eye.

Cyber in der Logistik 2024


C2

Einführung

Neues Wachstum. Neue Risiken.

Cyber in der Logistik 2024

Nachhaltigkeit. Wachstum. Digitalisierung. Schlagworte, die in der Logistikbranche im Jahr 2024 fast immer genannt werden. Aber was bedeuten sie für einzelne Unternehmen - und für die Sicherheit?

Zuerst die gute Nachricht. Nach der Pandemie hat sich die Logistikbranche gut erholt und erreichte im Jahr 2020 eine Marktkapitalisierung von 9,86 Billionen Euro. Statista prognostiziert, dass die Marktkapitalisierung bis 2028 auf 13,33 Billionen Euro steigen wird.[1] Dank dessen, was Kearney als "Zwillingstransitionen" bezeichnet - die Ausrichtung von digitalen und nachhaltigen Zielen - gewinnt die nachhaltige Transformation an Fahrt.[2] Eine Reihe von Initiativen, von Automatisierung, vorausschauender Wartung, IoT-Anwendungen bis hin zu intelligenten Transportsystemen und bedarfsgesteuerter Versorgung, trägt dazu bei, die Effizienz und die Reduzierung von Verschwendung in Unternehmen in der Branche zu verbessern.

Die Kehrseite? Die gleichen Faktoren, die die Betriebsabläufe verbessern und die Beschleunigung in Richtung Nachhaltigkeit fördern, öffnen die Tür für erhöhte Sicherheitsrisiken. Im Jahr 2020 stiegen die Cyberangriffe alarmierend um bis zu 700%. Der Logistiksektor war besonders betroffen, wobei Angriffe auf die Betriebstechnologie in der Schifffahrtsindustrie im Jahr 2020 um bis zu 900% stiegen.[3]

Infolge der Zunahme der Cyberkriminalität kommen neue Vorschriften, die auf Resilienz abzielen. Gemäß NIS2 - der Netzwerk- und Informationssicherheitsrichtlinie, die im nächsten Jahr in Kraft tritt - können Unternehmensleiter persönlich haftbar gemacht werden, wenn sie keine ausreichenden Sicherheitsmaßnahmen umsetzen.

Angesichts der Zunahme der Cyberbedrohungen, NIS2 und der hohen Kosten von Angriffen selbst sollte jedes Unternehmen im Logistiksektor jetzt seine Verteidigung stärken.

1 Größe der weltweiten Logistikbranche 2018-2028 (Statista Research Department, 2023)

2 Stand der Logistik 2023: Der große Neustart (Kearney, 2023)

3 'Maritime Cyberangriffe steigen um 900%' (Maritime Professional, 2020)

Eye Security bietet Unternehmen die unverzichtbaren Instrumente für Sicherheit auf höchstem Niveau, um sicherzustellen, dass ihre Daten geschützt bleiben und ihre Infrastruktur den Vorschriften entspricht. In diesem E-Book beleuchten wir die Risiken und Herausforderungen, die spezifisch für den Logistiksektor sind. Wir erläutern NIS2 und helfen Ihnen, den Zustand der Widerstandsfähigkeit Ihres Unternehmens einzuschätzen. Cyber-Risiken mögen zunehmen, aber wir stellen uns dagegen - und gemeinsam können wir Ihr Unternehmen schützen.

Vom E-Commerce bis hin zur Cyberkriminalität

Wie Veränderungen in der Branche die Tür öffnen

COVID mag die Grenzen nicht mehr schließen, aber die langfristigen Auswirkungen beeinflussen immer noch die Logistikbranche. Der rasant steigende Erfolg des E-Commerce mit einfachen Rückgabe- und Erstattungsrichtlinien hat eine entsprechende Nachfrage nach flexiblen Lieferdiensten ausgelöst. Das schnelle Wachstum erhöht den Druck auf nachhaltigere Transportlösungen.

Das Ergebnis? Schnelle Innovation und Digitalisierung in der gesamten Branche, angetrieben von neuen Technologien. Immer mehr neue Akteure und Herausforderer mit flexiblen und datengesteuerten Angeboten. Eine zunehmende digitale Präsenz, selbst wenn der Fokus auf ökologischen Zielen liegt. Und steigende Cyberkriminalität.

Digitalisierung, das zweischneidige Schwert

Durch maschinengetriebene Prozessänderungen hat sich die heutige Lieferkette transformiert. Transport- und Logistikunternehmen verwenden jetzt Edge- und IoT-Technologien, um den Standort von Waren zu verfolgen, die Temperatur zu überwachen und den Lagerbestand zu prüfen. Mit so vielen Echtzeitdaten können Unternehmen informierte Entscheidungen treffen, um Verderb zu reduzieren, Abfall zu minimieren und Angebot und Nachfrage zu optimieren.

Diese Verbesserungen passen gut zu den Zielen der Nachhaltigkeit - scheinbar eine Win-Win-Situation.

Bis 2025 prognostiziert das Weltwirtschaftsforum, dass die Digitalisierung in der Logistikindustrie einen Wert von bis zu 1,5 Billionen US-Dollar freisetzen könnte.[4]

Aber es gibt auch eine Kehrseite.

Diese Fortschritte erfordern, dass Unternehmen große Mengen an Daten in der Cloud speichern. Die Automatisierung in der gesamten Lieferkette bedeutet, dass die Abläufe auf unsichtbare, komplexe Weise miteinander verbunden sind. Die riesigen Datenmengen, die durch diese Prozesse erzeugt werden, können nur von KI analysiert werden.

In diesem Wirrwarr von Anbietern und undurchsichtigen Abläufen ist es schwieriger - und notwendiger - denn je, einen ganzheitlichen Überblick zu behalten.

4 Digitale Transformation der Industrien (Weltwirtschaftsforum, 2016)

Cyber-Risiken sind real und nehmen zu

Als eine der profitabelsten Branchen war die Logistik schon lange ein Ziel organisierter Cyberkriminalität. Und je mehr sie sich auf digitale Infrastruktur verlässt, desto anfälliger wird sie für Angriffe.

Mit wachsenden, großen Datensätzen aus dem Internet der Dinge (IoT) haben Angreifer eine potenziell verfügbare Datenquelle, die sie verkaufen oder ausnutzen können. Und genauso wie KI und Automatisierung Logistikunternehmen dabei helfen, effizienter zu sein, nutzen Cyberkriminelle diese Werkzeuge für Angriffe, die immer schwerer zu erkennen und zu bewältigen sind.

Ein hoher Anteil von Phishing-Angriffen richtet sich gegen Logistikunternehmen. Die stark vernetzte Natur der Branche macht sie besonders anfällig für Kriminelle, die sich als legitime Fachleute ausgeben und Zugang zu Passwörtern und Daten erlangen.

Wenn ein weniger geschützter Drittanbieter in der Lieferkette gehackt wird, können selbst Unternehmen mit einem hohen Maß an Cyberverteidigung gefährdet sein. Im Jahr 2021 wurde ein Logistikunternehmen, das in die COVID-Impfkette involviert war, auf diese Weise kompromittiert.[5]

Ransomware - wenn Hacker in die IT-Infrastruktur eines Unternehmens eindringen und Dateien oder ganze Systeme verschlüsseln und sie erst dann wieder zugänglich machen, wenn das Unternehmen ein Lösegeld zahlt - ist eine der am schnellsten wachsenden Bedrohungen. Im Jahr 2020 stiegen die gemeldeten Ransomware-Vorfälle um 700%, wobei Transport- und Logistikunternehmen ein Hauptziel waren.[6] Laut Angaben des Information Commissioner's Office (ICO) des Vereinigten Königreichs sind mittlerweile 1 von 3 Cyberverstößen Ransomware-Angriffe.[7] Angesichts der Tatsache, dass nicht alle solchen Angriffe gemeldet werden, könnte die Zahl sogar höher sein.

Solche Angriffe sind verheerend für jedes Unternehmen, aber in der Logistik, wo die Kontinuität von entscheidender Bedeutung ist, erholen sich einige Unternehmen nie mehr. Erst in diesem Monat meldete das große britische Unternehmen KNP Logistics Insolvenz an und führte einen Ransomware-Angriff als Ursache an.[8]

1 von 5 Unternehmen in der Logistik- und Transportbranche wird voraussichtlich einen Cybervorfall erleben

4,21 Millionen Euro ist der weltweite durchschnittliche Kostenpunkt eines Datenschutzverstoßes im Jahr 2023

~ 5% der neuen Kunden bei Eye Security waren bereits vor der Onboarding-Phase gehackt worden

Quelle: 'Kosten eines Datenverstoß-Berichts' (IBM, 2023)

5 'Wie eine E-Mail ein Logistikunternehmen zum Absturz brachte' (Darktrace, 2021)

6 Halbjahresbericht zur Bedrohungslage (Bitdefender, 2020)

7 Trends bei Datenschutzverstößen (Information Commissioner's Office, 2022)

8 'Britisches Logistikunternehmen gibt Ransomware die Schuld an Insolvenz und 730 Entlassungen' (The Record, 2023)

Die Wahrscheinlichkeit der Bedrohung, das Potenzial für Verluste in Millionenhöhe und die Auswirkungen auf den Ruf, die Kundenzufriedenheit und den Wettbewerbsvorteil machen es dringender denn je, dass Logistik- und Transportunternehmen ihre IT- und OT-Systeme schützen.

Was Logistikunternehmen sehen...		Was Cyberkriminelle sehen...
Rasantes Branchenwachstum und Rentabilität	>	Mehr zu gewinnen durch potenzielle Angriffe
Mehr Daten über Waren und Dienstleistungen	>	Mehr Daten zum Abgreifen und Verkaufen
Mehr Datenaustausch in Partnerschaften	>	Größere Chance, Schwachstellen zu finden
Mehr Remote-Arbeit, die den E-Commerce antreibt	>	Mehr ungesicherte Geräte zum Hacken
Wachsende Mitarbeiterzahlen für das Businesswachstum	>	Mehr ungeschulte Ziele für Phishing
Mehr Möglichkeiten für End-to-End-Automatisierung	>	Eine größere Angriffsfläche

Ihre Sicherheitsmaßnahmen stetig hinterfragen

Well die Auswirkungen eines Angriffs fast immer größer sind als erwartet, zahlt sich ein Sicherheitsupgrade aus. Durch die Verhinderung von Angriffen von vornherein können Organisationen bis zu 1,4 Millionen US-Dollar sparen.[9]

- Sind Ihre Mitarbeiter geschult, um Phishing-E-Mails zu erkennen?
- Sind Ihre HR-Anmeldungs- und Austrittsprozesse sicher?
- Sind Ihre IoT-Endpunkte und Netzwerke segmentiert?
- Sind Ihre Verschlüsselungs- und Authentifizierungsmethoden robust?
- Wie sicher sind Ihre Verbindungen zu Drittanbietern?
- Halten Sie sich auf dem Laufenden gegenüber neuen Angriffsformen?

9 'Studie: Die Verhinderung von Cyberangriffs-Penetration kann Unternehmen bis zu 1,4 Millionen US-Dollar pro Vorfall sparen' (Businesswire, 2020)

Ein Fall von Ransomware, gelöst

Wie Eye und ein belgisches Logistikunternehmen mit einem Cyberangriff umgingen

Mit über 350 Fahrzeugen und mehr als 700 Mitarbeitern ist dieses familiengeführte Logistikunternehmen seit über 50 Jahren im Geschäft und hat viele Niederlassungen in Belgien und noch mehr in ganz Europa.

Wie viele Unternehmen ist es auf seine IT-Infrastruktur angewiesen, die fast vollständig intern entwickelt wurde. An einem Samstagmorgen begannen merkwürdige Dinge mit den Servern des Unternehmens zu geschehen. Sie waren Opfer eines Cyberangriffs in Form von Ransomware geworden - bei weitem die größte Cyberbedrohung für Logistikunternehmen weltweit.

Sie wandten sich an Eye Security um Hilfe. Innerhalb weniger Stunden waren zwei Incident Responder vor Ort, die Systeme neu aufbauten und Sicherheitssoftware implementierten, bevor das Geschäft wieder online ging.

Die Cyberexperten von Eye Security stellten fest, dass der frühere externe IT-Partner des Unternehmens eine falsche Konfiguration in seinen Firewalls vorgenommen hatte, die den Angriff ermöglichte.

Die ersten Systeme waren innerhalb von Tagen wieder online, aber "die über 150 Verbindungen zu Kunden, Lieferanten und Partnern waren immer noch für die internen Systeme gesperrt, ebenso wie das Internet", erinnert sich der CEO.

Das Unternehmen hat nach und nach alle externen Standorte wieder verbunden, während es Sicherheitsmaßnahmen überprüfte und ergriff.

Eye konnte das Unternehmen beruhigen, dass die Angreifer keine Daten erfasst hatten, um sie weiterzuverkaufen. Der Angriff kostete das Unternehmen dennoch eine beeindruckende Summe von 1,3 Millionen Euro (von der zum Glück ein Großteil durch die Cyber-Versicherung abgedeckt wurde). Es dauerte fast ein Jahr, bis das Unternehmen wieder voll einsatzfähig war - jetzt mit einer gestärkten IT-Infrastruktur.

●●●

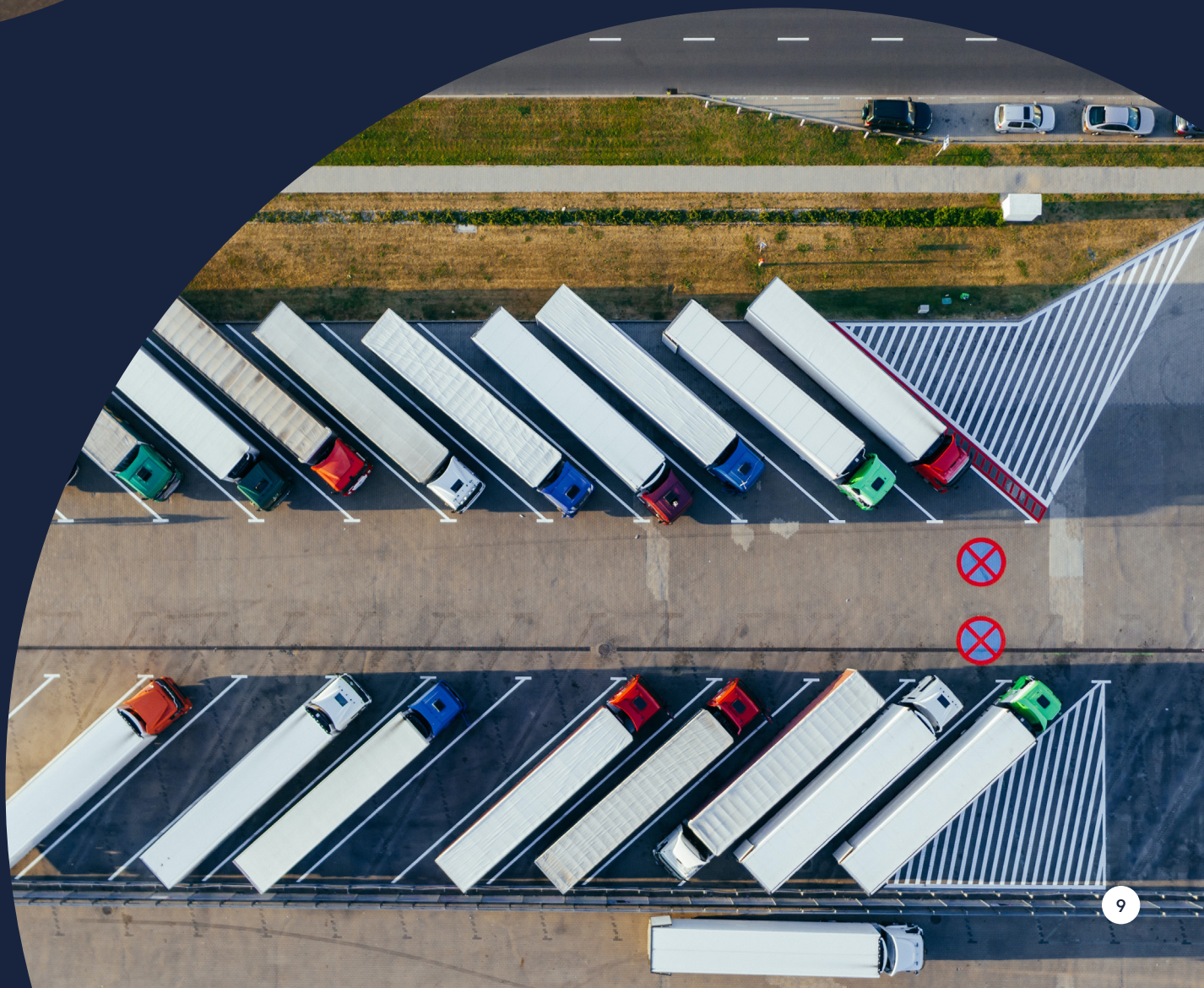
"Cybersecurity ist nie abgeschlossen... Es wird immer ein fortlaufender Prozess sein."

Die wichtigste Lektion, so der CEO, ist, dass Cybersecurity nie abgeschlossen ist. “Heute bleiben wir ständig wachsam. Ist die gesamte Infrastruktur sicher? Sind die Mitarbeiter geschult, um Phishing zu erkennen? Haben wir wichtige Patches übersehen? Es ist ein fortlaufender Prozess.”

Sie erhielten zusätzliche Ratschläge von Eye Security und profitierten von deren Wissen. Wie Anne Masson, CEO von Eye Security Belgium, sagt: “Wir sind in der Lage, große Herausforderungen mit persönlicher Aufmerksamkeit und zur vollen Zufriedenheit unserer Kunden zu lösen [...] Wir kennen den Markt in- und auswendig. Wir beraten Unternehmen bei Prozessverbesserungen, um ihre Infrastruktur sicherer zu machen, und welche Lösungen sie in Zukunft einsetzen können, um ausreichend geschützt zu sein.”

In der Zwischenzeit hat Eye Security seine Cyber Guard-Lösung in den Systemen seiner Kunden eingeführt und dabei auf Managed Extended Detection & Response-Technologie (mXDR) in Kombination mit Cloud-Erkennung gesetzt.

“Dadurch wird unser Kunde mit unserem 24/7 Security Operations Centre (SOC) verbunden und das ermöglicht es uns, sofort zu intervenieren, sollte ein weiterer Angriff auftreten”, sagt Masson.



Den Aufbau von Cyber-Resilienz mit NIS2

Warum die Einhaltung wichtiger ist denn je

NIS2, die neue Version der Richtlinie für Netzwerk- und Informationssicherheit, zielt darauf ab, das allgemeine Niveau der Cybersicherheit in der EU zu stärken. Die Richtlinie ist ein Meilenstein in der Cyberabwehr - und eine Herausforderung für die meisten kleinen und mittleren Unternehmen.

Kritische Infrastruktur - unsere Stromversorgung, Wasser, das Gesundheitssystem, die Art und Weise, wie wir uns von einem Ort zum anderen bewegen - ist das Hauptziel für böswillige Angriffe. Es ist nicht schwer zu verstehen, warum: Ein groß angelegter Angriff auf Transportsysteme kann eine Stadt lahmlegen.

NIS2 - ein wenig wie die DSGVO, aber für die Cybersicherheit - ist notwendig zum Schutz kritischer Infrastruktur. Die Richtlinien, die bis Oktober 2024 von allen EU-Mitgliedstaaten übernommen werden müssen, erfordern von Unternehmen eine strengere Cybersicherheitsverteidigung und Berichterstattung als das frühere NIS1.

Wie sein Vorgänger sollte NIS2 als Leitfaden betrachtet werden, wobei die Einhaltung das Minimum darstellt. Unternehmen sollten proaktiv sein, um ihre sensiblen Daten und kritischen Systeme zu schützen, denn die Auswirkungen eines Cyberangriffs erstrecken sich weit über die finanziellen Aspekte hinaus.

In der Logistik erodiert eine längere Ausfallzeit die Kundenzufriedenheit und das Vertrauen, stört die Geschäftskontinuität, verringert den Wettbewerbsvorteil und behindert das Wachstum. Im heutigen, wachsenden Wirtschaftsumfeld - mit neuen Wettbewerbern an jeder Ecke - können sich nur wenige Unternehmen leisten, ihren Vorsprung zu verlieren.

●●●

‘Indem Unternehmen jetzt auf NIS2 reagieren, haben sie die Möglichkeit, ihre Betriebsabläufe zu bewerten, ein besseres Verständnis für ihre Systeme und Integrationen zu erhalten und etwaige Schwachstellen zu stärken.’

Was ist neu in NIS2

Umfassender und strenger

NIS2 erweitert den Anwendungsbereich von NIS1 von 7 auf 18 Branchen (einschließlich Transport, Post- und Kurierdienste, Lebensmittelproduktion und Fertigung) und führt gleichzeitig strengere Cybersicherheitsstandards und genaue Meldepflichten für Zwischenfälle ein.

Mehr Auswirkungen auf die Logistik

In der Logistik sind IT und OT stärker miteinander verflochten. Um den neuen Standards gerecht zu werden, benötigen Unternehmen in diesem Sektor einen ganzheitlichen Überblick über Abhängigkeiten und Schwachstellen. Sie müssen Risikobereiche überwachen und Maßnahmen ergreifen, um auf Zwischenfälle zu reagieren.

Erhöhte persönliche Haftung

Die Nichtbefolgung von NIS2 zieht schwere Strafen nach sich. Ab 2024 können Unternehmensleiter persönlich für die Nichtumsetzung ausreichender Sicherheitsmaßnahmen haftbar gemacht werden, mit Geldbußen von bis zu 10 Millionen Euro.

eye.

Wie Eye Security helfen kann

Die meisten kleinen und mittleren Unternehmen verfügen nicht über die Ressourcen, um die Anforderungen von NIS2 zu verstehen und diese ganzheitlich in ihren Betrieb umzusetzen.

Wir können unsere Expertise für Sie einsetzen, angefangen bei der anfänglichen Bewertung von Cyber-Risiken bis hin zur Einführung eines robusten Cyber-Resilienz-Frameworks.

Wir betrachten NIS2 als eine Chance, nicht als Hindernis. Durch die Einführung von Maßnahmen zur Überwachung von Cyberangriffen, wie Managed XDR, können wir Ihnen helfen, solche Angriffe von vornherein zu vermeiden.

Statt mit den Folgen eines Angriffs umzugehen, können Sie sich auf Wachstumschancen konzentrieren.

Interview

F&A mit Danny Zeegers von QFirst

Welche Rolle spielen Sie in der Cybersicherheit?

Ich bin Cybersicherheitsbeauftragter bei QFirst, einem Unternehmen, das Unternehmen auf Zertifizierung vorbereitet - insbesondere im Zusammenhang mit der neuen europäischen NIS2-Gesetzgebung. Konkret überbrücke ich die Lücke zwischen der theoretischen und der praktischen Ebene und helfe den Menschen, Vorschriften in ihre tatsächlichen Betriebsabläufe zu übersetzen.

Wie hat sich die Cybersicherheit in den letzten Jahren verändert - und wohin geht sie?

Jedes IT-Unternehmen glaubt, dass es gute Arbeit leistet - sie haben ihre Firewalls gestärkt, ihre Verfahren und Prozesse verbessert. Die meisten haben bereits ISO27k (internationale Leitlinien zur Risikoverwaltung von Daten) eingerichtet oder sind dabei, es einzurichten.

Die Hauptaufgabe, vor der Unternehmen in den nächsten 3-5 Jahren stehen, ist die Umstellung auf einen Zero-Trust-Ansatz (bei dem jeder bei jeder Anforderung überprüft wird, auch wenn sie zuvor authentifiziert wurde). Das nationale Recht wird dies absolut wasserdicht verlangen. Und wenn nicht, wird eine ständige Überwachung durch ein Unternehmen wie Eye Security erforderlich sein.

Wie bereiten Sie Unternehmen auf die Zertifizierung vor?

Wir haben einen 5-Stufen-Prozess. Der erste Schritt besteht darin, sie zu überprüfen und zu sehen, was sie bereits in Bezug auf Cybersicherheit tun. Dann testen wir es - einen Black Hat Penetration Test auf allen Ebenen. Dann erstellen wir einen Beratungsbericht, der zur Entwicklung eines Lösungsfahrplans verwendet wird. Schließlich betrachten wir die laufende Überwachung und Berichterstattung.

Mit NIS2 hat das Unternehmen nur 72 Stunden Zeit, um einen Vorfall zu melden und zu registrieren, sobald ein Vorfall auftritt. Sie müssen ihn melden, damit andere Unternehmen wissen, dass es eine Schwachstelle gibt, und Maßnahmen ergreifen können.

Was ist die größte Herausforderung für die Cybersicherheit in der Logistik?

Logistikunternehmen haben viele Abteilungen und bewegliche Teile - sie sind wie ein Rubik's Zauberwürfel. Und jede Abteilung konzentriert sich darauf, was gerade erledigt werden muss. Die kontinuierliche Überwachung von Endpunkten steht nicht an erster Stelle. Daher ist die Überwachung und die Schaffung eines Überblicks eine große Herausforderung.

Außerdem müssen Logistikunternehmen ab 2024 sicherstellen, dass alle ihre Lieferketten auch NIS2-zertifiziert sind. Dazu gehören alle, die ihnen APIs bereitstellen - Fahrer und jeder, der sich mit den Anwendungen und Diensten der ICT-Infrastruktur verbindet. Das ist eine riesige Herausforderung. Aber es kann ein Rahmen entwickelt werden, um ihnen dies zu erleichtern.

Haben Sie Ratschläge für Unternehmen, die Cybersicherheits-Upgrades in Erwägung ziehen?

Lassen Sie sich nicht von Lösungen überwältigen (oder Ihr Budget). Konzentrieren Sie sich darauf, von Anfang an die richtigen Lösungen einzusetzen. Kennen Sie nicht nur die Vorschriften, sondern verstehen Sie auch, wie Sie sie in der Praxis für Ihr Unternehmen umsetzen können. Und stellen Sie sich selbst ein zentrales ISMS NIS2-Framework zur Verfügung, in dem Sie eine Verbindung zwischen Vorfallmanagement, Risikoanalyse, digitalen Vermögenswerten und Abteilungen haben.

Wo wir angefangen haben, wohin wir gehen...
...und wo Ihr Unternehmen hineinpasst

Eye Security wurde 2020 gegründet, um Cybersicherheit auf nationalem Geheimdienstniveau für Unternehmen jeder Größe verfügbar zu machen. Nur drei Jahre später sind wir stolz darauf, einen Aufsichtsrat mit fünf ehemaligen Experten für nationale Sicherheit, ein Team von 80 qualifizierten Mitarbeitern (und wachsend) und Büros in den Niederlanden, Belgien und Deutschland zu haben.

Bei Eye Security verstehen wir Menschen, die Unternehmen aufbauen. Wir wissen, wie viele Jahre Arbeit es kostet, eine Idee in ein erfolgreiches Unternehmen zu verwandeln. Wir wissen, dass, wenn eine Organisation Opfer eines Angriffs wird, mehr als nur finanzieller und Rufschaden auf dem Spiel stehen - Existenzen sind gefährdet.

Unsere Kunden vertrauen uns als ihrem Sicherheitspartner. Wir haben dieses Vertrauen gewonnen, indem wir das Wissen unserer Experten Unternehmen jeder Größe und zu jeder Zeit zur Verfügung gestellt haben. Unsere Arbeit wird erst dann abgeschlossen sein, wenn jedes Unternehmen in Europa den Schutz hat, den es benötigt.

"Wir verkaufen keine Technologie oder Software. Wir verkaufen die Sicherheit von Expertenwissen."

Unsere Produkte

Das Sicherheitsniveau führender Großunternehmen - erschwinglich für alle Unternehmen

Hunderte von Unternehmen verlassen sich auf Eye Security - angefangen bei einem der größten Carrier in den Niederlanden bis hin zu einem Hersteller für einige der bekanntesten europäischen Lebensmittelmarken.

Entwickelt von Sicherheitsexperten bietet unser auf Abonnement basierender Service umfassenden Schutz und Unterstützung, ohne die oft mit Cyberschutz gebündelten unnötigen Produkte.

Unser All-in-1-Paket bietet Cybersicherheitsüberwachung und -erkennung, 24/7-Cyberreaktion im Falle eines Vorfalls und neuerdings auch eine Cyber-Versicherung. Ein schlankes Paket der wirksamsten Sicherheitsmaßnahmen, es ist einfach, konform, robust - und das erste seiner Art, das einfach verfügbar gemacht wurde.

●●●

“Eye Security verfügt über das Fachwissen, das wir benötigen, um unsere Systeme zu schützen, weil sie ständig an Cyberkriminalität und -sicherheit arbeiten. Dies ermöglicht es uns, uns auf das zu konzentrieren, was wir gut können: den Tiefseecontainertransport durch Westeuropa.”

Gertjan van der Most,
Gründer von Van der Most Transport

Was ist enthalten - und warum es wichtig ist

1

Managed XDR

Unser Service für Managed Extended Detection and Response (XDR) bietet rund um die Uhr Überwachung und Erkennung abnormalen Verhaltens durch ein Team von menschlichen Cybersicherheitsexperten, um potenzielle Bedrohungen schnell zu identifizieren und zu entschärfen.

Cyberkriminelle operieren rund um die Uhr, 7 Tage die Woche, und nur 20% der Bedrohungen können allein durch Technologie bewältigt werden - 80% benötigen menschliches Urteilsvermögen und Eingreifen.

2

Cyber Awareness Training

Wir bieten interaktive Schulungsprogramme, um Ihre Mitarbeiter über bewährte Verfahren zu informieren und sie zu befähigen, Cyber-Risiken wie Phishing-E-Mails effektiv zu erkennen und darauf zu reagieren.

Phishing-Angriffe nehmen in Volumen und Raffinesse zu - es bedarf nur eines nachlässigen oder unwissenden Mitarbeiters, um eine Angriffskette freizusetzen, die Ihr Unternehmen Millionen kosten könnte.

3

Incident Response

Unser Incident-Response-Team ist rund um die Uhr persönlich für Sie da, falls ein Cyber-Vorfall eintritt, um den Schaden zu begrenzen und Ihr Geschäft so schnell wie möglich wieder in Gang zu bringen.

Selbst ein Tag Ausfallzeit kann Hunderttausende Euro kosten. In einem solchen Fall wollen Sie es mit erfahrenen Menschen zu tun haben, nicht mit einem Ticketsystem, einer E-Mail-Anweisung oder einem globalen Callcenter.

4

Intelligenz

Durch unser Kundenportal bieten wir Ihnen klare und spezifische Empfehlungen, wie Sie Ihre Cybersicherheitsmaßnahmen stärken können.

Diese Mehrwert-Intelligenz *nimmt das Rätselraten darüber, was getan werden muss, um Ihre Cyber-Resilienz zu verbessern - und möglicherweise Ihre Versicherungsprämien zu reduzieren - ohne den Aufwand von Beratungsstunden und zusätzlichen Kosten.*

5

Bedrohungssuche

Unser Intelligenzteam ist ständig auf der Suche nach neuen Bedrohungen. Wenn wir sie identifizieren, arbeiten wir mit unseren Kunden zusammen, um sicherzustellen, dass sie sicher sind.

Wir suchen proaktiv nach jeder Gelegenheit, um Ihre Systeme widerstandsfähig zu halten und den Cyberkriminellen einen Schritt voraus zu sein.

6

Cyber-Versicherung

Wir bieten einen schnellen und unkomplizierten Prozess zum Kauf oder zur Verlängerung der Cyber-Versicherung an, damit Sie die finanziellen Auswirkungen eines Cyber-Vorfalls mildern können.

1 von 5 kleinen und mittleren Unternehmen wird gehackt, was im Durchschnitt 400.000 Euro kostet. Die Cyber-Versicherung ist entscheidend, um Ihr Unternehmen vor den potenziell hohen Kosten von Angriffen zu schützen.

‘Jedes Unternehmen, unabhängig von seiner Größe, verdient Zugang zu hochwertiger Cybersicherheit.’

– Job Kuijpers,
CEO and Founder
of Eye Security

Bereiten Sie sich heute auf die Anforderungen von morgen vor.

Wir wissen, dass unsere Kunden im Transport- und Logistikbereich einer Vielzahl von Risiken ausgesetzt sind. Für diese Kunden bieten wir ein maßgeschneidertes Angebot für jede Risikokategorie an. Selbst wenn große Versicherer ihre Transport- und Logistikversicherungspolicen zurückfahren, sind wir in der Lage, eine vollwertige Lösung durch Eye Underwriting anzubieten, die die Komplexität der Beziehungen zu Drittanbietern in diesem Sektor berücksichtigt.

Besuchen Sie unsere Website, um einen Termin mit einem unserer Experten zu vereinbaren. Wir werden Ihnen helfen, Ihre Bedrohungslage zu verstehen, Ihre Infrastruktur zu stärken und die NIS2-Anforderungen zu erfüllen.

Eye Security macht Cybersicherheit einfach.

www.eye.security


CẢNG CÔNG-TEN-NƠ QUỐC TẾ HẢI PHÒNG
MAERSK SARAT

Möchten Sie weitere Informationen?

Kontaktieren Sie uns für ein unverbindliches Gespräch mit einem Cybersicherheitsspezialisten von Eye Security. Schließlich ist es jetzt wichtiger denn je, die Sicherheit Ihres Unternehmens zu gewährleisten.

Besuchen Sie www.eye.security oder kontaktieren Sie uns unter +49 211 8199 5603