MANTODEA

FOTOS: BLUE FROST SECURITY GMBH

Proaktive Cyber Security:

Wegweisende Verteidigung im digitalen Zeitalter

Text Patrick Ungeheuer

In der Popkultur werden Hacker oft durch die Leidenschaft dargestellt, mit der sie ihre Tastaturen bedienen. Diese Darstellung mag unterhaltsam sein, verfehlt aber etwas die wahre Natur des Hackens. Viele glauben, dass Cyberangriffe rein technische Übergriffe sind, denen mit technischen Abwehrmaßnahmen wie Firewalls, Anti-Malware und Intrusion-Detection-Systemen begegnet wird. Diese Maßnahmen sind tatsächlich unerlässlich, aber wenn man sich allein darauf verlässt, können Organisationen in eine trügerische Sicherheit gelockt werden. Tatsächlich nutzen Hacker oft eine Kombination aus technischen und menschlichen Schwachstellen aus.

Angesichts dieser dynamischen und sich ständig weiterentwickelnden Bedrohungslage müssen Cybersicherheitsstrategien adaptiv, zukunftsorientiert und ständig auf unbekannte Herausforderungen vorbereitet sein. Dieser Philosophie liegt die Offensive Cyber Security zugrunde. Es handelt sich um einen proaktiven Ansatz, der nicht nur Standards wie ISO 27001 erfüllt, sondern diese häufig übertrifft und die blinden Flecken identifiziert, die konventionelle Methoden übersehen könnten.

> Angesichts dieser dynamischen und sich ständig weiterentwickelnden Bedrohungslage müssen Cybersicherheitsstrategien adaptiv, zukunftsorientiert und ständig auf unbekannte Herausforderungen vorbereitet sein.

Bei Mantodea Security haben unsere Erfahrungen immer wieder gezeigt, dass gerade diese unvorhergesehenen Schwachstellen, die oft von automatisierten Tools übersehen werden, am gefährlichsten sind. Diese Art von Anfälligkeiten werden häufig zu Einfallstoren für Angreifer.

Einer unserer Hauptmaßnahmen zur Aufdeckung dieser Schwachstellen ist das Red Teaming. Dabei handelt es sich nicht nur um eine Routine-Sicherheitsüberprüfung; es ist eine sorgfältig geplante Simulation von realen Angriffen auf die digitale Infrastruktur eines Unternehmens. Was das Red Teaming von typischen Sicherheitsbewertungen unterscheidet, ist seine dynamische Natur, die sich eng an die sich entwickelnden Taktiken und Strategien echter Gegner anlehnt im Vergleich zu herkömmlichen Überprüfungen, die oft nur die Spitze des Eisbergs erfassen können.

Der letzte Baustein im Puzzle der Cybersicherheit liegt im Verständnis, dass es sowohl um Kultur als auch um Technologie geht. Die ausgefeiltesten Sicherheitssysteme können ins Wanken geraten, wenn eine umfassende Schulung fehlt oder wenn die Führungsspitze die Sicherheit nicht priorisiert.

Um uns in diesem digitalen Zeitalter wirklich zu schützen, benötigen wir eine zweigleisige Wachsamkeit: sowohl technologisch als auch organisatorisch. Dieser ganzheitliche Ansatz stellt sicher, dass wir bereit sind, den unvorhergesehenen Bedrohungen von morgen zu begegnen, unabhängig von ihrem Ursprung.

> Die ausgefeiltesten Sicherheitssysteme können ins Wanken geraten, wenn eine umfassende Schulung fehlt oder wenn die Führungsspitze die Sicherheit nicht priorisiert.

Patrick Ungeheuer
Geschäftsführer der Mantodea Security GmbH

Über den Autor

Patrick Ungeheuer ist der Geschäftsführer der Mantodea Security GmbH in Frankfurt am Main. Zuvor leitete er das Offensive Team bei Blue Frost Security GmbH.

Dieses erfahrene Team wurde zum eigenständigen Unternehmen Mantodea Security, welches sich auf Offensive Threat Intelligence, Red Team Engagements, Penetrationstests und individuelle Sicherheitsanalysen spezialisiert hat. Seine Expertise im Bereich Cybersicherheit wurde von Medien wie "Die Welt" anerkannt.

Weitere Informationen: **www.mantodeasecurity.de**