grundsätzlich plausibel? Passen die Links und Bilder in der E-Mail zum Absender?**
- **Vergeben Sie Nutzerrechte nur in dem Umfang, wie sie zur Erledigung der jeweiligen Aufgaben benötigt werden. Bei Autorisierungsrechten sollte nach dem Vier-Augen-Prinzip vorgegangen werden. Vermeiden Sie, wenn möglich, Einzelvollmachten.**

Wenn Sie diese Tipps beherzigen und Ihre Mitarbeiter regelmäßig für das Thema Cyberkriminalität sensibilisieren, reduzieren Sie das Risiko eines erfolgreichen Angriffs deutlich. Bemerken Sie dennoch, dass Sie das Opfer von Cyberkriminellen geworden sind, wenden Sie sich umgehend an Ihr Kreditinstitut. Die neue Broschüre „Zielscheibe Unternehmen: Cyberkriminalität“ fasst die wichtigsten Informationen und Tipps zusammen und kann kostenfrei beim Bankenverband heruntergeladen oder bestellt werden.