Sicherheit in Transport und Logistik

Ein Whitepaper von TIMOCOM

Kriminalität im Transportwesen

Sofort-Checks zur Verbesserung der Sicherheit

Dieses Whitepaper zeigt, wo typische Risiken liegen, und wie vermeiden Diebstahl in der Straßenlogistik verüben sogenannte Planenschlitzer, die genau wissen, wo sie unbewachte LKW finden und zuschlagen können. Sie sind an die Stelle der früheren Wegelagerer getreten, die Postkutschen aus dem Hinterhalt überfielen und die Insassen um ihr Hab und Gut (und nicht selten auch um ihr Leben) brachten.

Neben klassischen Diebstählen nehmen auch digitale Betrugsfälle deutlich zu. Das Ausmaß dieser Straftaten ist erschreckend. Die Zahlen sprechen für sich: Die Transported Asset Protection Association (TAPA) beziffert die registrierten Frachtverluste in der EU im Jahr 2023 auf 549 Millionen Euro, das macht einen Anstieg von 438 Prozent gegenüber 2022*. Mehr als 8,2 Milliarden Euro kostet Frachtkriminalität Unternehmen europaweit jährlich, so eine Studie des Europäischen Parlaments.

DAS BESTE MITTEL GEGEN PLANENSCHLITZER:
Nur sichere LKW-Parkplätze ansteuern. Für die Parkplatzsuche gibt es heute eine Reihe nützlicher digitaler Hilfsmittel.

▲ **438%**
Anstieg digitaler Betrugsfälle seit 2020

Alle 20 Minuten
Ladungsdiebstahl in Deutschland

* Quelle: https://trans.info/de/frachtdiebstaehle-steigen-eu-weit-419616

Grundregeln zu Nutzung von Online-Frachtenbörsen

Viele Marktteilnehmer nutzen heute Online-Frachtenbörsen, die sich als fester Bestandteil professioneller Disposition etabliert haben – insbesondere bei schwankender Auftragslage und begrenzten Kapazitäten.

Wie bei allen digitalen Transaktionsplattformen gibt es auch hier potenzielle Angriffsflächen.

MIT FOLGENDEN GRUNDREGELN LÄSST SICH DAS SICHERHEITSNIVEAU BEREITS DEUTLICH ERHÖHEN:

1. Achten Sie darauf, dass die Plattform sichere Logins (z. B. 2-Faktor-Authentifizierung), verschlüsselte Verbindungen (https), Schutz gegen Überlastungsangriffe und die Möglichkeit, Zugriffsrechte nach Rolle zu vergeben, unterstützt.

2. Kommunizieren Sie nur über den internen Messenger-Dienst der Frachtenbörse. So können sich Betrüger nicht von außen – etwa über eine gefakte E-Mailadresse – in eine Frachtvergabe einmischen.

3. Führen Sie regelmäßige Sensibilisierungs- und Datenschutzschulungen für die eigenen Beschäftigten durch, um den Umgang mit sensiblen Daten zu trainieren.

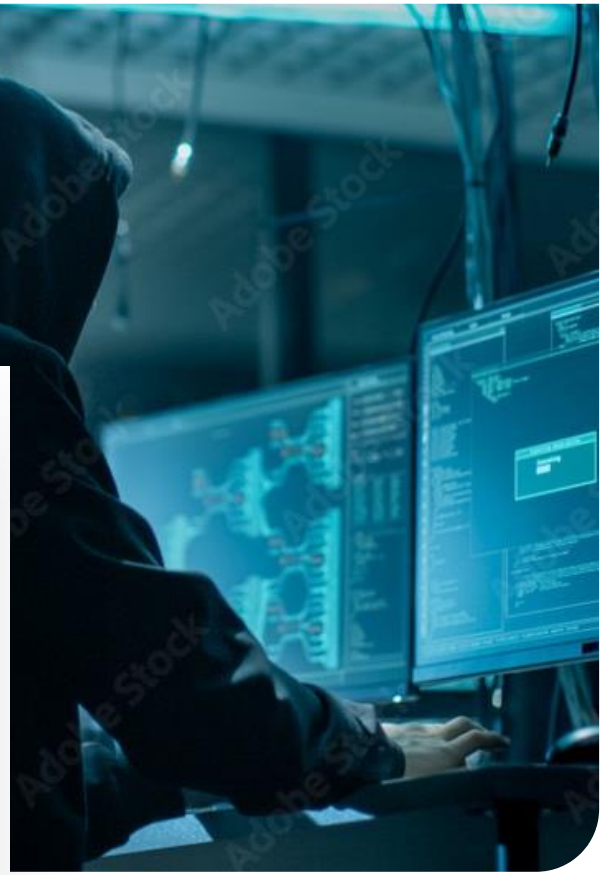
Cyberrisiken im operativen Alltag

Wo Cyberangriffe in der Disposition ansetzen

30% der Unternehmen erlitten 2023 wirtschaftlichen Schaden durch Phishing (Quelle: Bitkom).

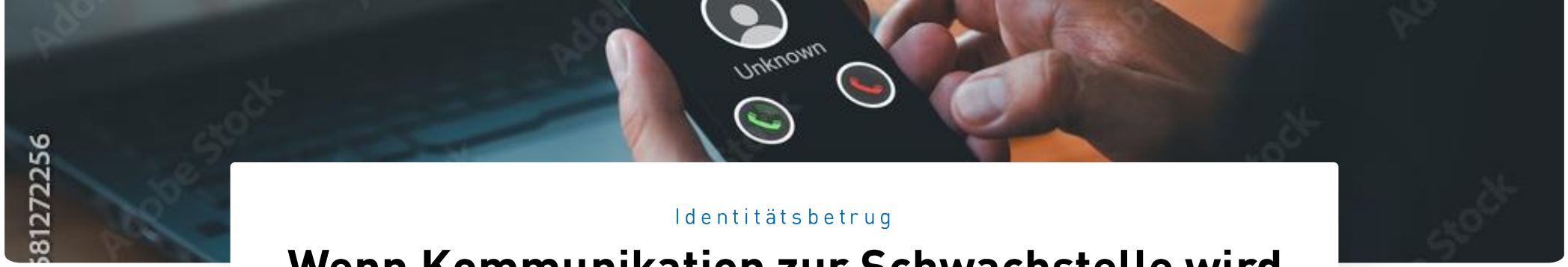
Die Transport- und Logistikbranche ist in besonderem Maße von Cyberkriminalität betroffen. Vernetzte Lager, Fahrzeuge und digitale Plattformen schaffen neue Einfallstore. Cyberkriminelle agieren zunehmend strategisch und nutzen gezielt Schwachstellen in Kommunikation, Identitätsprüfung und Dokumentenprozessen.

Typische Methoden sind Identitätsdiebstahl, manipulierte Transportdokumente und Phishing-Angriffe auf E-Mail-Postfächer oder Online-Frachtenbörsen. Täter treten dabei als vermeintlich seriöse Geschäftspartner auf und schleusen Ware in falsche Transportketten ein.



TYPISCHE ANGRIFFSMUSTER

- Identitätsdiebstahl durch gefälschte Domains und E-Mail-Adressen
- Phishing auf E-Mail-Postfächer und Frachtenbörsen
- Manipulation von Frachtbriefen und Transportdokumenten
- Zugriff über unsichere Logins ohne Zwei-Faktor-Authentifizierung



Identitätsbetrug

Wenn Kommunikation zur Schwachstelle wird

Vorsicht ist geboten, wenn unbekannte Dienstleister E-Mail oder Telefon nutzen, um Kontakt aufzunehmen. Betrüger wechseln häufig bewusst auf klassische Kommunikationswege außerhalb der Plattform. Sie geben sich als bereits existierende Unternehmen aus, die beliebte Transportplattformen nutzen, und verwenden dabei eine E-Mail-Adresse, die der des jeweiligen Unternehmens sehr ähnlich ist. Sie ändern lediglich die Reihenfolge der Buchstaben in der Mitte oder richten eine Adresse unter einer ähnlichen Domain oder sogar einer identischen Domain ein, die jedoch in einem anderen Land registriert ist.

Aus diesem Grund ist es immer sicherer, für Absprachen und die Auftragsvergabe innerhalb des Marktplatzes zu bleiben und die dort gebotenen digitalen Optionen auszuschöpfen. Dieser sollte, um wirksam vor Cyberrisiken zu schützen, verschiedene Sicherheitsmechanismen bereitstellen wie strenge Identitätsprüfungen, Betrugsüberwachung und verschlüsselte Services. Entscheidend ist jedoch das Zusammenspiel mit Kunden und Nutzer:innen. Mit ihrem verantwortungsvollen Handeln helfen sie, den Marktplatz für alle so sicher wie möglich zu machen.

Im Anschluss: Konkrete, sofort umsetzbare Maßnahmen zur Prävention.

IHR KALKÜL:
Der Spediteur, der ihnen die jeweilige Ladung im hektischen Alltag anvertraut, übersieht den Unterschied.

Identitätsbetrug vorbeugen

Zugang und Kommunikation absichern

ZUGANG ABSICHERN

Ein unzureichend geschütztes Benutzerkonto ist einer der häufigsten Einstiegspunkte für Identitätsbetrug.

Verwenden Sie ein starkes, einzigartiges Passwort und aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA). So bleibt Ihr Zugang geschützt, auch wenn Anmeldedaten kompromittiert werden.

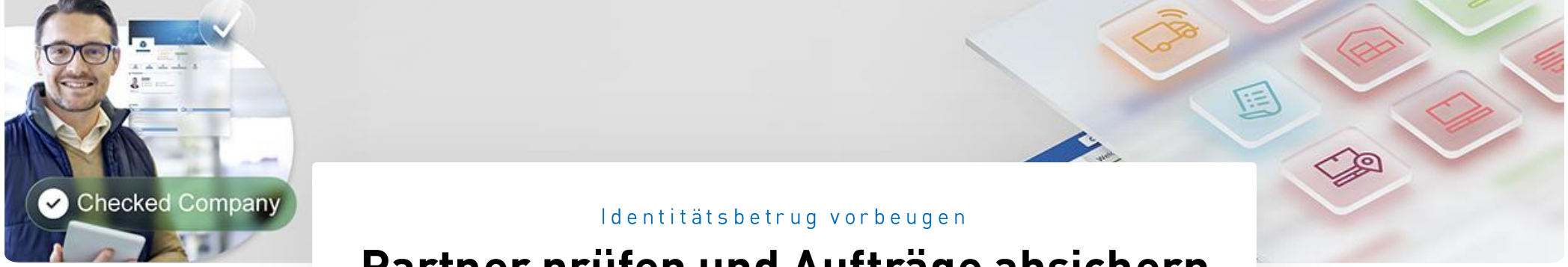
Greifen Sie ausschließlich über die offizielle Website des Marktplatzes zu und speichern Sie diese als Lesezeichen. Beenden Sie Sitzungen nach jeder Nutzung, um Missbrauch geöffneter Logins zu verhindern.

KANÄLE ABSICHERN

Identitätsbetrug beginnt häufig mit dem bewussten Wechsel auf externe Kommunikationskanäle.

Sobald Verhandlungen oder Auftragsdetails per E-Mail oder Telefon außerhalb der Plattform weitergeführt werden, steigt das Risiko deutlich. Nutzen Sie daher möglichst den internen Messenger des Marktplatzes.

Prüfen Sie eingehende E-Mails auf ungewöhnliche Absender, geringfügige Domainabweichungen oder Länderkennzeichen. Technische Absenderprüfungen (z. B. Outlook-Add-Ins) bieten zusätzlichen Schutz.



Identitätsbetrug vorbeugen

Partner prüfen und Aufträge absichern

PARTNER PRÜFEN

Begegnen sich zwei Geschäftspartner erstmals auf einer Online-Frachtenbörse, kennen sie zunächst nur die hinterlegten Profildaten. Vor einer Zusammenarbeit sollten diese sorgfältig überprüft werden. Vergleichen Sie Kundennummer und Kontaktdaten im Transportauftrag mit den Angaben im Unternehmensprofil.

Prüfen Sie bereitgestellte Dokumente wie Gemeinschaftslizenz oder OCP-/OCS-Versicherung auf Aktualität und Vollständigkeit. Kennzeichnungen wie „Checked Company“ bieten zusätzliche Orientierung, ersetzen jedoch nicht die eigene Prüfung.
Achten Sie bei externer Kontaktaufnahme besonders auf geringfügige Abweichungen in E-Mail-Adressen oder Domains. Schon kleine Unterschiede können auf einen Identitätsbetrug hinweisen.

AUFTRAG ABSICHERN

Bestätigen Sie Aufträge ausschließlich im Marktplatz, beispielsweise über den rechtsverbindlichen Transportauftrag oder die Transaktion „Geschäftsabschlüsse“. So vermeiden Sie Manipulationen oder Missverständnisse durch externe Kommunikationswege.

Fordern Sie bei sensiblen oder hochwertigen Sendungen die Live-Sendungsverfolgung an. Transparente Status- und Positionsdaten erhöhen die Sicherheit während des Transports und schaffen zusätzliche Kontrolle über den Ablauf.

Identitätsbetrug vorbeugen

Checkliste: Neuen Geschäftspartner prüfen

Kontaktdaten abgleichen

TIMOCOM-ID, Ansprechpartner und Kontaktdaten mit dem Unternehmensprofil vergleichen.

E-Mail-Adresse checken

Schreibweise der Domain mit den hinterlegten Kontaktdaten abgleichen.

Dokumente prüfen

EU-Lizenz, Versicherungen und andere Unterlagen auf Aktualität prüfen.

Business Partner Check beachten

Unternehmen mit grünem Haken (TIMOCOM Marktplatz) haben wichtige Dokumente prüfen lassen.

Bewertungen ansehen

Kommunikation, Pünktlichkeit und Umgang mit Dokumenten berücksichtigen.

Preisvorschlag im Marktplatz anfordern

So erkennen Sie, ob Ihr Gegenüber direkten Zugriff auf den Marktplatz hat.

WARUM PRÜFEN?

Risiken erkennen – sichere Auftragsbasis schaffen.

41 %

der Logistikunternehmen nutzen digitale Marktplätze (Bitkom Research – Digitalisierung der Logistik, 2022).

Wenn abgestellte LKW zum Ziel werden

LADUNGSDIEBSTAHL

Ladungen von nahezu 26.000 LKW werden in Deutschland jährlich gestohlen, das macht einen Diebstahl alle 20 Minuten, wie die Arbeitsgemeinschaft Diebstahlprävention in Güterverkehr und Logistik errechnet hat, zu der unter anderem der Bundesverband Güterkraftverkehr Logistik und Entsorgung (BGL) gehört.

Damit verursacht der Diebstahl aus LKW einen wirtschaftlichen Schaden von 1,3 Milliarden Euro pro Jahr. Zuzüglich der Kosten durch Konventionalstrafen.

Ladungsdiebstahl vorbeugen

PARKPLATZ

SICHERUNG

ROUTE & PAUSEN

SICHERE PARKPLÄTZE WÄHLEN

- nur bewachte / beleuchtete Flächen nutzen
- Stellplatz wenn möglich reservieren

ANHÄNGER SICHERN

- zusätzliche Schlösser / Plomben einsetzen
- Türsensor oder Blockade verwenden

ROUTE PLANEN

- sichere Pausen einplanen
- Routenplanungstools nutzen

Unbefugten Zugang verhindern

Sicherung des Anhängers auf dem Parkplatz

- Zusätzliche Türschlösser installieren (z. B. weitere Vorhängeschlösser, Schlossbügel oder verstärkte Scharnierschutzplatten)
- Transportplomben anbringen (aus Stahl oder elektronisch)
- GPS-Plomben nutzen (optional) (Plombe übermittelt Standortdaten des Anhängers)
- Digital Consulting Türöffnungssensor einbauen (erkennt ungeplante Türöffnungen)
- Türöffnungssensor einbauen (erkennt ungeplante Türöffnungen)
- Türblockade / mechanische Blockierung montieren (z. B. zusätzliche Verriegelungsstangen)
- Fahrzeugüberwachung aktivieren (Telematik- oder GPS-Tracking, Alert-Funktionen)

Fazit

Im Spotmarkt gehört es zum täglichen Business, kurzfristig neue Geschäftsbeziehungen zu knüpfen. Frachtenbörsen sind beliebte Plattform dafür, daher ist es nicht verwunderlich, dass Kriminelle nach Möglichkeiten suchen, sie für betrügerische Zwecke zu missbrauchen. Auftraggeber wie Auftragnehmer sollten angesichts des mit der heutigen digitalen Vernetzung verbundenen Anstiegs der Cyberkriminalität besonders wachsam sein und potenzielle Partner genau prüfen. Ist der Transportunternehmer oder aber auch der Auftraggeber wirklich der, der er vorgibt zu sein?

Moderne Online-Frachtenbörsen, wie sie TIMOCOM in seinem Road Freight Marketplace zur Verfügung stellt, unterstützen bei der Wahrung Ihrer Sicherheit auf mehrere Arten. Zum einen wird jedes Unternehmen vor Freischaltung einer Eingangsprüfung unterzogen, bestehende Kunden können ihre Dokumente und Lizenzen zudem durch einen unabhängigen Dienst prüfen lassen. Marktteilnehmer können einen Business Partner Check durchlaufen und sich so als verifiziertes Unternehmen kennzeichnen.

Und auch die Erfahrungen aus dem Netzwerk und Bewertungen lassen sich gut zur Prüfung neuer Geschäftspartner heranziehen. Das ändert jedoch nichts daran, dass jeder Geschäftspartner vom Unternehmen nochmals intern überprüft werden sollte. Denn so gut die Werkzeuge zur Nutzerverifizierung der führenden Frachtenbörsen sind, jeder einzelne muss trotzdem wachsam bleiben. Nur gemeinsam sind Plattformanbieter und Marktteilnehmer in der Lage, der steigenden Cyberkriminalität Herr zu werden.

Hier gibt es weitere Informationen, wie TIMOCOM Sicherheit auf seiner Frachtenbörse umsetzt.

Thank You

timocom.com