

So machen IT-Systemhäuser **den Menschen** zur stärksten Verteidigungslinie

Cyberangriffe sind längst keine reine Technikfrage mehr – sie zielen auf den Menschen. Eine harmlose E-Mail, ein freundlicher Anruf, eine glaubwürdige Nachricht auf LinkedIn: Hinter scheinbar harmlosen Kontaktaufnahmen steckt oft hochprofessionelles Social Engineering – also der gezielte Versuch, durch psychologische Manipulation Sicherheitsbarrieren zu überwinden.

Das Perfide: Während Firewalls und Virens Scanner selbstverständlich sind, bleibt die „menschliche Firewall“ häufig untrainiert. Dabei sind laut Studien 79 Prozent der Angriffe

Deshalb darf Sicherheit nicht nur auf „kritische“ Rollen abzielen. Social Engineering trifft dort, wo Sicherheitsbewusstsein fehlt – oft in alltäglichen Situationen, in denen niemand einen Angriff vermutet.

Auch Systemhäuser stehen dabei in der Verantwortung. Natürlich lässt sich IT-Sicherheit nicht vollständig auf den IT-Partner übertragen – doch Kunden dürfen erwarten, dass sie kompetent beraten werden. Aufklärung über Bedrohungen gehört heute zur Pflicht, nicht zur Kür. Die Realität zeigt: Prävention wird oft erst nach einem Angriff ernst genommen.



infinigate | HORNETSECURITY | ProSec

Social Engineering, das lukrativste Geschäftsmodell der Welt

Webinar mit Ethical Hacker Immanuel Bär und Hornetsecurity

2024 ganz ohne Malware ausgekommen. Stattdessen setzen Cyberkriminelle verstärkt auf psychologische Tricks – mit wachsendem Erfolg.

Alarmierend ist vor allem der rasante Anstieg von Voice-Phishing („Vishing“) um 442 Prozent. Auch Business Email Compromise (BEC) zählt weiterhin zu den teuersten Angriffsmethoden. Künstliche Intelligenz verschärft die Lage zusätzlich: Deepfake-gestützte Täuschungen erreichen eine neue Qualität – wie ein aktueller Fall zeigt, bei dem ein CFO digital imitiert wurde. Der Schaden: 25 Millionen US-Dollar.

Jedes Unternehmen kann betroffen sein – aber welche Verantwortung tragen IT-Systemhäuser bei einem Cyberangriff?

Ein Irrglaube ist, dass sich Social-Engineering-Angriffe nur auf hochrangige Entscheider richten. In Wahrheit sind es oft Dienstleister, Partner oder kleine Unternehmen mit geringeren Schutzmaßnahmen, über die Angreifer sich Zugang verschaffen – getarnt durch scheinbar vertrauenswürdige Kommunikation. Genau dieses Vertrauen ist die Schwachstelle.

Immer mehr Reseller bieten daher – oft über Distributoren wie Infinigate – strukturierte Security-Awareness-Trainings an. Denn gezielte Schulungen helfen nachweislich, die Angriffsfläche zu minimieren.

Im exklusiven Webinar zeigen **Immanuel Bär**, einer der renommiertesten Ethical Hacker Deutschlands, und **Torben Hochmayr** von Hornetsecurity, wie Social Engineering funktioniert – und wie IT-Systemhäuser sich und ihre Kunden schützen können.

Bär, Mitgründer der ProSec GmbH, bringt über 25 Jahre Erfahrung mit. Er war an der Zerschlagung einer der weltweit größten Black-Hat-Communities beteiligt und ist gefragter Experte beim BSI sowie in den Medien.



Melden Sie sich jetzt kostenfrei an – und lernen Sie, wie Sie aus der größten Schwachstelle im Unternehmen eine starke Verteidigungslinie machen: den Menschen.