»Vertrauen ist größte Schwachstelle«

Webinar: Warum Social Engineering so gefährlich ist

Social Engineering gilt als eine der perfidesten Angriffsformen, weil es den Menschen ins Visier nimmt. Florian Jira, Geschäftsführer von Infinigate Österreich und bekannt als »Mr. Security«, über menschliche Schwächen – und warum IT-Reseller beim Thema Awareness mehr Verantwortung übernehmen müssen.

Florian Jira, Geschäftsführer von Infinigate Österreich, bekannt als »Mr. Security«

Warum ist Social Engineering so gefährlich?
Florian Jira: 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.
Was Social Engineering so perfide macht, ist die Tatsache, dass jeder Mensch individuell reagiert – es gibt keine einheitliche Schutzlösung gegen menschliches Fehlverhalten. Die Angriffsmethoden nutzen Hilfsbereitschaft, Angst oder Vertrauen aus. Und selbst geschulte Personen sind nicht davor gefeit, im entscheidenden Moment eine falsche Entscheidung zu treffen.

Gibt es Zielgruppen innerhalb von Unternehmen, die besonders anfällig für Social Engineering sind?
Ein weitverbreiteter Irrglaube ist, dass sich Social-Engineering-Angriffe ausschließlich auf hochrangige Entscheidungsträger oder technische Administratoren konzentrieren. Cyberkriminelle denken strategisch und weichen gezielt auf weniger offensichtliche Angriffspunkte aus – etwa auf Mitarbeitende aus der Buchhaltung, der Personalabteilung, dem Marketing oder auch auf administrative Assistenzen. Diese Personen stehen oft in engem Kontakt mit Schlüsselrollen im Unternehmen, sind aber deutlich seltener auf solche Szenarien vorbereitet oder durch spezielle Security-Trainings geschult.

Können Unternehmen IT-Sicherheit nicht vollständig an ein Systemhaus oder einen IT-Partner auslagern?
Die Verantwortung für IT-Sicherheit lässt sich nicht vollständig auf ein Systemhaus oder einen externen IT-Partner übertragen – rechtlich nicht und auch nicht in der Praxis. Natürlich darf man als Unternehmen erwarten, dass ein IT-Dienstleister seine Aufgaben kompetent erfüllt. Dazu gehört auch, dass er nicht nur technische Lösungen liefert, sondern seine Kunden umfassend über Sicherheitsrisiken aufklärt. In gewisser Weise besteht also eine Aufklärungs- und Beratungspflicht.
Daher bieten viele Reseller – etwa auch über Distributoren wie Infinigate – strukturierte Awareness-Trainings an. Denn gezielte Schulungen helfen nachweislich, die Angriffsfläche zu minimieren.

Welche Unterstützung bietet Infinigate IT-Resellern im Bereich Security-Awareness konkret – und was erwartet Teilnehmende beim geplanten Webinar am 16. Juni?
Infinigate versteht sich auch im Bereich Security-Awareness als strategischer Partner und »Trusted Advisor« für IT-Reseller. Wir begleiten unsere Partner nicht nur bei der Auswahl technischer Lösungen, sondern auch bei der inhaltlichen und praktischen Umsetzung von Awareness-Maßnahmen. Das Thema ist hochdynamisch, die Anforderungen und Bedrohungsszenarien verändern sich laufend – entsprechend groß ist der Informationsbedarf aufseiten der Reseller. Und genau hier setzen wir an.
Am 16. Juni veranstalten wir dazu ein spezielles Webinar, das gezielt auf die Bedürfnisse von Resellern eingeht. Im Mittelpunkt steht dabei die Frage, wie moderne Awareness-Tools funktionieren, wie sie im Unternehmensalltag implementiert werden können und worauf es bei der Auswahl der passenden Lösung ankommt. Wir geben einen Überblick über die verfügbaren Angebote, zeigen Unterschiede in Qualität und Funktionalität auf und erläutern, was eine gute Lösung von einer weniger geeigneten unterscheidet. Ein besonderer Fokus liegt auf der langfristigen Wirkung: Awareness darf kein einmaliger Impuls sein, sondern muss regelmäßig trainiert werden, um effektiv zu bleiben. Das Webinar am 16. Juni ist eine großartige Gelegenheit, noch tiefer in das Thema einzusteigen.

infinigate
spark your growth

WEBINAR SOCIAL ENGINEERING AM 16. JUNI
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.
Melden Sie sich jetzt zum Webinar am 16. Juni kostenfrei an – und lernen Sie, wie Sie aus der größten Schwachstelle im Unternehmen eine starke Verteidigungslinie machen: den Menschen.