Schnellecke Logistics: Cyber-Security im Fokus nach DDoS-Angriffen!

Schnellecke Logistics stärkt Cyber-Sicherheit nach DDoS-Angriffen. Neues Pressegespräch beleuchtet aktuelle Bedrohungen.

Schnellecke Logistics, Deutschland - Heute ist der 8. Juli 2025 und die digitale Welt steht nach wie vor Kopf. Cyberangriffe, insbesondere DDoS-Attacken, sind ein zentrales Risiko für Unternehmen weltweit. Während wir in eine neue Ära der digitalen Transformation eintauchen, sehen wir, dass die Bedrohungen komplexer und aggressiver werden. Schnellecke Logistics, mit Wurzeln in der Automobilbranche, hat die Dringlichkeit von Cyber-Security erkannt und priorisiert diese in seiner Unternehmensstrategie.

Am 7. Juli fand ein Pressegespräch statt, bei dem Markus Werner, Head of Group Competence Center IT Infrastructure, Einblicke in die Herausforderungen gab, mit denen Schnellecke

in den vergangenen Jahren konfrontiert war. Das Unternehmen hat mehrere Cyber-Angriffe erlebt, der letze größere Vorfall war eine DDoS-Attacke gegen den VPN-Konzentrator zu Ostern 2023. Dieser Angriff hatte gravierende Auswirkungen, da Mitarbeitende teilweise nicht mehr arbeiten konnten. Janine Rauch, Head of Corporate Security und CISO, betonte die enorme Wichtigkeit, handlungsfähig zu bleiben.

DDoS-Angriffe: Ein wachsendes Problem

Der Link11 European Cyber Report 2025 zeigt, dass DDoS-Angriffe um satte 137 Prozent im Vergleich zum Vorjahr angestiegen sind. Diese Angriffe sind nicht nur eine Frage der Bandbreite, sie entwickeln sich zu intelligenten Bedrohungen, die immer raffinierter, kurzlebiger und zielgerichteter werden. Nicht weniger als zwei Drittel dieser Angriffe erreichen ihren Höhepunkt innerhalb von nur 10 bis 60 Sekunden, was es schwierig macht, adäquat darauf zu reagieren.

Traditionelle Abwehrmechanismen stoßen hier oft an ihre Grenzen. Die Firma Link11 hebt hervor, dass moderne Botnetze hochgradig koordinierte Angriffe durchführen, unterstützt durch künstliche Intelligenz. Echtzeitsysteme, die durch KI gestützt sind, können Angriffsmuster schnell erfassen und automatische Gegenmaßnahmen einleiten.

Die Lösung: Adaptive Sicherheitsstrategien

Um gegen diese neue Generation von Angriffen gewappnet zu sein, ist es unerlässlich, die Sicherheitsstrategien kontinuierlich anzupassen. Unternehmen wie Schnellecke müssen sich stärker auf adaptive Abwehrmechanismen konzentrieren, die verdächtige Verbindungen analysieren, anstatt nur den Verkehr zu blockieren. Es zeigt sich, dass viele dieser Angriffe politisch motiviert sind, mit einem besonderen Fokus auf kritische Infrastrukturen.

Die Anzahl und Komplexität der DDoS-Angriffe erfordert eine

ganzheitliche Sicherheitsstrategie. Dazu zählen fortschrittliche DDoS-Mitigation, kontinuierliches Monitoring und vor allem der Schutz von Web-Applikationen und APIs (WAAP). Ein Beispiel aus dem Bericht zeigt, dass ein Multi-Vektor-Angriff, der über vier Tage hinweg ging, diverse Angriffstechniken kombinierte, um die Verteidigungssysteme zu überwinden. Effektives Bandbreiten-Monitoring fußt nicht mehr nur auf dem Datenvolumen, sondern benötigt eine weitreichendere Analyse der Angriffsmuster.

Cyber-Security bleibt also ein entscheidendes Thema für Unternehmen, die in der modernen digitalen Landschaft operieren. Schnellecke Logistics hat ihre Lektion gelernt und zeigt, wie wichtig es ist, proaktiv und durchdacht zu handeln. Wie ein alter Spruch sagt: ƷWenn der Fisch stinkt, muss man schnell handelnƷ, und das merkt man in der Cyber-Welt mehr denn je.

Für mehr Informationen über die Herausforderungen und Lösungen in der Cyber-Security werfen Sie einen Blick auf die Berichte von Verkehrsrundschau, Security Insider und Infopoint Security.

Details	
Ort	Schnellecke Logistics, Deutschland
Quellen	• www.verkehrsrundschau.de • www.security-insider.de • www.infopoint-security.de

Besuchen Sie uns auf: wom87.de