eraneos

E-Paper

Cyber Security bei Verkehrsbetrieben erhöhen

Wo fährt die Gefahr mit?

Einleitung

Cyber-Attacken beziehungsweise Vorfälle, die böswillige und kriminelle Aktivitäten im digitalen Raum beschreiben, nehmen laufend zu. Die Gründe für die Zunahme sind unterschiedlicher Natur. So arbeitet aufgrund der Covid-19-Pandemie beispielsweise eine Vielzahl von Arbeitnehmenden neu von zu Hause aus. Dies eröffnet Hackern eine Bandbreite zusätzlicher Möglichkeiten für ihre schädlichen Absichten. Auch die zunehmende Vernetzung von Geräten bietet eine immer grösser werdende Angriffsfläche für Cyber-Attacken. Ob Phishing, Ransomware oder DoS, niemand ist vor Cyber-Attacken geschützt – auch nicht die Verkehrsbetriebe.

In dieser Publikation zeigen wir nicht nur mögliche Gefahren für Verkehrsbetriebe auf, sondern wir erklären auch, wie mit einfachen Mitteln bereits viel zum Schutz vor solchen Cyber-Attacken geschehen kann.

Michael Flückiger
Consultant, Cyber Security & Privacy

Axel Sitt
Manager, Cyber Security & Privacy

Fabian Zumkehr
Consultant, Smart Mobility

Cyber Security betrifft auch Verkehrsbetriebe

Waren lange Zeit hauptsächlich renommierte Grossunternehmen oder Unternehmen in spezifischen Branchen im Fokus von Cyber-Angriffen, änderte sich dies in den letzten Jahren drastisch. Um ihre Dienstleistung effizient und den modernen Nutzeranforderungen entsprechend anbieten zu können, treiben die Verkehrsbetriebe die Digitalisierung voran. Neben den Vorteilen macht dies die Betriebe aber auch abhängiger von ihren digitalen Infrastrukturen, wodurch die Cyber Security zu einem kritischen Erfolgsfaktor wird. Die nachfolgenden Schlagzeilen aus der Presse machen deutlich, dass heutzutage durchaus auch Verkehrs- und Bahnbetriebe sowie Fahrzeughersteller ein attraktives Ziel für Kriminelle aus dem digitalen Raum darstellen.

Der Fahrzeugbauer Aebi Schmidt ist Anfang 2020 Leidtragender einer Cyber-Attacke geworden[1]). Das internationale Netzwerk sowie der digitale Nachrichten-Versand waren betroffen und es dauerte über zwei Wochen, bis der Versand sowie der Empfang von E-Mails wieder funktionierten. Die operativen Systeme blieben vom Angriff verschont.

Im Bahnbereich hat es den renommierten Hersteller von Schienenfahrzeugen, die Stadler Rail, getroffen. Nach einem Sicherheitsvorfall, der Anfang Mai 2020 entdeckt wurde, kam man einer Forderung nach Lösegeld nicht nach, woraufhin die Angreifer entwendete Dokumente mit firmeninternen Informationen an die Öffentlichkeit brachten[2]).

Auch die Auto AG Group aus Rothenburg wurde Anfang April 2019 Opfer einer Cyber-Attacke[3]). Der mutmassliche Ransomware-Angriff hatte zwar keine direkten Auswirkungen auf die Fahrgäste oder die eingesetzten Fahrzeuge, jedoch konnten Bestellungen über mehrere Tage nur manuell abgearbeitet werden.

Ransomware

Ransomware ist eine sich ständig weiterentwickelnde Form von Malware, die darauf ausgelegt ist, Dateien auf einem Gerät zu verschlüsseln, wodurch alle Dateien und die Systeme, die auf ihnen basieren, unbrauchbar werden. Böswillige Akteure fordern dann Lösegeld im Austausch für die Entschlüsselung.

Mythen zum Thema Ransomware:

- „Wir sind als Ziel nicht attraktiv genug."
- „Das wird schon nicht so schlimm."
- „Da reicht ein zusätzliches Back-up."

1 https://www.inside-it.ch/de/post/wie-lief-der-hack-von-aebi-schmidt-ab-20190514

2 https://www.nzz.ch/wirtschaft/hacker-stellen-stadler-rail-ein-ultimatum-ld.1558845?reduced=true

3 https://www.luzerner-zeitung.ch/wirtschaft/auto-ag-faehrt-systeme-nach-hackerattacke-wieder-hoch-ld.1148569

Einfache Strukturen erhöhen die Angriffs-Risiken

Die Beispiele zeigen, dass auch Verkehrsbetriebe nicht vor Cyber-Attacken gefeit sind. Tatsächlich können solche Betriebe sogar ein äusserst interessantes Ziel für Hacker darstellen. Verkehrsbetriebe weisen im Grundsatz eine vergleichbare Struktur wie ein Schweizer KMU aus anderen Branchen auf. Aus unserer Erfahrung sind nachfolgende Aspekte gewichtige Gründe, warum solche Unternehmen zu Angriffszielen werden können:

- Die IT-Abteilung umfasst wenig Personal. Die verfügbaren Ressourcen reichen oftmals nicht aus, um sich vertieft mit Cyber Security auseinanderzusetzen.
- Das vorhandene Know-how im Bereich Cyber Security ist unternehmensweit begrenzt.
- Die meisten eingesetzten Informatikmittel werden zwar mit Schutzsoftware betrieben und es existieren zweckmässige Schutzmassnahmen, es fehlt aber an einer unternehmensweiten Sicherheitskultur und einem übergreifenden Konzept für Cyber Security.
- Es fehlt grösstenteils an Bewusstsein für die Cyber Security-Thematik seitens der Mitarbeitenden. Die meisten sind sich ihrer wichtigen Rolle als „First-Line of Defense" nicht bewusst.

Heutzutage ist es für einen Angreifer vergleichsweise einfach abzuschätzen, ob sich eine Cyber-Attacke lohnt, beziehungsweise, ob die Sicherheitslage einer Unternehmung einen attraktiven Angriff zulässt. Es stehen eine Vielzahl an Tools zur Verfügung, mit denen potenzielle Opfer mit geringem Aufwand ausgekundschaftet werden können. Die Mehrheit der Angreifer aus dem digitalen Raum ist auf der Suche nach einfachen Wegen und offensichtlichen Lücken. Ihr Antrieb ist rein ökonomischer Natur, sie streben nach dem bestmöglichen Return on Investment. Die oben aufgeführten Merkmale sind alles Indikatoren, die die Sicherheitslage einer Unternehmung für Angreifer attraktiv machen. Die Wahrscheinlichkeit, dass ein Verkehrsunternehmen Opfer eines Angriffs mit einem APT wird, kann als gering eingeschätzt werden. Cyber-Attacken, die sogenannte „0-Day-Schwachstellen" ausnutzen oder nach dem Prinzip eines „Wasserstellen-Angriffs" funktionieren, sind da schon deutlich wahrscheinlicher. Zu den prominentesten und am weitesten verbreiteten Angriffsmustern gehört das „Phishing", das „Spear-Phising" und das „Whale-Phising". Angriffe dieser Art führten bei den KMU aus verschiedensten Branchen bereits zu Verlusten in Millionenhöhe. Getrieben wird diese Entwicklung mitunter auch durch die Tatsache, dass für Angriffe immer weniger Know-how notwendig ist. Im Darknet existieren Märkte, wo für wenig Geld die unterschiedlichsten Arten von Angriffsmethoden als vorgefertigte Pakete feilgeboten werden. Exemplarisch dafür ist die nachfolgende Auflistung von solchen Angeboten inklusive Preisangabe aus dem Darknet aus dem Jahr 2020.

Advanced Persistent Threat (APT)

Eine fortgeschrittene, anhaltende Bedrohung ist ein verdeckter Cyberangriff auf ein Computernetzwerk, bei dem der Angreifer unbefugten Zugriff auf das an-visierte Netzwerk erlangt, aufrechterhält und dabei für einen erheblichen Zeitraum unentdeckt bleibt

Zero-Day (0-Day)

Ein Zero-Day-Exploit ist ein Cyberangriff, der am selben Tag stattfindet, an dem eine Schwachstelle in einer Software entdeckt wird. Zu diesem Zeitpunkt wird die Schwachstelle ausgenutzt, bevor ein Fix vom Hersteller verfügbar ist.

Wasserstellen-Angriff

Eine bei Benutzern beliebte und oft besuchte Webseite wird kompromittiert und für die Auslieferung von Malware genutzt. Ahnungslose Besucher erhalten darüber Malware auf ihr Endgerät.

Phishing

Angelehnt ans Angeln von Passwörtern (password + fishing), werden bei diesem Cyber-Angriff Daten über gefälschte Internetadressen, E-Mail oder SMS abgefangen. Dabei steht die Nachahmung eines für das Opfer bekannten Designs im Zentrum.

Spear-Phising

Spear-Phisher finden und verwenden Daten, die frei im Internet verfügbar sind, um sich selbst vertrauenswürdig erscheinen zu lassen und andere dazu zu bringen, ihnen mehr persönliche Informationen zu geben. Solche Cyber-Angriffe sind schwierig von „echten" Meldungen zu unterscheiden.

Whale-Phising / CEO-Fraud

Während Spear-Phishing auf „kleinere Fische" abzielt, wie z. B. einen Mitarbeitenden eines mittelgrossen Unternehmens oder ein zufällig ausgewähltes Ziel in den sozialen Medien, hat es Whale-Phishing auf die „grossen Fische" abgesehen. Diese Angriffe zielen oft auf Führungskräfte wie CEOs oder CFOs ab, um an grössere Auszahlungen und sensiblere Daten zu gelangen, für welchen sich die letzten Jahre der Begriff des CEO-Fraud durchgesetzt hat.

DoS

Ein Denial-of-Service-Angriff (DoS) liegt vor, wenn Benutzer aufgrund der Aktionen eines Cyber-Angriffs nicht auf Informationssysteme, Geräte oder andere Netzwerkressourcen zugreifen können. Ein Denial-of-Service-Zustand wird erreicht, indem die IT-Infrastruktur mit Anfragen überflutet wird, sodass diese nicht mehr reagieren kann oder sogar abstürzt. DoS-Angriffe können eine Organisation sowohl Zeit als auch Geld kosten, während ihre Ressourcen und Dienste unzugänglich sind.

2020 Pricing (USD): Exploit Kits for Phishing, Ransomware and Others	
Ransomware exploit kitw	$ 9
Legacy ransomware, bundle of 9 types	$ 12
Tailored phishing page with tutorial	$ 35
Office365 exploit kit	$ 125

Quelle:
Pricing_Analysis_2020_
WhitePaper_121820_Final
by Flashpoint: Dark Web
marketplaces 2020

Handbuch für Verkehrsbetriebe

Ein Verkehrsbetrieb übernimmt teilweise auch die Rolle des Betreibers einer kritischen Infrastruktur. Er stellt die Verfügbarkeit des Verkehrs sicher, denn ein (Teil-)Ausfall kann bereits beträchtliche Auswirkungen auf die Schweizer Wirtschaft und die Bevölkerung haben. Ein kürzlich erschienenes Handbuch[4]) des BWL[5]) für Betriebe des öffentlichen Verkehrs adressiert diese Thematik speziell in Bezug auf Cyber Security. Es beschreibt unter anderem die kritischen Prozesse eines Verkehrsbetriebes. Hier wird deutlich, das Cyber Security ein unternehmensweites Thema ist und nicht nur die unmittelbaren Prozesse der Informatik betrifft. Von Instandhaltungs-Prozessen, deren Bewirtschaftung über die Erbringer von Verkehrsleistung bis hin zur Unternehmensführung - in allen Bereichen eines Verkehrsbetriebes sind kritische Prozesse vorhanden, die es zu schützen gilt. Das Handbuch weist auf die entsprechenden „digitalen" Risiken, aber auch auf die Möglichkeiten zur Minderung dieser hin. Es verleiht damit der Bedeutung der Thematik Cyber Security zusätzlich Gewicht und liefert einen weiteren Grund für Verkehrsbetriebe, sich mit der eigenen Sicherheitslage auseinanderzusetzen.

4
https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/oeffentlicher_verkehr.html

5
Bundesamt für wirtschaftliche Landesversorgung

In drei Schritten die Cyber Security verbessern

Für eine lohnende Auseinandersetzung mit der eigenen Situation hinsichtlich Cyber Security muss das Rad nicht neu erfunden werden. So beschreibt das erwähnte Handbuch einen etablierten und bewährten Prozess zur Verbesserung der Cyber Security. Eraneos wendet diese Vorgehensweise regelmässig an und bietet erfahrene Begleitung durch den aus drei Schritten bestehenden Prozess.

Schritt 1 – Bestimmung des Cyber Security-Ist-Zustands

Der aktuelle Cyber Security-Reifegrad der Unternehmung wird bestimmt. Dies geschieht mithilfe von anerkannten Rahmenwerken (Frameworks), die für alle relevanten Bereiche der Cyber Security umfangreiche Mechanismen und Handlungen formulieren.

Schritt 2 – Bestimmung des Cyber Security-Ziel-Zustands

Weiter bestimmt die Unternehmung den für sie passenden Ziel-Zustand. Dieser gestaltet sich individuell für jede Firma und formuliert dementsprechend beispielsweise unterschiedliche Prioritäten oder unterschiedlich angestrebte Reifegrade.

Schritt 3 – Identifikation und Priorisierung von Massnahmen

Die Lücken zwischen Ist- und Ziel-Zustand werden gezielt adressiert und behoben. Dafür werden passende Massnahmen identifiziert und priorisiert, hierbei unterstützen wieder die Rahmenwerke mit Best-Practice-Vorgaben, Mechanismen und Handlungsvorschlägen.

Ein wichtiger Bestandteil des vorgestellten Vorgehens zur Verbesserung der Cyber Security sind die erwähnten Rahmenwerke. In den vergangenen Jahren haben sich einige solche etabliert, wobei das ISO 27001 Cyber Security Framework[6]) und das NIST Cyber Security Framework[7]) zu den bekanntesten gehören und am weitesten verbreitet sind.

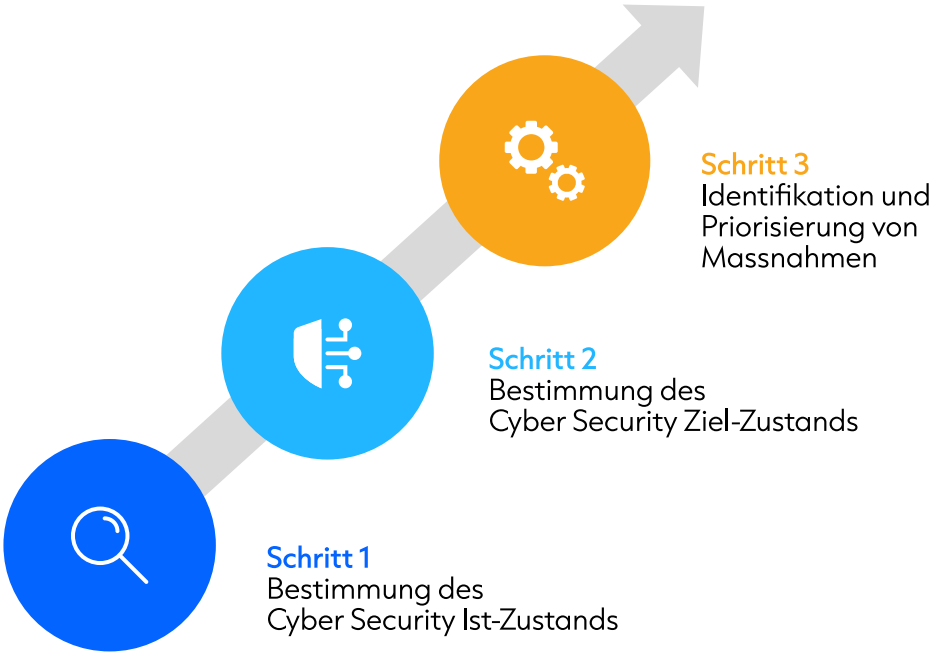
6 https://www.iso.org/standard/54534.html

7 https://www.nist.gov/cyberframework

NIST Cyber Security Framework

Das NIST Cyber Security Framework bietet einen technologieneutralen und branchenunabhängigen Ansatz für die Identifikation, Beurteilung und Regelung von Cyber Security-Risiken. Es basiert auf einer breiten Anzahl von bestehenden Standards, Richtlinien sowie Praktiken und stellt Firmen eine gemeinsame Taxonomie und Mechanismen zum besseren Verständnis und besserer Handhabung ihrer Cyber Security-Risiken zur Verfügung. Das Framework unterstützt sowohl bei der Beschreibung des aktuellen- als auch des angestrebten Cyber Security-Zustands bei der Identifikation und Priorisierung von Verbesserungspotenzial und der Bewertung des Verbesserungsfortschritts.

Verbesserung der Cyber Security Sicherheitslage



Identify - Protect - Detect - Respond - Recover

Der Kern des NIST Cyber Security Frameworks stellt eine Auswahl an Handlungen zur Erreichung von spezifischen Cyber Security-Zielen bereit. Dabei fassen fünf Funktionen diese Handlungen thematisch zusammen und erlauben damit einen strategischen Blick von angemessener Granularität auf das Management von Cyber Security-Risiken.

Identifizieren (Identify)

Schaffung eines unternehmensweiten Verständnisses für das Management von Cyber Security-Risiken.

Schützen (Protect)

Entwicklung und Umsetzung von Schutzmassnahmen, welche die Ausübung der (relevanten) Geschäftstätigkeiten sicherstellen.

Erkennen (Detect)

Entwicklung und Umsetzung von Mechanismen zur Identifikation von Cyber Security-Vorfällen.

Reagieren (Respond)

Entwicklung und Umsetzung von Massnahmen in Bezug auf erkannte Cyber Security-Vorfälle.

Wiederherstellen (Recover)

Entwicklung und Umsetzung von Plänen, Prozessen und Fähigkeiten zur Wiederherstellung von Geschäftsprozessen, die durch Cyber Security-Vorfälle beeinträchtigt sind.

Einfach starten mit einem Assessment

Als Ausgangspunkt empfiehlt sich die Durchführung eines Assessments, in dem Schwachstellen und blinde Flecken aufgedeckt sowie systematisch, gezielt und priorisiert angegangen werden können. Damit wird ein Bewusstsein für die Thematik geschaffen und der Grundstein für den Verbesserungsprozess gelegt. Ein solches Assessment adressiert die folgenden Fragestellungen:

- Wie sieht der aktuelle Reifegrad bezüglich Cyber Security in meiner Unternehmung aus?
- Was für ein Ziel-Zustand ist sinnvoll und erstrebenswert?
- Welche Massnahmen sind für die Erreichung der gewünschten Reifegradstufe umzusetzen?

Mit den richtigen Werkzeugen wie dem NIST Cyber Security Framework ist die Klärung dieser Fragestellungen keine Hexerei. Die notwendigen Hilfsmittel, Guidelines und Anleitungen sind öffentlich verfügbar, erprobt und können in der Regel frei verwendet werden. Ein Unternehmen kann sich damit ausrüsten und zeitnah mit der Verbesserung der eigenen Sicherheitslage beginnen. Aber obschon Rahmen und Vorgehen mehrheitlich vorgegeben sind, gilt es doch, einige mögliche Hürden zu beachten, damit ein solches Projekt den grösstmöglichen Erfolg mit sich bringt.

So besteht die Gefahr, dass ein durch eine interne Stelle durchgeführtes Assessment bewusst oder unbewusst heikle Bereiche meidet und nicht mit der notwendigen Hartnäckigkeit nach möglichen Schwachstellen sucht. Zusätzlich bringt eine interne Untersuchung keine unvoreingenommene, neutrale Aussensicht. Eine solche verhilft aber gerade beim Erkennen von Schwachstellen in etablierten Verhaltensmustern, Strukturen und Prozessen zu einem entscheidenden Mehrwert. Weiter sind bei der Priorisierung und Auswahl von geeigneten Massnahmen zur Erreichung des angestrebten Ziel-Zustands vertiefte Kenntnisse der Materie hilfreich.

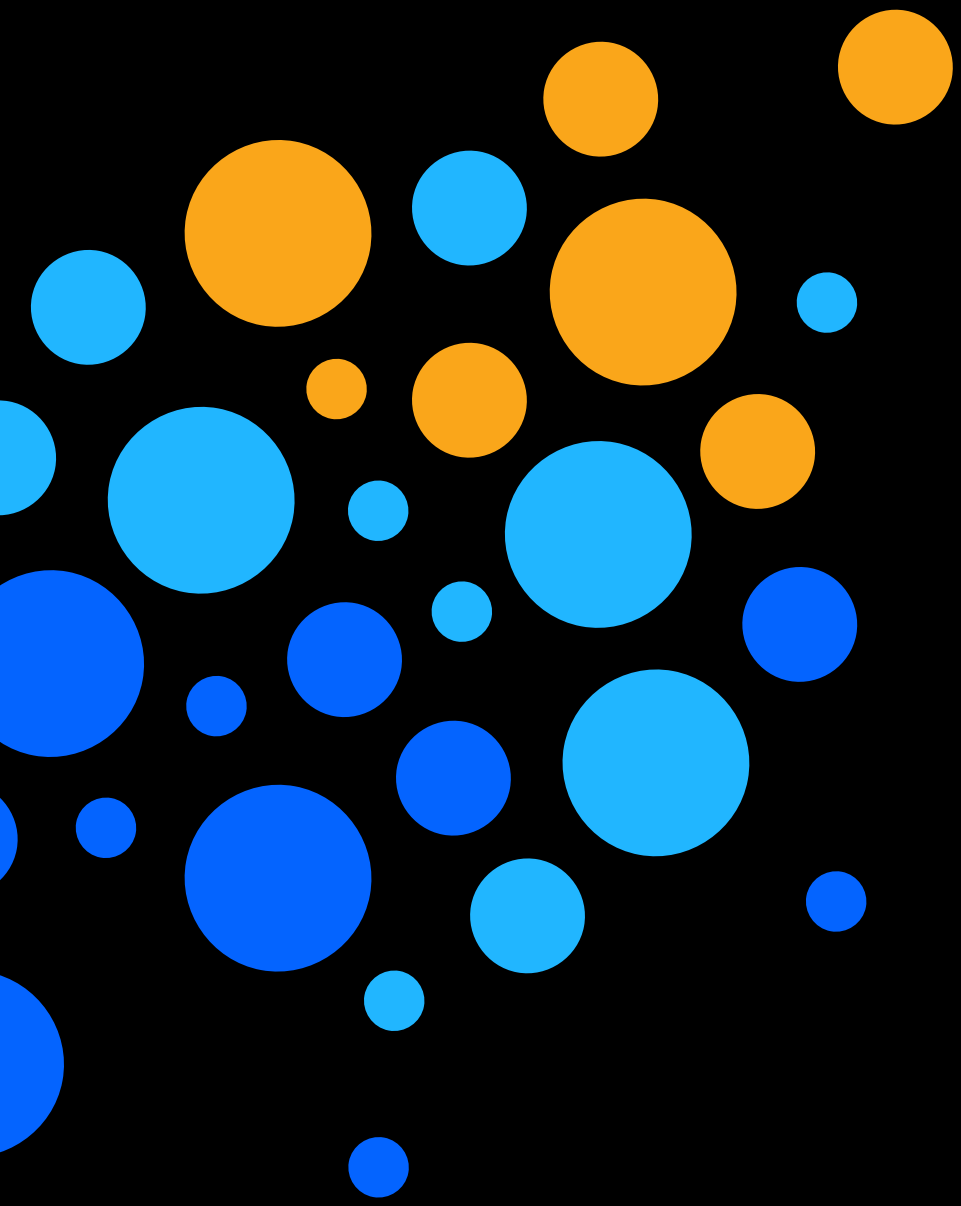
Als Beispiel: Ein Verkehrsbetrieb, der keinerlei Fahrausweiskontrollen durchführt, ist für Schwarzfahrer äusserst attraktiv. Allein durch die Einführung von gelegentlichen Kontrollen können aber die meisten Fahrgäste zum Kauf einer gültigen Fahrkarte bewegt werden. Auch die Mehrzahl der Angreifer aus dem digitalen Raum ist ökonomisch getrieben. Lässt sich bei einer Cyber-Attacke kein verhältnismässig einfacher Einstiegspunkt ausmachen, so verliert ein mögliches Ziel schnell an Attraktivität und ein neues Opfer wird stattdessen ins Visier genommen. Mit einem Assessment kann die Cyber Security entlang der drei vorgestellten Schritte auf eine einfache und bewährte Art angegangen werden. Durch die Auswahl von passenden Massnahmen wird es möglich, die Attraktivität der eigenen Unternehmung für Cyber-Kriminelle zielgerichtet und massgeblich zu vermindern.

Mit der Expertise im Bereich Cyber Security & Privacy und einem grossen Know-how im Bereich Verkehrsbetriebe kann Eraneos optimal unterstützen und massgeschneiderte Assessments anbieten. Zuletzt durfte Eraneos im öffentlichen Verkehr beispielsweise die Bus Ostschweiz (BOS) bei der Evaluierung und Verbesserung ihrer Cyber Security unterstützen.

„Durch das professionelle Security-Assessment von Eraneos konnten wir den Reifegrad unserer Cyber Security evaluieren und gezielte Massnahmen zum angestrebten Ziel-Zustand identifizieren. Zudem konnte unsere Security-Awareness im Unternehmen gestärkt werden."

Hans Koller, Leiter Markt, BUS Ostschweiz

eraneos



Experienced in a wide range of industries

Eraneos Group ist eine internationale Management- & Technologieberatungsgruppe, die Dienstleistungen von Strategie bis Implementierung anbietet. Sie ist aus dem 2021 angekündigten Zusammenschluss von Ginkgo Management Consulting, Quint Group und AWK Group hervorgegangen. Die Gruppe betreut Kunden auf drei Kontinenten, wo rund 1.000 engagierte und hochqualifizierte Fachleute gemeinsam daran arbeiten, das volle Potenzial der Digitalisierung auszuschöpfen. Die Dienstleistungen reichen von der Entwicklung digitaler Geschäftsmodelle und Datenanalysen bis hin zu Cybersicherheit, von Sourcing und IT-Beratung zum Management komplexer Transformationsprojekte. Eraneos Group hat Niederlassungen in der Schweiz, Deutschland, Luxemburg, Spanien, den Niederlanden, China, Singapur und den USA. 2021 erzielte die Gruppe einen Umsatz von fast 200 Millionen Euro.

Contact us >

Our offices >

Visit our website >