Costa Rica. Mai 2026

Das größte Risiko eines Cyberangriffs liegt im Unternehmen selbst: Menschliches Versagen und fehlende Investitionen entlarven Unternehmen

- **Grupo EULEN Costa Rica empfiehlt die Einführung von Multi-Faktor-Authentifizierung, permanenter Überwachung und interner Aufklärungsprogramme zur Vorbeugung von Vorfällen**

In einem Umfeld, in dem die digitale Transformation schneller voranschreitet als die technologische Reife vieler Organisationen, gehören menschliches Versagen und fehlende nachhaltige Investitionen in Cybersicherheit weiterhin zu den Hauptschwachstellen, die Unternehmen Vorfällen aussetzen, die ihren Betrieb vollständig beeinträchtigen können.

Das Öffnen von E-Mails zweifelhafter Herkunft, das Betreten nicht verifizierter Webseiten, das Herunterladen externer Dateien oder das Anschließen von USB-Geräten an Firmencomputer sind scheinbar alltägliche Maßnahmen, die unbefugten Zugriff, den Diebstahl von Zugangsdaten, die Installation von Malware oder Ransomware-Angriffe erleichtern können. Das Wachstum von Hybridarbeit, beschleunigte Digitalisierung und die Vernetzung mit externen Anbietern haben die Angriffsfläche von Unternehmen erheblich erweitert und die Schwachstellen erhöht, von denen aus ein Cyberkrimineller Unternehmensabläufe gefährden kann.

Laut dem Threat Landscape Report 2026 *von FortiGuard Labs* verzeichnete Costa Rica im **Jahr 2025 mehr als 225,7 Millionen versuchte Cyberangriffe**, was den wachsenden Druck auf öffentliche und private digitale Infrastrukturen widerspiegelt. Weltweit nehmen Bedrohungen, die sich gegen Unternehmensnetzwerke richten, zu, angetrieben durch automatisierte Kampagnen, künstliche Intelligenz und fortschrittliches Social Engineering.

Menschliches Versagen: der Hauptangriffsvektor

Laut José Ricardo López García, Direktor für Cybersicherheit bei Grupo EULEN, bleibt menschliches Verhalten in der Verteidigungsstrategie entscheidend, obwohl sich technologische Plattformen weiterentwickelt haben, um mehrere Schutzebenen zu integrieren. "*Der Nutzer ist nicht das schwächste Glied, sondern die letzte Verteidigungslinie, wenn alle anderen Schutzmechanismen versagen. Das funktioniert jedoch nur, wenn die Organisation ihn schult, ihm die richtigen Werkzeuge an die Hand gibt und konsequent in alles investiert, was nötig ist, damit ein Angriff gestoppt werden kann, bevor er ausgeführt wird*".

Zu den risikoreichsten Praktiken, die in Unternehmensumgebungen identifiziert wurden, gehören:

- Interaktionen mit gefälschten E-Mails oder Phishing-Kampagnen.
- Das Durchsuchen von nicht vertrauenswürdigen oder unseriösen Webseiten, die von Unternehmenskontrollen nicht validiert wurden. Das Herunterladen unautorisierter Apps oder Dateien.

Für weitere Informationen:
Natalia Carvajal Lorenzo Tel. +506 6081-7777
ncarvajal@themapcomm.com
http://www.themapcomm.com
Die Kartenkommunikation

- Die Verwendung externer Geräte ohne Gerätekontrolle oder DLP-Richtlinien.
- Das Teilen von Firmenzugangsdaten auf anderen Kanälen.

López García warnt, dass sich diese Bedrohungen ständig durch Social-Engineering-Techniken entwickeln, die von künstlicher Intelligenz angetrieben werden und in der Lage sind, hyperpersonalisierte Nachrichten, Deepfakes und Imitationen zu erzeugen, die zunehmend schwer zu erkennen sind.

Mangel an Investitionen und kontinuierlicher Überwachung

Über einzelne Maßnahmen hinaus warnt Grupo EULEN vor einem strukturellen Problem: Viele Unternehmen integrieren Cybersicherheit weiterhin nicht in ihre strategische oder budgetäre Planung.

"Es gibt immer noch Organisationen ohne dauerhafte Überwachung, ohne kontinuierliche Wartung ihrer Plattformen und ohne Kontrolle darüber, was innerhalb ihrer Unternehmensnetzwerke passiert. In der heutigen digitalen Umgebung entspricht das einem Betrieb ohne Sichtbarkeit", sagte López García.

Zu den wichtigsten Schwachstellen, die in Organisationen festgestellt wurden, gehören das Fehlen einer Mehrfaktor-Authentifizierung (MFA), veraltete Systeme und das Fehlen einer dauerhaften Überwachung. Fachleute warnen, dass Multi-Faktor-Authentifizierung nicht länger als fortschrittliche Maßnahme, sondern als grundlegender Schutzstandard für jede Unternehmensumgebung angesehen werden sollte.

Fernando Gamboa, Sicherheits- und Betriebsleiter von Grupo EULEN Costa Rica, betont die Notwendigkeit spezialisierter Unterstützung: "Unternehmen müssen sich für eine umfassende Sicherheitsstrategie entscheiden, bei der Cybersicherheit nicht mehr als optionale Ausgabe, sondern als entscheidender Bestandteil der Geschäftskontinuität enthalten ist. Spezialisten ermöglichen es uns, Bedrohungen in Echtzeit zu verhindern, zu überwachen und darauf zu reagieren, wodurch die operative und finanzielle Auswirkungen erheblich reduziert werden."

Angesichts zunehmend ausgefeilter Bedrohungen wechseln viele Organisationen zu Zero-Trust-Sicherheitsmodellen, einem Ansatz, bei dem kein Benutzer, kein Gerät oder keine Verbindung standardmäßig als vertrauenswürdig gilt, auch nicht jene, die dem Unternehmensnetzwerk selbst angehören.

Spezialisten sind sich einig, dass Cybersicherheit mit einer umfassenden Vision angegangen werden muss, die Technologie, kontinuierliche Überwachung, Risikomanagement und kontinuierliche Schulung der Mitarbeitenden kombiniert – insbesondere in Situationen, in denen Bedrohungen schneller und komplexer werden.

Bei der EULEN Group begleiten wir Organisationen bei der Identifizierung, Erkennung, Überwachung und Reaktion auf Cybervorfälle.

Für weitere Informationen:
Natalia Carvajal Lorenzo Tel. +506 6081-7777
ncarvajal@themapcomm.com Die Kartenkommunikation
http://www.themapcomm.com