SOCIAL ENGINEERING

DER WIRTSCHAFTSSPIONAGE EINEN SCHRITT VORAUS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

VIELFÄLTIGE ANGRIFFE AUF IHRE FIRMENDATEN ODER INFRASTRUKTUR ERKENNEN

SENSIBILISIEREN SIE IHRE MITARBEITER

Betriebsgeheimnisse sollten bei Ihnen bleiben. Ist dies nicht der Fall, leidet Ihre Reputation. Durch Charme, Überredungskunst und präparierte Ereignisse können Sicherheitszonen hintergangen werden.

- Im Gegensatz zu technischen Angriffen können Übergriffe auf Ihre Mitarbeiter oder Subunternehmer nur schwer erkannt werden!
- Ihre Mitarbeiter eröffnen Schwachstellen für Angreifer, sei es durch Nutzung von Social Networks, als auch durch Unkenntnis von gezielten Social Engineering Angriffen!
- Sicherheit beginnt nicht also in der IT, sondern in den Köpfen der Mitarbeiter.
- Wie setzen Sie den Kompass für eine ausreichende Befähigung Ihrer Mitarbeiter?

„Eine Umfrage unter Führungskräften, die für das Thema Wirtschaftsschutz verantwortlich sind, zeigt: **19%** der Befragten waren bereits Ziel von Social Engineering Angriffen. In den USA waren **59%** der Befragten von dieser Angriffsart bereits betroffen."
*__Umfrage Statista GmbH__

IHR NUTZEN

ERHÖHEN SIE IHR GESAMTES SICHERHEITSNVEAU

- Aufzeigen möglicher Sicherheitslücken und kennenlernen potentieller Gefahren und Risiken im Bereich Informationssicherheit
- Demonstration, wie Social Engineering gezielt ausgenutzt wird zum Erlangen sensibler Unternehmensinformationen
- Erhöhung des Sensibilisierungseffekts durch einen sehr hohen praktischen Anteil unter Einbezug der Teilnehmer
- Dadurch Befähigung Ihrer Mitarbeiter, zur Erkennung verschiedener Angriffe auf das Unternehmen oder auf schützenswerte Informationen Ihres Unternehmens

Security Consulting & Data Protection
TRAINING AND AWARENESS CENTER
Expertise from practice in IT Security and Data Privacy Services

T · · Systems ·

DIGITALE WERTE SCHÜTZEN

Die T-Systems Multimedia Solutions schützt Ihre digitalen Werte und begleitet Sie bei den Themen Sicherheit und Datenschutz im digitalen Wandel. Mit passgenauen Konzepten, umfassender Beratung, aktivem Risikomanagement und der Kooperation mit ausgewählten Partnerunternehmen, sorgen wir für einen anwendbaren und ganzheitlichen Schutz Ihrer sensiblen Daten, „Made in Germany".

SOCIAL ENGINEERING

UNSERE METHODEN UND WERKZEUGE
FÜR EIN PERFEKTES ERGEBNIS

- Hoher Praxisbezug durch interaktive Live Demos
- Aufzeigen von Angriffen mittels Social Engineering
- Bevorzugte Methoden: Human-based vs. Computer–based

Der Impulsvortrag zum Thema Informationssicherheits-Awareness besteht aus den einleitenden Themen (Sensible Daten und Hacker) sowie aus den praktischen Demonstrationen, welche die Teilnehmer mit einbezieht und anhand von live Demonstration das Vorgehen der Angreifer bzw. Hacker aufzeigt.

IHR SCHNELLEINSTIEG
MIT UNSEREM ANGEBOT

- Interaktiver Impulsvortrag zum Thema Informationssicherheits-Awareness
- Dauer: 2 Stunden

Erstdurchführung enthält:
- Individuelle Anpassung der Vortragsinhalte auf Ihre Bedürfnisse und Anforderungen
- Auswahl der gewünschten der Live Demos
- Individualisierung der Schulungsinhalte auf Ihr Unternehmen durch Einbettung von kundenspezifischen Richtlinien für bspw. Passwörter
- Durchführung der Schulung bei Ihnen vor Ort mit anschließender Feedback Runde

Ab dem zweiten Vortrag:
- Durchführung des Impulsvortrags anhand der im ersten Durchlauf zugeschnittenen Inhalte

UNSERE LIVE DEMOS

Live Demo 1
Social Engineering
- Definition der Schwachstelle Mensch
- Wie gehen Angreifer vor

Live Demo 2
Passwörter
- Regeln und Passwort-Richtlinien
- Einfaches hacking von Passwörtern

Live Demo 3
USB-Sticks
- USB-Sick als Hilfmittel der Angreifer
- Richtiger Umgang mit Speichermedien

Live Demo 4
Smartphones
- Informationen beschaffen oder gleich Mitlesen
- Smartphone und WLAN

Live Demo 5
WIFI - vertrauenswürdig oder nicht (Evil Twin AP)
- Gezielte Übernahme von bestehenden WIFI-Verbindungen um als Man in the Middle aktiv zu werden
- Mitlesen von http und https Verbindungen
- Aktives Verändern der Kommunikationsinhalte für das Opfer

Live Demo 6
E-Mails
- Mails von Mitarbeitern oder Vorgesetzten ?!?
- E-Mail Spoofing und deren Erkennung

Live Demo 7
E-Mailanhänge & Links
- E-Mails mit versteckten Inhalten
- Ausspionieren derjenigen, die die Links anklicken

Live Demo 8
Angriffe auf PC mit fehlendem Patch
- Wie kommt die Ransomware auf Ihren PC?
- Opfer PC wird gezielt und unbemerkt angegriffen und unter die Kontreolle des Angreifers gebacht

ANSPRECHPARTNER
Attila Misota
Telefon: +49 (0) 351 - 2820 5745
Mobil: +49 (0) 171 3077 245
E-Mail: Attila.Misota@t-systems.com

Web: www.training-and-awareness.com
Web: www.digitale-werte-schuetzen.de

HERAUSGEBER
T-Systems Multimedia Solutions GmbH
Riesaer Straße 5
D-01129 Dresden
Telefon: +49 (0) 351 - 2820 – 0

www.t-systems-mms.com

T · · Systems ·