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, oder durch Unkenntnis von gezielten Social Engineering Angriffen!
- Sicherheit beginnt nicht also in der IT, sondern in den Köpfen der 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
- Live Demonstrationen: wie Social Engineering gezielt die Schwachstelle Mensch ausnutzt
- 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

DIGITAL RELIABILITY

Digital Trust: Schützen Sie ihre digitalen Werte unter Berücksichtigung ganzheitlicher IT-Sicherheit, aktuellen Datenschutzanforderungen, aktivem Risikomanagement und innovativen Technologien.

Certified Quality: Gewährleisten Sie die Funktionalität, Nutzerfreundlichkeit und Sicherheit Ihrer Geschäftsprozesse basierend auf umfassenden Qualitätsmaßnahmen und zertifizierten Tests.

Reliable Operations: Kombinieren Sie zuverlässigen Betrieb und agile Entwicklungen (DevOps) auf der Basis individueller Service-Stacks von Kundenumgebungen bis hin zu Hyperscale-Cloud-Plattformen.

T · · Systems ·

SOCIAL ENGINEERING

IHR SCHNELLEINSTIEG
MIT UNSEREM ANGEBOT

Der zwei stündige Impulsvortrag zum Thema Informationssicherheits-Awareness besteht aus den einleitenden Themen (Sensible Daten und Hacker), sowie aus praktischen Demonstrationen, welcher die Teilnehmer aktiv mit einbezieht und verschiedene Angriffsvektoren und Vorgehen visualisiert.

Erstdurchführung enthält:
- Individuelle Anpassung der Vortragsinhalte auf Ihre Bedürfnisse und Anforderungen
- Auswahl der gewünschten Live Demos
- Individualisierung der Schulungsinhalte auf Ihr Unternehmen durch Einbettung von kundenspezifischen Richtlinien, wie bspw. Passwörter, der Umgang mit Speichermedien oder die Nutzung von öffentlichen WLAN
- 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
FÜR EIN PERFEKTES ERGEBNIS

Social Engineering
- Definition der Schwachstelle Mensch
- Wie gehen Angreifer vor?

Passwörter
- Regeln und Passwort-Richtlinien
- Einfaches Hacking von Passwörtern

USB-Sticks
- USB-Stick als Hilfmittel der Angreifer
- Richtiger Umgang mit Speichermedien

Smartphones
- Informationen beschaffen oder gleich Mitlesen
- Smartphone und WLAN-Nutzung

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

WLAN
- „Man in the Middle“ Angriffe
- Mitlesen von http und https Verbindungen

E-Mails
- Kommt die Mail tatsächlich von Mitarbeitern oder Vorgesetzten
- E-Mail Spoofing und deren Erkennung

Angriffe auf PC mit fehlendem Patch
- Ransomware auf Ihren PC?
- Opfer-PC wird gezielt und unbemerkt angegriffen und unter die Kontrolle des Angreifers gebracht

Künstliche Intelligenz
- Visualisierung neuer Angrifffsvektoren
- Sprachsynthese als Erweiterung des CEO Fraud

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

Web: www.t-systems-mms.com

ANSPRECHPARTNER
Thomas Rahm
Telefon: +49 (0) 351 2820 2699
Mobil: +49 (0) 170 9168 837
E-Mail: Thomas.Rahm@t-systems.com

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

Web: www.digital-trust.eu

T · · Systems ·