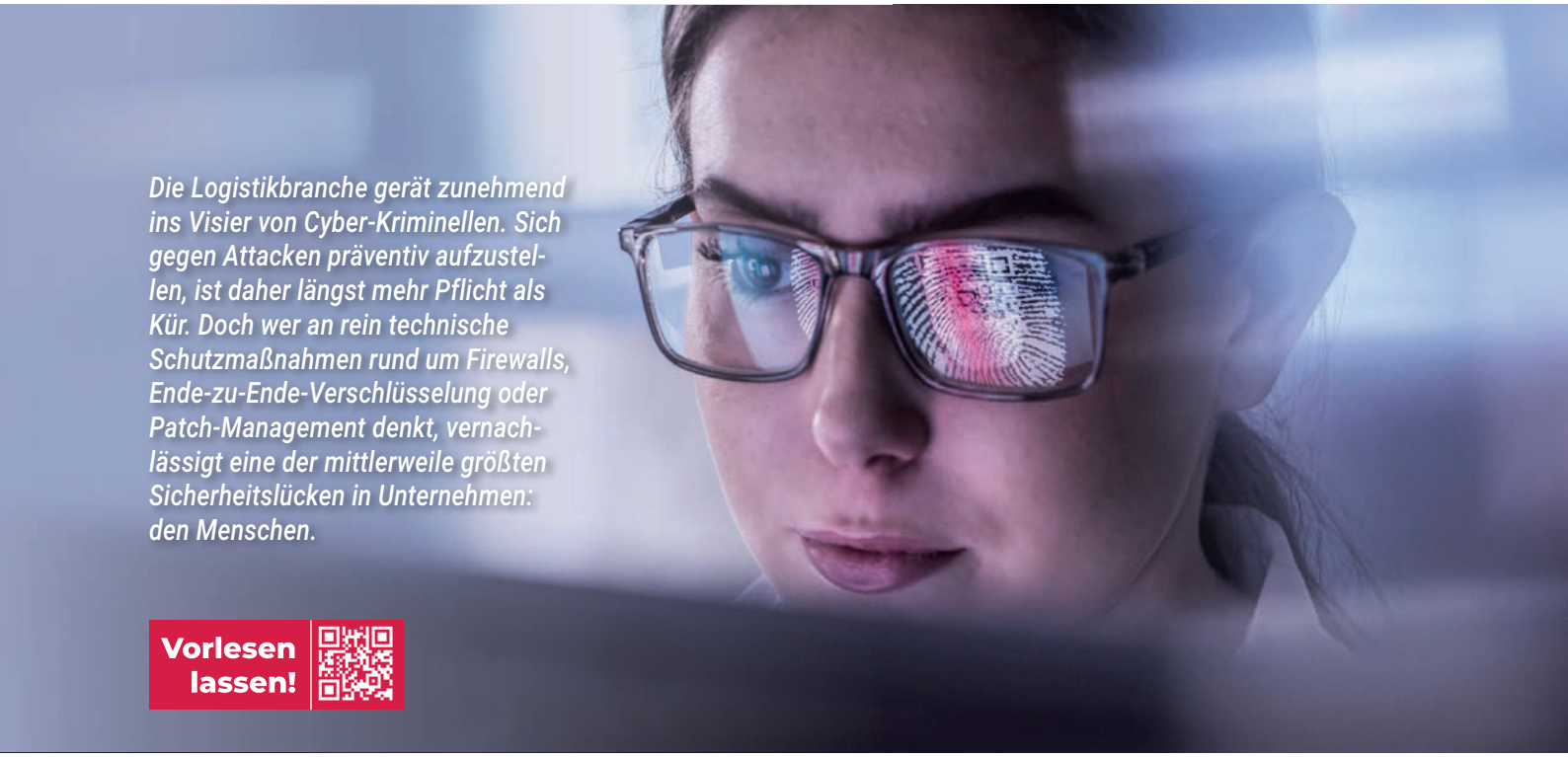
Sicherheitsbewusstsein schärfen



Die Logistikbranche gerät zunehmend ins Visier von Cyber-Kriminellen. Sich gegen Attacken präventiv aufzustellen, ist daher längst mehr Pflicht als Kür. Doch wer an rein technische Schutzmaßnahmen rund um Firewalls, Ende-zu-Ende-Verschlüsselung oder Patch-Management denkt, vernachlässigt eine der mittlerweile größten Sicherheitslücken in Unternehmen: den Menschen.

Vorlesen lassen!

Täglich greifen Mitarbeiter auf sensible Netzwerke zu und somit auf vertrauliche Daten. Durch Vorspiegelung falscher Tatsachen – eine vermeintliche Bekanntschaft, eine scheinbar legitime Nachricht oder ein angeblich legitimer Telefonanruf – setzen Cyber-Angreifer ihre Attacke immer häufiger erfolgreich um. In der Logistik rücken dabei besonders häufig Lieferinformationen, Zollunterlagen, Zahlungsdaten oder Systemzugänge in den Fokus. Wer an dieser Stelle unbedacht klickt, weiterleitet oder bestätigt, kann ganze Lieferketten zum Erliegen bringen. Phishing, Social Engineering und CEO-Fraud sind längst keine Einzelfälle mehr, sondern zunehmend ernstzunehmende Alltagsbedrohungen.

Technik kann also viel leisten, um die Unternehmensgrenzen zu schützen – aber nicht alles. Ohne aufgeklärte, sicherheitsbewusste Mitarbeiter bleibt jede technische Abwehr unvollständig. Um Kriminellen keine Chance zu geben, muss das Sicherheitsbewusstsein innerhalb der gesamten Firma auf- und ausgebaut werden. Dafür rücken die zwei Denkweisen – intuitiv und schnell vs. logisch und entschleunigt – in den Mittelpunkt.

Schnelles Denken als Risikofaktor

Die Psychologie zeigt: Wir treffen Entscheidungen auf zwei Ebenen. System 1 ist schnell, intuitiv, automatisiert. Es hilft uns, im Alltag effizient zu handeln. System 2 ist langsamer, reflektierter, logisch und prüft, hinterfragt und erkennt Musterbrüche. Cyber-Angreifer setzen gezielt auf System 1. Sie gestalten E-Mails, Prozesse oder Nachrichten so, dass sie vertraut, dringend oder emotional aufgeladen wirken – genau das, was unseren Verstand in den Schnellmodus versetzt. Der Klick passiert, der Anrufer wird durchgestellt, der Link geöffnet.

Cyber Security Awareness setzt an diesem Punkt an – und beugt vor. In Schulungen trainieren Mitarbeiter, im richtigen Moment einen Schritt zurückzutreten. Wachsam zu bleiben, Signale zu erkennen, innezuhalten. Eine Fähigkeit, die sich systematisch aufbauen lässt. Wichtig: Die Formate sollten sich am Unternehmen, konkreten Risiken, beobachteten Mitarbeiterverhalten und internen Rollenverteilungen orientieren. Die individuelle Auswahl – einmalige Pflichtkurse gegenüber sich stufenweise aufbauenden Awareness-Schulungen – können Organisationen gemeinsam mit Cyber-Security-Experten treffen. Vorteilhaft ist, wenn diese ebenso auf Erfahrung in der Logistik zurückgreifen können, wie bei der q.beyond logineer der Fall.

Awareness-Programme mit Tiefenwirkung

Im Optimalfall entscheidet sich die Chefetage gegen einmalige Schulungen oder sporadische Hinweise und für ein mehrstufiges Awareness-Programm – zugeschnitten auf die Bran-

Bild: ©Westend61/gettyimages.com

che, die Organisation und die Menschen darin.

1. **Basis-Trainings:** Jeder Einstieg beginnt mit einfachen, unternehmensweit ausrollbaren Schulungen. Themen wie Passwortsicherheit, Phishing-Erkennung und Umgang mit mobilen Geräten stehen hier im Vordergrund.
2. **Risiko- und rollenbasierte Vertiefungen:** Je nach Aufgabenbereich, Abteilung oder Zugriffsebene sollten Mitarbeiter zusätzliche Trainings erhalten. In der Logistik etwa für Disposition, Zollabwicklung oder IT-nahe Rollen. Außerdem benötigen Angestellte, die aus dem Homeoffice arbeiten, andere Inhalte als solche im Lager.
3. **Individuelle Assessments und Wissensstand erfassen:** Ein gezielter Fortschritt wird nur möglich, wenn der Ist-Zustand bekannt ist. Mit Fragen, Tests und simulierten Angriffen lässt sich erkennen, wo blinde Flecken bestehen – und welche Trainings die Organisation priorisieren sollte.
4. **Aktuelle Bedrohungslage integrieren:** Awareness ist kein statisches Thema. Unternehmen sollten regelmäßig Inhalte anpassen: Neue Betrugsmaschen, veränderte Kommunikationskanäle oder gezielte Kampagnen erfordern aktuelle Szenarien.
5. **Bewusstsein zur Kultur machen:** Awareness endet nicht mit dem letzten Trainingsmodul. Es braucht regelmäßige Updates, Reminder, Kampagnen, Ansprechpersonen. Im besten Fall mündet dies in einer Unternehmenskultur, für die Nachfragen, Wachsamkeit und Meldungen selbstverständlich sind.

Weniger Risiko, mehr Reaktionsfähigkeit

Ein durchdachtes Awareness-Programm reduziert nicht nur das Risiko menschlicher Fehlhandlungen – es stärkt auch das Sicherheitsklima im Unternehmen. Mitarbeiter fühlen sich eingebunden und vorbereitet, nicht belehrt. Führungskräfte erhalten belastbare Daten zur Risikolage. Im Ernstfall greift schließlich kein reines Reaktionsschema, sondern verinnerlichte Aufmerksamkeit.

Unternehmen profitieren auf vielen Ebenen:

- Reduzierte Angriffsfläche durch weniger Fehlverhalten
- Stärkere Sicherheitskultur über alle Hierarchiestufen hinweg
- Schnellere Reaktion im Ernstfall durch geschulte Mitarbeiter
- Nachweisbare Maßnahmen für Audits und Kundenanforderungen
- Höhere Sensibilität in der gesamten Lieferkette

Aufmerksam bleiben – bevor es andere werden

Technische Schutzmaßnahmen sind unverzichtbar. Doch sie greifen zu kurz, wenn der menschliche Faktor unberücksichtigt bleibt. Gerade in der Logistik, in der sich Prozesse schnell, datenintensiv und oft standortübergreifend gestalten, braucht es mehr als Firewalls und Verschlüsselung.

> „In der Logistik, in der Prozesse schnell, datenintensiv und standortübergreifend sind, braucht es mehr als Firewalls und Verschlüsselung."

Cyber Security Awareness ist dabei kein Add-on. Sie ist der aktive Teil der IT-Sicherheit, den alle mittragen – vom Lager bis zum Vorstand. Wer Schulungen durchdacht aufsetzt, kontinuierlich verbessert und gezielt auf reale Gefahren abstimmt, gewinnt nicht nur Sicherheit. Am Ende blickt die Firma auf ein Team, das im entscheidenden Moment richtig handelt.

Q.Beyond Logineer GmbH
www.logineer.com