NIS2 ERKLÄRT:

Warum der **Baustoffgroßhandel** trotzdem **handeln** muß!

Die Digitalisierung hat den Baustoffgroßhandel in eine neue Ära katapultiert. Digitale Warenwirtschaftssysteme, automatisierte Lagerprozesse und vernetzte Lieferketten ermöglichen eine Effizienz, die vor wenigen Jahren noch unvorstellbar war. Doch mit dieser Transformation geht eine massive Herausforderung einher: die Cybersicherheit … | VON THOMAS KRESS

Jedes digitale System, das den Arbeitsalltag erleichtert, ist auch ein potentielles Einfallstor für Cyberkriminelle. Ein einziger Angriff kann Lieferketten lahmlegen, Bestellungen blockieren und den Ruf eines Unternehmens nachhaltig schädigen. Genau hier setzt die EU mit dem *NIS2-Umsetzungsgesetz* an. Es verpflichtet Unternehmen dazu, sich besser gegen diese Bedrohungen zu wappnen – und zwar mit einem klar definierten Maßnahmenkatalog. Auch wenn der Baustoffgroßhandel nicht unmittelbar betroffen ist, sollten die Maßnahmen nicht ignoriert werden. Viele Kunden sind betroffen und werden über die IT-Sicherheit der Lieferkette den Großhandel als wichtigen Bestandteil mit zur Einhaltung verpflichten. Die folgenden zehn zentralen Anforderungen von NIS2 können helfen, Cyberrisiken zu minimieren.

TKUC Group

Thomas Kress ist IT-Sicherheitsexperte und Inhaber der TKUC Group mit den Marken TKUC und TheUnified. Nach über 25 Jahren als IT-Consultant und Projektmanager machte er sich im Bereich IT-Sicherheit und Telekommunikation selbständig. TheUnified bietet professionelle IT-Security-Lösungen, um Unternehmen perfekt vor Cyberangriffen zu schützen. (Bild: TKUC Group)

Warum der Baustoffgroßhandel im Fokus steht

Der Baustoffgroßhandel nimmt eine Schlüsselrolle in der Bauwirtschaft ein. Baustellen, ob groß oder klein, sind auf eine reibungslose Lieferung von Materialien angewiesen. Beton, Ziegel, Dämmstoffe – ohne die richtige Logistik steht alles still. Was viele nicht bedenken: Diese Abläufe werden heute fast vollständig digital gesteuert. Von Bestellsystemen über Lagerverwaltungssoftware bis hin zur Routenplanung der Lkw – jedes Glied dieser Kette ist potentiell angreifbar. Ein Cyberangriff auf ein System kann daher weitreichende Konsequenzen für den Endkunden haben. Es geht nicht nur um finanzielle Schäden, sondern auch um das Vertrauen der Kunden. Lieferverzögerungen oder Datenlecks könnten langfristig die Geschäftsbeziehungen gefährden. Die Einführung von NIS2 zeigt, daß die EU diese Bedrohung ernstnimmt. Unternehmen müssen sich nun fragen: Sind wir bereit für die Herausforderungen der digitalen Sicherheit?

Die 10 Maßnahmen von NIS2 – so sichern Sie Ihr Unternehmen ab

Das NIS2-Umsetzungsgesetz verlangt von Unternehmen, zehn zentrale Maßnahmen umzusetzen. Diese Vorgaben sind nicht als starre Regeln gedacht, sondern lassen Raum für individuelle Anpassungen – ein Vorteil, aber auch eine Herausforderung. Hier ein genauer Blick auf die Anforderungen und wie sie im Baustoffgroßhandel sinnvoll umgesetzt werden können.

Risiken erkennen und minimieren

Alles beginnt mit einer fundierten Analyse. Unternehmen müssen systematisch Schwachstellen in ihrer IT-Infrastruktur identifizieren. Welche Systeme sind am anfälligsten? Besonders kritisch sind oft Lagerverwaltungssysteme und Bestellplattformen. Es reicht jedoch nicht, diese Risiken nur zu erkennen. Es geht auch darum, sie zu bewerten: Welche Auswirkungen

hätte ein erfolgreicher Angriff? Ein gut durchdachtes Risikomanagement legt den Grundstein für alle weiteren Maßnahmen. Regelmäßige Aktualisierungen sind dabei unerläßlich, denn Bedrohungen entwickeln sich ständig weiter.

Eine Sicherheitsstrategie entwickeln

Ein wirksamer Schutz erfordert klare Ziele und Vorgaben. Eine umfassende Sicherheitsstrategie sollte nicht nur definieren, wie kritische Systeme geschützt werden, sondern auch festlegen, wie auf Angriffe reagiert wird. Dazu gehört auch ein Plan für den Ernstfall: Welche Prozesse müssen priorisiert wiederhergestellt werden, um den Betrieb so schnell wie möglich wieder aufzunehmen? Wichtig ist, daß die Strategie dynamisch bleibt und angepaßt wird.

Die erste Verteidigungslinie stärken

Der Mensch ist oft das schwächste Glied in der Sicherheitskette. Phishing-Mails, unsichere Passwörter und Unachtsamkeit sind häufig die Ursache für erfolgreiche Angriffe. Umso wichtiger ist es, die Mitarbeiter regelmäßig zu schulen. Sie müssen lernen, Bedrohungen zu erkennen und sicher mit sensiblen Daten umzugehen. Dabei sollten die Trainings nicht einmalig, sondern kontinuierlich stattfinden. Das Bewußtsein für Cybersicherheit muß ein fester Bestandteil der Unternehmenskultur werden.

Netzwerksicherheit aufbauen

Das Netzwerk eines Unternehmens ist das Rückgrat seiner IT-Infrastruktur. Angriffe auf dieses System können verheerend sein. Firewalls und Intrusion-Detection-Systeme sollten daher Standard sein. Doch das allein reicht nicht. Durch Netzwerksegmentierung können Unternehmen verhindern, daß Angreifer ungehindert auf alle Systeme zugreifen. Regelmäßige Sicherheitsupdates sind ebenso wichtig, um bekannte Schwachstellen zu schließen.

Incident Response: Schnelles Handeln

Was tun, wenn der Ernstfall eintritt? Ein Incident-Response-Plan hilft, Chaos zu vermeiden. Er definiert, wer im Falle eines Angriffs was zu tun hat. Eine schnelle Kommunikation ist entscheidend, um den Schaden zu begrenzen – sowohl intern, als auch extern. Kunden und Geschäftspartner sollten informiert werden, bevor Gerüchte die Runde machen. Gleichzeitig muß sichergestellt sein, daß alle kritischen Daten durch Backups gesichert sind und schnell wiederhergestellt werden können.

Zugriffsrechte beschränken

Nicht jeder Mitarbeiter benötigt Zugriff auf alle Daten und Systeme. Ein effektives Zugriffsmanagement stellt sicher, daß nur autorisierte Personen Zugang zu sensiblen Informationen haben. Tools wie Mehr-Faktor-Authentifizierung erhöhen die Sicherheit zusätzlich, indem sie verhindern, daß gestohlene Zugangsdaten direkt genutzt werden können.

Lieferkettensicherheit garantieren

Der Baustoffgroßhandel ist eng mit Lieferketten verknüpft. Wenn ein Partnerunternehmen angegriffen wird, können die Konsequenzen auch Ihr Unternehmen treffen. Deshalb sollten Unternehmen klare Anforderungen an die IT-Sicherheit ihrer Partner stellen und deren Einhaltung regelmäßig überprüfen. Ein starkes Netzwerk ist nur so sicher wie sein schwächstes Glied.

Daten durch Verschlüsselung schützen

Daten sind das Herzstück jedes Unternehmens. Von Kundendaten bis hin zu Preislisten – sie müssen jederzeit geschützt sein. Moderne Verschlüsselungstechnologien sorgen dafür, daß Daten während der Übertragung und Speicherung sicher bleiben. Wichtig ist, regelmäßig zu prüfen, ob die eingesetzten Technologien noch dem aktuellen Stand der Technik entsprechen.

Regelmäßige Audits durchführen

Sicherheitsmaßnahmen sind nur dann wirksam, wenn sie regelmäßig überprüft werden. Interne Audits sollten dazu genutzt werden, Schwachstellen frühzeitig zu erkennen. Externe Audits bringen zusätzliches Fachwissen und einen objektiven Blick auf die Sicherheitslage des Unternehmens. Diese Überprüfungen sollten fest in den Betriebsablauf integriert sein.

Berichtspflichten erfüllen

Sollte ein Cyberangriff dennoch gelingen, schreibt das NIS2-Umsetzungsgesetz vor, daß Unternehmen den Vorfall innerhalb von 72 Stunden melden. Diese Transparenz schafft nicht nur Vertrauen, sondern hilft auch, ähnliche Angriffe in Zukunft zu verhindern. Ein klarer Prozeß für die Dokumentation und Meldung von Vorfällen ist daher essentiell.

FAZIT

Das NIS2-Umsetzungsgesetz mag auf den ersten Blick wie eine zusätzliche Belastung wirken, doch es bietet Unternehmen, nicht nur im Baustoffgroßhandel, auch eine große Chance. Wer die Anforderungen ernstnimmt, stärkt nicht nur die eigene IT-Sicherheit, sondern auch das Vertrauen von Kunden und Geschäftspartnern. In einer Branche, in der Zuverlässigkeit und Pünktlichkeit entscheidend sind, wird Cybersicherheit zum Wettbewerbsvorteil. Die Digitalisierung bietet enormes Potential – aber nur, wenn sie sicher gestaltet wird. Jetzt ist die Zeit zu handeln, bevor es zu spät ist.

Noch Fragen? *www.theunified.de*

IMPRESSUM

Computern im Handwerk/ handwerke.de
gegründet 1984, dient als unabhängiges Fachmagazin für moderne Kommunikation den Betrieben der **Bauhaupt- und Nebengewerbe** im „portionierten" Wissens- und Technologietransfer.

Herausgeber: Horst Neureuther

CV Computern-Verlags GmbH
Goethestraße 41, 80336 München

Telefon 0 89/54 46 56-0
Telefax 0 89/54 46 56-50
Postfach 15 06 05, 80044 München
E-Mail: info@cv-verlag.de
redaktion@cv-verlag.de
www.handwerke.de

Geschäftsleitung:
Dipl.-Vw. H. Tschinkel-Neureuther

Anzeigenleitung:
Dipl.-Vw. Heide Tschinkel-Neureuther
e-mail: anzeigen@cv-verlag.de

Redaktion und redaktionelle Mitarbeiter in dieser Ausgabe:
Shirin Arnold, Jan Höppner, Thomas Kress, Björn Lorenz, Horst Neureuther (verantw.), Karin Örarbäck, Gundo Sanders, Verena Sommerfeld, Steven Vindevogel, Alex Wallberger

Anzeigenvertretung:
Medienmarketing SANDERS

Layout:
AD&D Werbeagentur GmbH, Silvia Romann, Dietmar Kraus

Druck:
Walstead NP Druck GmbH, St. Pölten

Druckauflage: 50.500
Tatsächliche Verbreitung: 48.967 (IV/24)

Auflage und Verbreitung kontrolliert.

42. Jahrgang
Erscheinungsweise: 10 x jährlich

Abo-Preis:
29,– € p.a. plus Porto inkl. MwSt.

Einzelpreis: 2,90 €
Ein Abonnement verlängert sich automatisch um ein Jahr, wenn es nicht spätestens 3 Monate vor Ablauf des Bezugszeitraumes gekündigt wird.

ISSN 0931-4679
Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) Berlin

Zur Zeit gilt die Anzeigenpreisliste Nr. 42 vom 01.11.2024.

Titelkopf: © Fotolia.de/yellowj