AI SECURITY GAME EVENT

WISSEN KOMPAKT

SOCIAL ENGINEERING

Social Engineering ist „psychologisches Hacken“.

Social Engineers manipulieren uns, um an unsere Daten und Informationen zu gelangen.

Sie sind psychologisch perfekt geschult.

Deshalb bemerken wir nicht, wenn uns ein Social Engineer manipuliert.

Fast alle erfolgreichen Cyberangriffe beginnen mit Social Engineering.

MINDCRAFT

5 KI-gestützte Social Engineering-Angriffe

KI-basiertes Social Media Crawling

Mithilfe von KI werden große Mengen an öffentlich zugänglichen Social-Media-Daten automatisch gescannt und analysiert.
Die KI identifiziert gezielt persönliche Informationen, Interessen, Netzwerke und Schwachstellen potenzieller Opfer. Diese Daten dienen als Grundlage für weitere individualisierte Angriffe wie Spear-Phishing oder Identitätsdiebstahl.

KI-generiertes Spear Phishing

Die KI nutzt zuvor gesammelte Daten (z. B. aus Social Media Crawling), um täuschend echte und personalisierte Phishing-Nachrichten zu generieren – oft mit perfektem Sprachstil, Kontextbezug und emotionaler Ansprache.
Dies erhöht die Erfolgsquote massiv im Vergleich zu herkömmlichem Massen-Phishing.

KI-gestütztes Password Hacking

Moderne KI-Modelle analysieren große Datenlecks und Benutzerverhalten, um Passwörter vorherzusagen. Mit Machine Learning werden Muster erkannt und gezielte Passwortkombinationen erstellt, die deutlich effizienter sind als klassische Brute-Force- oder Wörterbuchangriffe.

KI-basierter Identitätsdiebstahl

Die KI erstellt aus öffentlich verfügbaren Daten umfassende digitale Klone von Personen – inklusive Schreibstil, Lebenslauf, Interessen und sogar Stimmproben. So können Angreifer glaubwürdige Fake-Profile erstellen und sich gegenüber Dritten (z. B. HR, Banken) erfolgreich als Zielperson ausgeben.

KI-basierte Real-time Deepfakes

Dank KI lassen sich in Echtzeit täuschend echte Videos oder Audiosequenzen erzeugen, bei denen Personen Dinge sagen oder tun, die sie nie gesagt oder getan haben. Solche Deepfakes können für Erpressung, Desinformation oder gezielte Manipulation in Live-Kommunikation (z. B. Videoanrufe) eingesetzt werden.

5 Goldene Regeln – Wie kann ich mich dagegen wehren?

1

Lass dich von niemandem unter Druck setzen.

Druck ist oft ein Anzeichen dafür, dass dich jemand manipulieren möchte.

PRAXISTIPP: Wenn du unter Druck gesetzt wirst, dann lege IMMER (!) einen "10-Sekunden-Stopp" ein und halte inne. Komm zur Ruhe, denke kurz nach, mache nichts. Und erst nach dieser 10-s-Pause machst du weiter. Das hilft dabei, einen klaren Kopf zu behalten.

2

Glaube niemandem, dessen Identität du nicht zu 100% bestätigen kannst.

Ja, auch nicht dem netten Typen mit Anzug und Krawatte auf LinkedIn.

PRAXISTIPP: Wenn du nicht zu 100% sicher bist, dann übernimm Verantwortung. Eine kurze Rückfrage über einen zweiten, selbst gewählten Kanal (z. B. bekannte Mobil-Nr., bekannter Chat, persönliches Treffen) stoppt über 90 % der Vishing-/Deepfake-Betrugsversuche.

3

Wenn sich etwas komisch anfühlt, sprich mit anderen darüber.

Du musst nicht alles immer alleine machen und können.

PRAXISTIPP: Schon bei leisen Zweifeln kannst du die Stärken deiner Kolleginnen und Kollegen nutzen, indem du mit ihnen darüber sprichst und sie um Rat bittest. Du wirst überrascht sein, wie gerne sie helfen und wie viel besser ihr gemeinsam geschützt seid.

4

Halte dich immer an eure Richtlinien

Die wurden nicht geschrieben, um euch zu ärgern – sondern um euch zu schützen.

PRAXISTIPP: Lass dir von euren Security Experten einen Überblick über die aktuellen Cyber-Richtlinien geben, und drucke sie dir aus. Wenn du sie brauchst, weißt du genau, wo du nachschauen kannst.

5

Fehler melden ist Heldensache!

Angriffe scheitern oft erst, wenn jemand rechtzeitig laut wird.

PRAXISTIPP: Firmen mit klaren Melde-Kanälen und "zero blame"-Kultur halbieren laut Studien erfolgreich ihre Phishing-Raten. Lass also Kolleginnen und Kollegen teilhaben an deinen Erkenntnissen – zum Schutz aller. Sie werden dich dafür feiern!