CORPORATE TRUST
business risk & crisis management

Sicherheitsbewusstes Verhalten im Internet

ZIELSETZUNG:

Das Risiko, dass durch Surfen im Internet Viren, Trojaner oder sonstige Malware auf den PC gelangen, nimmt ständig zu. Kriminelle legen es immer häufiger darauf an, durch unbedachtes Handeln der Nutzer an vertrauliche Daten zu gelangen oder durch das Infizieren vieler tausend Computer sog. Bot-Netze zu errichten. Es vergeht kaum ein Tag, an dem nicht von einem Datendiebstahl bei einem Unternehmen oder von Phishing-Attacken auf die PIN oder TAN von Kontoinhabern berichtet wird. Die Angriffsformen werden dabei immer ausgefeilter und häufig nutzen die Hacker die Unachtsamkeit der Internet-Nutzer aus.

Mithilfe von vertraulichen Daten können Täter heute ganz einfach Identitäten fälschen oder Passwörter generieren. Die nötigen Informationen werden von Profilen Sozialer Netzwerke wie Facebook oder XING ausgelesen und am Telefon nähere Details geschickt erfragt (sog. Social Engineering). Die fremden Identitäten können dann zur Bestellung im Internet genutzt werden, z.B. bei eBay oder Amazon, oder für einen Angriff auf das Firmennetzwerk mit einem vermeintlich berechtigten Passwort.

Wie kann ich mich vor Viren, Trojanern oder Drive-by-Downloads schützen? Welche Möglichkeiten gibt es, Social Engineering bereits im Ansatz zu erkennen? Wie verhalte ich mich in sozialen Netzwerken richtig? Wenn Sie bis jetzt noch keine Antwort auf diese und ähnliche Fragen haben, sollten Sie die Möglichkeit zur Sensibilisierung nutzen.

Corporate Trust zeigt bei der Schulung zum sicherheitsbewussten Verhalten im Internet sämtliche aktuell bekannten Angriffsformen auf sowie die Möglichkeiten, sich dagegen zu schützen. Neben der Sensibilisierung, um Social Engineering rechtzeitig zu erkennen, erfahren Sie, welche Einstellungen in sozialen Netzwerken Sie vor dem Verlust Ihrer vertraulichen Daten schützen und wie Sie kritische Internet-Attacken erkennen können.

Für Kinder und Jugendliche bieten wir eine speziell auf ihre typischen Verhaltensweisen (z.B. Online-Spiele, Chat-Rooms etc.) angepasste Schulung

ZIELGRUPPE:

- Internetnutzer im geschäftlichen Umfeld
- Privatpersonen
- Kinder und Jugendliche

ERGEBNIS:

Durch die Sensibilisierung, welche Risiken im Internet bestehen, wie man sich dagegen schützen kann und welche Privacy-Einstellungen man in Sozialen Netzwerken treffen sollte, können Sie Ihre Privatsphäre und das Know-how Ihres Unternehmens schützen.

TRAINER:

Die Schulung wird durch einen Trainer von Corporate Trust durchgeführt, der über langjährige praktische Erfahrung bei der Bekämpfung von Computerkriminalität und Industriespionage verfügt.

INHALT UND ABLAUF:

1. Aktuelle Angriffsformen durch Viren, Trojaner und sonstige Malware

2. Typische Vorgehensweisen der Täter bei:
   - Social Engineering
   - Phishing
   - Identitätsdiebstahl

3. Schutzmaßnahmen beim Surfen im Internet
   - Anti-Viren-Programme & Firewalls
   - Umgang mit E-Mails
   - Einstellungen im Explorer

4. Soziale Netzwerke
   - Privacy-Einstellungen
   - Erkennen kritischer Kontaktaufnahmen
   - Einstellen von Bildern und persönlichen Daten
   - Verknüpfungen mit weiteren Diensten

5. Notfallmaßnahmen bei
   - Verdacht auf einen infizierten PC
   - Identitätsdiebstahl / Phishing etc.

DAUER:

2 – 3 Stunden

VERANSTALTUNGSORT:

Die Schulung findet bei Ihnen statt.

KOSTEN:

2.000,- €

KONTAKT:

Für weitere Informationen oder ein konkretes Angebot wenden Sie sich bitte an:

Christian Schaaf
Geschäftsführer
Telefon 089 / 599 88 75 80
schaaf@corporate-trust.de