Täuschung als Verteidigung: So funktioniert Cybersecurity 2025

Mit einem eigenen Entwicklungsteam im Herzen Wiens verfolgt CyberTrap ein klares Ziel: Cyberangriffe nicht nur erkennen, sondern ihnen einen entscheidenden Schritt voraus sein. CEO und Mitbegründer Adi Reschenhofer sowie CTO Dr. René Heinzl erklären im Interview, warum herkömmliche Sicherheitsarchitekturen angesichts zunehmend automatisierter Angriffe an ihre Grenzen stoßen – und wie moderne Cybersecurity durch aktive Täuschung, KI-gestützte Analyse und adaptive Digital Twins neu gedacht werden muss. Dabei sprechen sie nicht nur über technologische Durchbrüche, sondern auch über den wachsenden Druck auf CISOs – und warum immer mehr von ihnen an ihre Grenzen kommen.

Herr Reschenhofer, Herr Dr. Heinzl, welche strategischen Herausforderungen kommen auf Unternehmen zu, wenn sie ihre Cyber Defense wirklich zukunftssicher gestalten wollen?
Dr. René Heinzl: Die größte strategische Herausforderung besteht darin, mit der Geschwindigkeit der Angreifer Schritt zu halten – oder ihnen sogar einen Schritt voraus zu sein. Denn die Bedrohungsakteure von heute nutzen bereits KI: von automatisierten Phishing-Kampagnen über KI-generierte Malware bis hin zu adaptivem Verhalten in kompromittierten Netzwerken. Klassische, rein reaktive Sicherheitsansätze kommen da schlichtweg an ihre Grenzen.

Adi Reschenhofer: Cyberabwehr der nächsten Generation ist vorausschauend – sie erkennt Muster, bevor daraus Angriffe werden, und nutzt Täuschung gezielt als strategisches Werkzeug. Wer Sicherheit nicht als Limit, sondern als vorausschauende Intelligenz begreift, legt die Basis für digitale Souveränität und öffnet Räume für echte Innovation. Unser Motto: anders denken.

Angesichts rasant wachsender Cloud-Abhängigkeit und der EU-Regulierung (NIS2, DORA, CRA): Warum muss Cybersicherheit heute Chefsache sein, noch bevor die erste Code-Zeile geschrieben wird?
Dr. René Heinzl: Sicherheit ist heute ein zentraler Bestandteil moderner Systemarchitektur und muss bereits in der Planungsphase mitgedacht werden. Unsere Plattform verfolgt einen technologiegetriebenen Ansatz, bei dem Schutzmechanismen von Anfang an intelligent integriert sind. Gerade mit Blick auf Cloud-Komplexität und Vorgaben wie NIS2 zeigt sich, wie entscheidend eine stabile und zugleich adaptive Architektur ist.

KI kann Angriffe automatisieren, tarnen und skalieren. Welche realen Szenarien ergeben sich daraus für Unternehmen und ihre Sicherheitsstrategien?
Adi Reschenhofer: Cyberabwehr von morgen erkennt Gefahren, bevor sie Form annehmen – sie lernt, täuscht, lenkt und antizipiert. In einer Welt, in der Angreifer mit KI arbeiten, müssen Verteidiger Räume schaffen, in denen der Angriff zur Illusion wird. Wahre Sicherheit entsteht nicht durch Mauern, sondern durch Intelligenz, die das Unbekannte sichtbar macht – und dem Angreifer immer einen Gedanken voraus ist.

Dr. René Heinzl: KI verändert die Spielregeln – und zwar zugunsten der Angreifer. Sie erlaubt es, Schwachstellen automatisiert zu analysieren und Angriffe in Echtzeit anzupassen – schneller, als menschliche Analysten reagieren können. Das Grundproblem bleibt: Der Angreifer muss nur einmal durchkommen, die Verteidiger müssen jeden einzelnen Angriff erkennen und abwehren.

Dr. René Heinzl, CTO

KI-gestützte Bots generieren Phishing-Kampagnen, schreiben Exploits und testen Passwörter. Welche realen Szenarien haben Sie 2024/25 bereits beobachtet, und wie trennt man Hype von akuter Gefahr?
Dr. René Heinzl: Seit 2024 sehen wir eine starke Professionalisierung von Angriffen durch generative KI – etwa durch automatisch erstellte Phishing-Mails oder angepasste Exploits. Was früher Tage dauerte, geschieht heute in Minuten – oft vollautomatisch. Unsere Plattform reagiert darauf mit KI-gestützter Anomalieerkennung und verhaltensbasierten Decoys, die Angreifer frühzeitig enttarnen, noch bevor Schaden entsteht.

Wenn Angreifer KI einsetzen – mit welchen Mitteln kann sich die Verteidigung überhaupt noch behaupten?
Dr. René Heinzl: Wenn Angreifer KI nutzen, bleibt als eine wirksame Antwort nur, selbst KI einzusetzen – aber intelligenter, schneller und vorausschauender. Statt statischer Regeln braucht es lernende Systeme, die auch versteckte Muster erkennen und automatisiert darauf reagieren. Genau das ist die Stärke moderner proaktiver Cyber Defense: Sie erkennt Bedrohungen, bevor sie zum Vorfall werden.

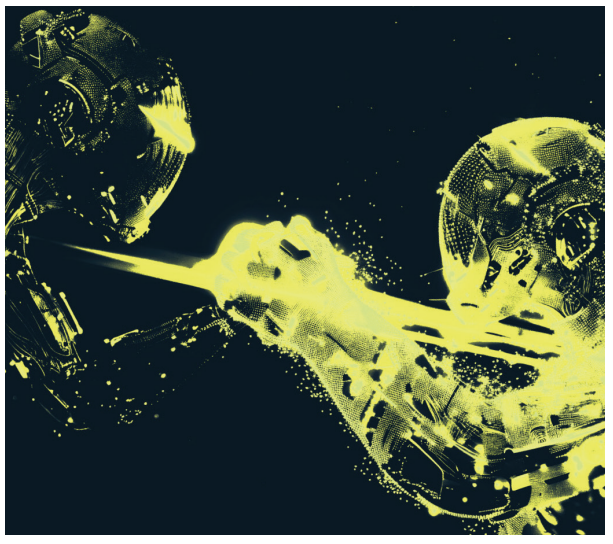
Adi Reschenhofer: In einer automatisierten Bedrohungswelt muss Verteidigung klüger und irreführender sein, um bestehen zu können. KI zwingt uns, Cybersecurity – wie viele andere Bereiche – komplett neu zu denken.

Deepfake-Voicemails, CEO-Fraud, Erpressung im Homeoffice – wie unterstützen Sie Unternehmen dabei, nicht nur Technik, sondern auch Menschen resilienter zu machen?
Dr. René Heinzl: Angriffe wie Deepfake-Anrufe oder CEO-Fraud zielen direkt auf die Verunsicherung von Mitarbeitenden. Deshalb setzen wir nicht nur auf Awareness-Trainings, sondern integrieren täuschungsbasierte Szenarien in den Arbeitsalltag – etwa durch simulierte E-Mails oder Decoy-Zugriffe. So schaffen wir einen sicheren Lernraum, der auf Verständnis und Handlungssicherheit statt Angst basiert.

Welche Rolle spielen täuschungsbasierte Sensoren und automatisierte SOAR-Playbooks, um KI-getriebene Angriffe in Minuten statt Stunden einzudämmen?
Dr. René Heinzl: Täuschungstechnologien wie Honey-Tokens oder Decoy-VMs sind heute hochpräzise Sensoren in Bereichen, die klassische Sicherheitslösungen oft übersehen. Unsere Plattform platziert diese Artefakte dynamisch und verhaltensbasiert – je nach Aktivität im Netzwerk. Kombiniert mit KI-Agenten und SOAR-Systemen entsteht so eine automatisierte Echtzeit-Reaktion, die Angriffe sofort erkennt, isoliert und neutralisiert.

Wie sieht eine Sicherheitsarchitektur aus, die nicht nur schützt, sondern Angreifer aktiv in die Irre führt und daraus lernt – und welche Technologien braucht es dafür?
Dr. René Heinzl: Sicherheitsarchitektur muss heute mehr leisten als nur Abschottung – sie muss Angreifer gezielt fehlleiten und beobachten können. Dafür kombinieren wir Täuschungstechnologien, KI-gestützte Verhaltensanalyse und dynamische Angriffserkennung. Konkret heißt das: Digitale Zwillinge produktiver Systeme werden als Decoys eingebunden, die Angreifer anziehen und deren Verhalten in Echtzeit sichtbar machen – ohne dass sie es bemerken.

Adi Reschenhofer, CEO und Mitbegründer



Zum Abschluss eine persönliche Frage: Viele CISOs stehen heute unter massivem Druck – kurze Reaktionszeiten, hohe Verantwortung, permanente Alarmbereitschaft. Warum geraten so viele in Richtung Burnout – und was müsste sich strukturell ändern, damit Cybersecurity nicht zur psychischen Dauerbelastung wird?
Adi Reschenhofer: Das Thema wurde zu lange ignoriert. CISOs sind heute nicht nur für den Schutz hochkomplexer digitaler Infrastrukturen verantwortlich, sondern müssen gleichzeitig zwischen Management, Regulatorik, IT und Fachabteilungen vermitteln – oft rund um die Uhr und unter enormem Erwartungsdruck. Viele arbeiten im Reaktionsmodus, ständig alarmbereit, ohne die nötige strategische Unterstützung oder klare Entscheidungsbefugnisse. Was es braucht, ist ein Umdenken: Wer CISOs entlasten will, muss ihnen genügend Personal und moderne, automatisierte Werkzeuge zur Seite stellen – und klare Rückendeckung aus der Führungsebene geben. Nur so lässt sich der Druck mindern, bevor er krank macht.

Weitere Informationen via QR-Code:

CYBERTRAP

Genius Tip

»Welchen einen Schritt sollten CISOs morgen früh zuerst setzen, um ihre **Angriffsfläche** kurzfristig um mindestens 30 Prozent **zu reduzieren**? Beginnen Sie mit einer **systematischen Kartierung Ihrer digitalen Assets** – nicht aus Sicht der IT, sondern aus Sicht eines potenziellen Angreifers. Platzieren Sie gezielt **Decoys und Honey-Tokens** an sensiblen Punkten, um unerlaubte Zugriffe sichtbar zu machen. Schon diese eine Maßnahme **schafft Transparenz**, erhöht die **Reaktionsgeschwindigkeit** und **reduziert die Angriffsfläche** spürbar.«