Hacker lieben Menschen

Der Ethical Hacker Immanuel Bär zeigt im Webinar am 16. Juni, wie IT-Systemhäuser die grösste Schwachstelle im Unternehmen – den Menschen – in eine starke Verteidigungslinie verwandeln können.

Cyberangriffe sind heute oft keine Frage von Technik, sondern der Psychologie. Eine freundliche E-Mail, ein vermeintlich vertrauenswürdiger Anruf oder eine glaubwürdige Nachricht in sozialen Netzwerken – hinter diesen harmlos wirkenden Kontaktaufnahmen steckt oft professionelles Social Engineering: der gezielte Angriff auf den Menschen. Genau das macht diese Methode so gefährlich.

Während Firewalls und Virenscanner längst zur Grundausstattung gehören, bleibt die «menschliche Firewall» häufig deaktiviert. Dabei ist sie wichtiger denn je: 79 Prozent der Angriffe im Jahr 2024 kamen ganz ohne Malware aus. Stattdessen setzen Cyberkriminelle zunehmend auf psychologische Manipulation – mit einer erschreckenden Erfolgsquote.

Besonders alarmierend: Voice-Phishing (Vishing) ist 2024 um ganze 442 Prozent gestiegen. Business E-mail Compromise (BEC) zählt weiterhin zu den häufigsten und teuersten Angriffsmethoden. Und mit KI-basierten Deepfakes erreicht die Täuschung eine neue Dimension. Ein Fall aus dem März 2025 zeigt, wie ein CFO per Deepfake imitiert wurde – mit 25 Millionen US-Dollar Schaden als Folge.

Social Engineering ist heute das lukrativste Geschäftsmodell der Cybercrime-Szene – und es kann und wird jeden treffen.

Es ist nur eine Frage der Zeit, bis es passiert

Ein weitverbreiteter Irrglaube ist, dass sich Social Engineering-Angriffe ausschliesslich auf hochrangige Entscheidungsträger und grössere Unternehmen konzentrieren.

Zwar sind deren Zugangsdaten für Angreifer besonders wertvoll, doch genau diese Personen sind meist gut geschult, sicherheitsbewusst und entsprechend vorsichtig im Umgang mit sensiblen Informationen. Das macht sie zwar nicht unangreifbar, aber schwerer zu täuschen. Zudem verfügen grosse Organisationen meist über spezialisierte Security-Teams und klare Schutzmechanismen, die direkte Angriffe wirksam abwehren.

Cyberkriminelle wählen daher zunehmend einen anderen Weg. Sie richten ihren Fokus gezielt auf Zulieferer oder Dienstleister – Partner, die häufig ein geringeres Sicherheitsniveau aufweisen. Über diesen Umweg der scheinbar harmlosen Partnerunternehmen verschaffen sie sich Zugang zu sensiblen Systemen und Informationen. Entscheidend dabei: Die Kontaktaufnahme wirkt nach aussen hin glaubwürdig. Und genau dieses Vertrauen ist die Schwachstelle, die Social Engineering ausnutzt – ob online oder im persönlichen Gespräch.

Das zeigt deutlich: Eine wirksame Sicherheitsstrategie darf sich nicht nur auf kritische Positionen beschränken. Social Engineering trifft dort, wo Sicherheitsbewusstsein fehlt – und oft genau da, wo es am wenigsten erwartet wird.

Welche Verantwortung tragen IT-Systemhäuser bei einem Cyberangriff?

Die Verantwortung für IT-Sicherheit lässt sich weder rechtlich noch in der Praxis vollständig auf ein Systemhaus oder einen externen IT-Partner übertragen. Unternehmen dürfen erwarten, dass die IT-Dienstleister ihre Aufgaben kompetent erfüllen. Das schliesst nicht nur die Bereitstellung technischer Lösungen ein, sondern auch eine fundierte Beratung über aktuelle Bedrohungsszenarien. Gerade weil das Vertrauen in die Expertise der IT-Partner gross ist, besteht also eine klare Aufklärungs- und Beratungspflicht.

Die bittere Realität: Viele Unternehmen erkennen den Wert präventiver Massnahmen erst dann, wenn es zu spät ist. Deshalb ist es entscheidend, IT-Sicherheit als gemeinsamen Prozess zu verstehen. Der IT-Partner kann und soll unterstützen – doch die letztendliche Verantwortung liegt immer auch beim Unternehmen selbst und dessen Entscheidungsträgern.

Daher bieten viele Reseller – häufig über Distributoren wie Infinigate – strukturierte Security Awareness-Trainings an. Solche gezielten und kontinuierlichen Schulungen können das Risiko erfolgreicher Angriffe deutlich senken.

Bewusstsein schaffen und handeln – Seien Sie dabei!

Im exklusiven Webinar zeigen Immanuel Bär, einer der renommiertesten White Hat Hacker Deutschlands, und Torben Hochmayr, Distribution Manager bei Hornetsecurity, wie Social Engineering in der Praxis funktioniert – und wie Sie sich selbst und Ihre Kunden schützen können.

Immanuel Bär, Mitgründer der ProSec GmbH, verfügt über mehr als 25 Jahre Erfahrung in der IT-Sicherheit. Er war unter anderem an der Zerschlagung einer der grössten Black Hat Communities weltweit beteiligt und ist gefragter Experte in Medien und beim BSI.

Melden Sie sich jetzt kostenfrei an – und schützen Sie Ihre Kunden dort, wo sie am verwundbarsten sind: beim Menschen.