

Cyberangriffe im IoT: So sichern sich Unternehmen ab!

Das IoT transformiert Unternehmen weltweit, steigert Effizienz und wirft zugleich erhebliche Cybersecurity-Risiken auf.



Asien-Pazifik, Region - Das Internet der Dinge (IoT) hat die Spielregeln in der Geschäftswelt umgekrempelt. Nie zuvor war der Austausch von Informationen und Daten so schnell und effizient. Damit einher gehen jedoch auch ernste Sicherheitsrisiken, die Organisationen nicht ignorieren können. **Frontier Enterprise** hebt hervor, dass die APAC-Region bis 2030 über 3 Billionen US-Dollar im IoT-Markt erreichen könnte, mit einer jährlichen Wachstumsrate von 30,1%. Diese Zahlen wirken beeindruckend, doch wie sieht es mit der Sicherheit aus?

Umso mehr IoT-Geräte in einer Organisation eingesetzt werden, desto größer wird die Angriffsfläche für Cyberkriminelle. 48% der Nutzer von zellularen IoT-Lösungen nennen

Sicherheits Herausforderungen als eine der größten Hürden beim Skalieren ihrer IoT-Implementierungen. Ein prägnantes Beispiel für die Folgen von Sicherheitsanfälligkeiten ist der SingHealth-Cyberangriff, bei dem die Daten von 1,5 Millionen Patienten kompromittiert wurden. Solche Vorfälle verdeutlichen, dass Downtime großen Organisationen schätzungsweise 400 Milliarden US-Dollar jährlich kostet und damit eine ernsthafte Bedrohung darstellt.

Sicherheits Herausforderungen im IoT

Die wachsende Vernetzung bringt nicht nur Vorteile mit sich, sondern auch Herausforderungen. Laut einer Analyse von **Research Axiom** und **Data Insights Market** wächst der APAC IoT-Sicherheitsmarkt mit einer bemerkenswerten CAGR von 38,67% bis 2033. Dieser Aufschwung wird durch zunehmende regulatorische Anforderungen und das gestiegene Bewusstsein für Cybersicherheitsrisiken angetrieben. Insbesondere in kritischen Infrastrukturen wie im Gesundheitswesen oder in der Fertigung sind die Risiken enorm. Doch welche Lösungen sind notwendig, um diese Herausforderungen zu meistern?

Das wachsende Bedürfnis nach Netzwerksicherheit, Endpunktsicherheit und cloudbasierten Sicherheitslösungen ist unübersehbar. Organisationen integrieren zunehmend IoT-Geräte in kritische Infrastrukturen, was ihre Angriffsfläche vergrößert. Die Komplexität von IoT-Netzwerken und Cyberangriffen stellt eine ständige Herausforderung dar. So ist es nicht verwunderlich, dass die Nachfrage nach spezialisierten Lösungen wie Identity Access Management (IAM) und Intrusion Prevention Systems (IPS) stark steigt.

Strategien zur Verbesserung der Sicherheit

Was können Organisationen tun, um ihre Sicherheit zu verbessern? **Frontier Enterprise** rät zu einer Kombination aus proaktiven und reaktiven Strategien. Proaktiv sollten Unternehmen Authentifizierungsprozesse stärken und in

Schulungen zur Bedrohungserkennung investieren. Reaktive Maßnahmen umfassen das Verständnis für Bedrohungen und den Einsatz digitaler Zwillinge zur Erhöhung der Vorbereitungsfähigkeit auf Angriffe. Dies ist besonders wichtig, da Cyberangriffe eine kontinuierliche Bedrohung darstellen.

Die Lage zu beobachten und die Strategien laufend anzupassen, ist unverzichtbar, um die Sicherheit verbundener Geräte zu gewährleisten. Die Integration von KI-gestützten Technologien zur Bedrohungserkennung wird an Bedeutung gewinnen. Immer mehr Anbieter erkennen dies und entwickeln Sicherheitslösungen, die nicht nur effektiv, sondern auch kosteneffizient sind.

Der Markt wird also nicht nur durch das Angebot an IoT-Geräten, sondern auch durch die Komplexität und die damit verbundenen Sicherheitsherausforderungen geprägt. Das Augenmerk sollte daher auf eine umfassende Sicherheitsstrategie gelegt werden, die sowohl fortschrittliche Technologien als auch Best Practices in der Cybersicherheit einbezieht.

Die Reise in die vernetzte Zukunft ist spannend, birgt jedoch auch ihre Herausforderungen. Bleiben wir agiler und stellen sicher, dass wir die richtigen Maßnahmen ergreifen, um die Risiken in den Griff zu bekommen.

Details	
Ort	Asien-Pazifik, Region
Quellen	• www.frontier-enterprise.com • www.researchaxiom.com • www.datainsightsmarket.com

Besuchen Sie uns auf: wom87.de