Cybersicherheit: Unternehmen in Deutschland müssen endlich handeln!

Zentrale Erkenntnisse zum Handlungsbedarf in der Cybersicherheit für Unternehmen - Experten fordern proaktive Maßnahmen und Awareness-Training.

Deutschland - Was geht ab in der Welt der Cybersicherheit? Niels Beuck, stellvertretender Hauptgeschäftsführer des DSLV Bundesverbands Spedition und Logistik, hat da einige klare Worte gefunden. In einem aktuellen Beitrag auf dispo.cc macht er deutlich, dass es Handlungsbedarf gibt. Viele Unternehmen haben Cybersicherheit lange Zeit auf die lange Bank geschoben und kümmern sich erst nach einem Vorfall um entsprechende Maßnahmen. Dabei sind sie insbesondere mit ihren sensiblen Daten zu Frachten, Routen und Lagerstandorten äußerst verwundbar.

Beuck, der aktiv an einem internationalen Leitfaden zur Cybersicherheit mitarbeitet, empfiehlt, dass dieses Thema

Chefsache werden muss. Awareness-Trainings und regelmäßige Schulungen für Mitarbeiter sind essentielle Bausteine, um Unternehmen widerstandsfähiger gegen Cyberangriffe zu machen. Interessanterweise wird bei vielen Firmen der Datendiebstahl, besonders das gezielte Abgreifen geplanter Transporte, oft unterschätzt. Peter Wachinger von der Oskar Schunck GmbH & Co. KG verdeutlicht, dass laut dem Allianz Risk Barometer Cyberrisiken gerade in Deutschland die größte Bedrohung für Unternehmen darstellen.

Die Gefahr durch Cyberangriffe

Cyberangriffe sind kein Einzelfall ج sie sind weltweit ein Problem, das auch Deutschland betrifft. Die Lage wird auf security-insider.de diskutiert, wo wir erfahren, dass Deutschland im Vergleich zu anderen Ländern oft hinterherhinkt. Hier sind Unternehmer und auch die Gesellschaft gefordert, digitale Sicherheit ernst zu nehmen. Viele Firmen wiegen sich in falscher Sicherheit, während sie naiven Sicherheitsansätzen folgen. Die westliche Welt ist im Cyberkrieg, während Fachkräfte in den IT-Bereich ins Ausland abwandern, da sie hierzulande oft für ihre Fähigkeiten unterbezahlt werden.

Dass Angela Merkels Aussage über das Internet als ȝNeulandȝ nach wie vor relevant ist, zeigt die Passivität, mit der viele Unternehmen im Umgang mit Cyberrisiken agieren. Die Gefahr durch Ransomware, Phishing-Mails und Identitätsfälschungen wird oft nicht ausreichend ernst genommen, was Unternehmen anfällig macht.

Digitale Resilienz und moderne Ansätze

Wie können Unternehmen ihre Resilienz gegen Cyberangriffe stärken? Ein Schlüssel hierzu ist, sich der Risiken bewusst zu werden und diese aktiv zu bewerten. Diese Thematik wurde auch von Prof. Dr. Dennis-Kenji Kipker angesprochen, der auf dem CYBERsicher Zukunftstag über die Rolle der Cybersicherheit für kleine und mittlere Unternehmen referierte. Seine

Präsentation findet sich auf transferstelle-cybersicherheit.de . Viele KMU vernachlässigen grundlegende Aspekte der Cybersicherheit und wie eine aktuelle Studie des TÜV zeigt, überschätzen sie ihre Abwehrmöglichkeiten.

Der Einsatz von Künstlicher Intelligenz (KI) wird immer wichtiger, sowohl zur Verteidigung als auch für Cyberkriminelle bei der Optimierung ihrer Angriffe. Die NIS2-Richtlinie fordert von den Unternehmen den Einsatz innovativer Technologien zur Cyberabwehr. Eine verstärkte Awareness für Cybersicherheit muss in den Unternehmen etabliert werden, oft führt das Geschäftsführungsteam hier das beste Beispiel vor.

Zusammenfassend lässt sich sagen, dass es an der Zeit ist, Cybersicherheit in einem ganzheitlichen Ansatz zu denken. Die Resilienz wird nicht nur als Schutzmaßnahme, sondern auch als Chance zur Innovation betrachtet. Unternehmen, die proaktive Strategien zur Cybersicherheit entwickeln, sind besser für die digitale Zukunft gerüstet.

Details	
Ort	Deutschland
Quellen	• dispo.cc • www.security-insider.de • transferstelle-cybersicherheit.de