InfoGuard
SWISS CYBER SECURITY

Checkliste

Schutz vor Social Engineering

Cyberangriffe zielen heute nicht mehr nur auf Technologien, sondern zunehmend auf den Menschen ab. Beim sogenannten Social Engineering versuchen Angreifer, Mitarbeitende gezielt zu manipulieren, um vertrauliche Informationen zu erhalten oder Zugriff auf Systeme zu erlangen.

Unternehmen investieren zwar in moderne Sicherheitslösungen und technische Schutzmassnahmen, doch selbst die beste Technologie kann nicht verhindern, dass sensible Daten durch menschliches Verhalten preisgegeben werden.

Genau hier setzen Social-Engineering-Angriffe an. Umso wichtiger ist es, sich und seine Mitarbeitenden zu sensibilisieren und klare Verhaltensregeln zu definieren. Die folgenden Praxistipps helfen Ihnen, Social-Engineering-Angriffe frühzeitig zu erkennen und sich wirksam davor zu schützen.

15 praktische Tipps zum Schutz vor Social Engineering im Geschäftsalltag

1. Geben Sie keine vertraulichen Informationen heraus (egal ob per Mail, am Telefon oder auf Social Media) und diskutieren Sie Geschäftsthemen nicht in der Öffentlichkeit.
2. Schliessen Sie vertrauliche Informationen weg, sperren Sie Ihren Computer, wenn Sie Ihren Arbeitsplatz verlassen und vernichten Sie nicht mehr benötigte Unterlagen im Schredder.
3. Sprechen Sie unbekannte Besucher an, wenn sie sich ohne Begleitung auf dem Firmengelände bewegen. Verifizieren Sie Angaben im Zweifelsfall.
4. Schliessen Sie keine unbekannten USB-Sticks an Ihren Computer an.
5. Publizieren Sie auf dem Internet und sozialen Netzwerken nur so viele Informationen wie nötig.
6. Nehmen Sie Freundschaftsanfragen auf Social Media nur von Personen an, die Sie auch wirklich kennen. Fragen Sie im Zweifelsfall lieber nach.
7. Geben Sie persönliche Passwörter nie weiter und verwenden Sie unterschiedliche Passwörter mit 12 Zeichen – Buchstaben, Zahlen und Sonderzeichen.
8. Verhindern Sie die Einsicht durch Dritte bei der Passworteingabe – genauso wie beim Geldautomaten.
9. Klicken Sie Sicherheits-Warnung und -Hinweise nicht einfach weg! Diese enthalten wichtige Informationen. Fragen Sie bei Unklarheit Ihren Helpdesk.
10. Deaktivieren Sie Makros in Office-Programmen wie Word, Excel und Power Point, diese können schadhaften Code enthalten.
11. Öffnen Sie keine dubiosen E-Mails und überprüfen Sie die Absenderadresse. Melden Sie diese E-Mails sofort Ihrer IT-Abteilung.
12. Wenn Sie versehentlich eine verdächtige E-Mail geöffnet haben:
    a. Öffnen Sie keine Anhänge und klicken Sie keine Links an – auch wenn Sie explizit dazu aufgefordert werden.
    b. Prüfen Sie, ob Dringlichkeit erzeugt wird (z. B. „sofort handeln!“ oder „dringend!“) oder ob Sie zur Angabe sensibler Daten aufgefordert werden.
    c. Achten Sie sich zudem auch auf die Anrede.
13. Verifizieren Sie den Link in E-Mails per Mouseover – zeigt der angezeigte Link auch auf die entsprechende Zielseite?
14. Informieren Sie sich über aktuelle Gefahren, da Cyberkriminelle im KI-Zeitalter immer glaubwürdigere Methoden nutzen (z. B. Deepfakes und Voice Cloning), wodurch Angriffe überzeugender und automatisierbar werden.
15. Lesen Sie interne Weisungen zur Sicherheit und dem Datenschutz aufmerksam und halten Sie sich an die geltenden Prozesse.

Ihre Cybersicherheit - Unsere Leidenschaft & Expertise

Cyber Defence & Incident Response sind entscheidend, aber nur zwei Aspekte einer umfassenden und erfolgreichen Cybersicherheit. Unser 360°-Cyber-Security-Ansatz umfasst zudem Cloud Security, Managed Security & Network Solutions für IT-, OT- und Cloud-Infrastrukturen, Penetration Testing & Red Teaming sowie Security Consulting Services. Die SOC-Services werden aus dem ISO 27001-zertifizierten und ISAE 3000 Typ2 überprüften Cyber Defence Center (CDC) in der Schweiz sowie aus Deutschland erbracht – mit 24/7 Betrieb und durchgehend personeller Besetzung.

Gerne unterstützen wir Sie dabei, sich wirksam vor Social Engineering zu schützen

Kontaktieren Sie uns für ein unverbindliches Beratungsgespräch.
info@infoguard.ch · www.infoguard.ch

Baar (Hauptsitz)
InfoGuard AG
Lindenstrasse 10
6340 Baar
Schweiz
infoguard.ch

Bern
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Schweiz
infoguard.ch

Frankfurt
InfoGuard Deutschland GmbH
Frankfurter Straße 233
63263 Neu-Isenburg
Deutschland
infoguard.de

München
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 München
Deutschland
infoguard.de

Düsseldorf
InfoGuard Deutschland GmbH
Am Gierath 20A
40885 Ratingen
Deutschland
infoguard.de

Wien
InfoGuard GmbH
Kohlmarkt 8-10
1010 Wien
Österreich
infoguard.at