CYBERDISE etabliert „Behavioral Defense Engineering“ als Antwort auf KI-gestützte Bedrohungen

Perspektivenwechsel in der Cybersecurity

ZUG, SWITZERLAND, June 23, 2026 /EINPresswire.com/ -- Die globale Cybersicherheitsbranche hat jahrelang das richtige Problem mit den falschen Methoden bekämpft. Während klassische Security-Awareness-Programme seit über zwei Jahrzehnten stark auf theoretischen Wissenstransfer setzen, bleibt das messbare Risiko unverändert hoch. Eine gemeinsame Studie von CYBERDISE und der Hochschule Luzern (HSLU) belegt wissenschaftlich, was die Praxis längst zeigt: Mehr Wissen führt bei Mitarbeitenden nicht automatisch zu sicherem Handeln, wenn sie mit realen, psychologisch optimierten Angriffen konfrontiert werden.

> “Klassische Sensibilisierung zielt auf das Wissen. Dagegen verbessert Behavioral Defense Engineering das konkrete Verhalten der Leute”
>
> *Palo Stacho*

Als Konsequenz aus dieser Branchenerkenntnis leitet CYBERDISE einen grundlegenden Paradigmenwechsel ein und stellt das Konzept des Behavioral Defense Engineering (BDE) vor. Ziel ist es, menschliches Verhalten nicht länger als rein theoretisches Compliance-Kriterium zu betrachten, sondern als messbaren, operativen Bestandteil der aktiven IT-Sicherheitsprozesse. Mit der Veröffentlichung der neuen Systemversion CYBERDISE V3.2 liefert das Unternehmen die technologische Infrastruktur, um Verhalten zu verbessern und menschliche Reaktionen direkt in verwertbare Cyber-Abwehrdaten zu übersetzen.

Das Problem liegt nicht im Wissen, sondern im Handeln

Die meisten Angestellten wissen heute, dass Phishing-Mails gefährliche Links enthalten können. Dennoch klicken Menschen im stressigen Arbeitsalltag auf bösartige Anhänge, geben Daten preis oder versäumen die rechtzeitige Meldung an die IT-Abteilung. Das Problem moderner Cybersecurity ist demnach kein Wissensdefizit, sondern eine Verhaltenslücke.

„Klassische Sensibilisierung zielt auf das Wissen. Dagegen verbessert Behavioral Defense Engineering das konkrete Verhalten der Leute“, erklärt Palo Stacho, Gründer von CYBERDISE. „Im Zeitalter des KI-gestützten Angriffe reicht theoretisches Wissen nicht mehr aus. Social

Engineering erfolgt hochgradig personalisiert über mehrere Kanäle und es wird immer Angriffe geben, welche bis zum Empfänger durchschlagen, am Security Operations Center (SOC) vorbei. Unternehmen müssen in der Lage sein, auch menschliche Signale in Echtzeit-Sicherheitsdaten umzuwandeln, um die kollektive Reaktionsgeschwindigkeit zu optimieren."

"Unsere Forschung zeigt, dass Mitarbeitende eine effektive erste Verteidigungslinie bilden können – aber nur, wenn die richtigen Werkzeuge zum exakt richtigen Zeitpunkt eingesetzt werden. Da Angreifer immer raffinierter vorgehen, müssen unsere Reaktionen einen Schritt voraus sein. Ein System, das menschliches Verhalten aktiv mobilisiert, ist eine notwendige Ergänzung im modernen Sicherheitsarsenal", ergänzt Dr. Carlo Pugnetti von der (HSLU)."

Behavioral Defense Engineering als operativer Sicherheitsfaktor

Der Kern von Behavioral Defense Engineering liegt in der kontinuierlichen Messung und Optimierung des realen Verhaltens in Akut-Situationen – statt des blossen Abhakens von Schulungsvideos oder Multiple-Choice-Tests. Menschliche Reaktionen werden dadurch zu einem aktiven Frühwarnsystem, dem Cyber Defense Intelligence System geformt.

Vom Echtzeit-Angriff zur sofortigen Immunisierung

Wie dieser Ansatz in der Praxis funktioniert, zeigen automatisierte Sofortkampagnen: Durchbricht eine echte Phishing-Mail die technischen Filter, wandelt CYBERDISE den Angriffsvektor sofort in eine sichere Simulation um, sobald das SOC die Bedrohung identifiziert und aus den Mailboxen entfernt hat. Die Belegschaft wird so in Echtzeit mit einer Kopie des realen Angriffs konfrontiert und für diese spezifische Bedrohung immunisiert.

Die Version 3.2 der CYBERDISE Suite validiert diesen strategischen Ansatz durch eine Reihe weiterer, koordinierter Werkzeuge:

- Mehrkanal-Angriffssimulationen: Überprüfung des Realverhaltens bei Phishing, Smishing, KI-gestütztem Conversational Vishing, QR-Code-Betrug (Quishing) und Microsoft-Teams-Szenarien.
- Edukative Schwachstellenprofile: KI-gestütztes OSINT analysiert öffentlich verfügbare Daten der Mitarbeitenden für automatisierte, hochgradig personalisierte Angriffssimulationen in Echtzeit.
- SOC-Infrastruktur-Integration: Automatisierbare Workflows verkürzen die Zeitspanne vom gemeldeten Signal bis zur aktiven Incident Response drastisch.

Um diesen notwendigen Sicherheitsansatz für Organisationen jeglicher Grösse flächendeckend zugänglich zu machen, stellt CYBERDISE weiterhin eine voll funktionsfähige Freemium-Edition zum Download bereit.

Über CYBERDISE

Die Cyberdise AG ist ein Pionier im Bereich Behavioral Defense Engineering. Das 2023

gegründete Schweizer Unternehmen mit Hauptsitz in Zug kombiniert wissenschaftliche Erkenntnisse der Verhaltensforschung mit einer KI-gestützten Suite für Incident Reporting, Angriffssimulation, schneller Vorfallreaktion und klassischer Schulung. CYBERDISE beugt heute komplexen Social-Engineering-Bedrohungen bei mehr als 500.000 lizenzierten Nutzern effektiv vor.
Weitere Infos unter: www.cyberdise.io

Palo Stacho
Cyberdise AG
+41 41 511 78 10
palo.stacho@cyberdise.io
Visit us on social media:
LinkedIn
