

Checkliste: Wie schütze ich mich vor Social Engineering?

Mehr als 60 Prozent der Angriffe auf die unternehmensweite IT erfolgen heutzutage von den eigenen Mitarbeitern - meist aus Unwissenheit und Höflichkeit. Sensibilisieren Sie sich und Ihr Unternehmen im Bereich der IT-Sicherheit, damit Angreifern der Einlass verwehrt wird.

○ Hinweise für Mitarbeiter zum Schutz vor Social Engineering

- Seien Sie zurückhaltend bei Auskünften. Geben Sie nur so viele Informationen preis wie nötig und hinterfragen Sie ungewöhnliche Anliegen eines Anrufers
- Machen Sie sich bewusst, dass ein Angreifer über einen unscheinbaren PC in das Unternehmensnetzwerk und an sensible Informationen gelangen kann [1]
- Lassen Sie sich nicht einschüchtern oder unter Druck setzen. Halten Sie im Zweifelsfall Rücksprache mit Ihrem Vorgesetzten
- Seien Sie wachsam: Sprechen Sie unbekannte Personen an, die ohne Begleitung eines Mitarbeiters in den Fluren oder gar in den Räumen unterwegs sind
- Melden Sie offen stehende Türen, die gewöhnlich geschlossen sind, noch nicht dagewesene technische Vorrichtungen oder ungewöhnliche Beobachtungen

○ Schützen Sie sensible Informationen

- Bewahren Sie schriftliche Notizen und Ihren Briefverkehr verschlossen auf
- Speichern Sie sensible Dokumente stets verschlüsselt auf Ihrem PC
- Sperren Sie jedes mal Ihren Rechner, wenn Sie ihn verlassen [1]
- Vermeiden Sie an öffentlichen Orten Gespräche über Unternehmensinterna
- Schreddern Sie nicht mehr benötigte Dokumente im Aktenvernichter

○ Tipps für Unternehmer zum Schutz vor Social Engineering

- Wecken Sie bei Ihren Mitarbeitern Verständnis für das Thema Sicherheit. Bewährt haben sich Web-based-Trainings oder Live-Hacking-Demonstrationen [2]
- Definieren Sie Vertraulichkeitsstufen für Informationen und deren Handhabung
- Führen Sie Richtlinien für Wechseldatenträger ein. Durch die Benutzung fremder Datenträger bei Firmencomputern besteht ein enormes Sicherheitsrisiko
- Legen Sie Kontaktpersonen für Geschäftspartner und Kunden fest
- Legen Sie Kommunikationskanäle (z.B. Telefon, Fax, E-Mail oder Brief) für bestimmte Kommunikationen (z.B. Rechnung, Vertrag) fest

Weiterführende Informationen zu diesem Thema:

- [1] <http://ratgeber.it-sicherheit.de> IT-Sicherheitstipps und Hintergrundinfos
- [2] <http://www.internet-sicherheit.de/live-hacking/>
<http://www.kmu-sicherheit.de>
<http://sicherheitskultur.at>

Autoren

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit
Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit
Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter:

<http://www.internet-sicherheit.de>

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: <http://www.kmu-sicherheit.de>