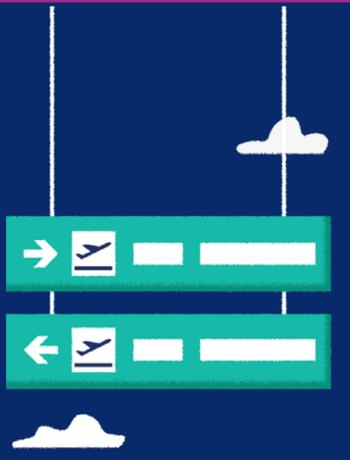
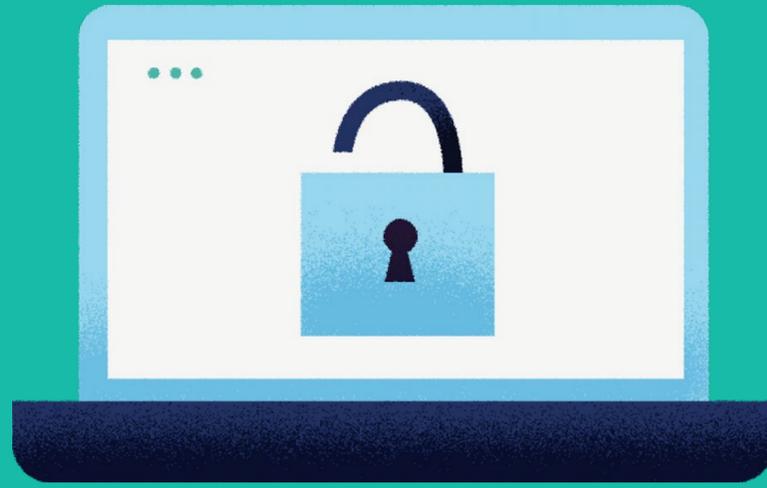
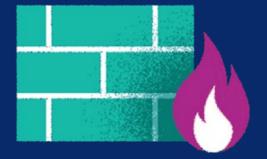
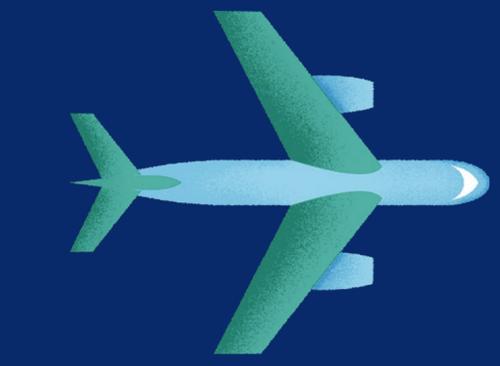


Instrumentarium für die Cybersicherheit im Verkehrssektor



Einführung

Die Generaldirektion Mobilität und Verkehr der Europäischen Kommission (GD MOVE) hat die Entwicklung dieses Instrumentariums in Auftrag gegeben, um die Interessenträger im Verkehrssektor stärker für Cyberbedrohungen zu sensibilisieren und darauf vorzubereiten. Das Instrumentarium soll helfen, Cyberbedrohungen richtig einzuschätzen und ihre Auswirkungen einzudämmen. Es werden darin zwei Sensibilisierungspfade für verschiedene Profile aufgezeigt:

- alle Beschäftigten im Verkehrssektor (mit allgemeinen Informationen und Beratung)
- im Verkehrssektor für die Cybersicherheit zuständige Entscheidungsträger

Zur leichteren Navigierbarkeit sind die verschiedenen Teile des Instrumentariums durch Querverweise miteinander verknüpft.

Die in diesem Instrumentarium beschriebenen Vorgehensweisen sind rein informativ. Die Empfehlungen sind weder bindend noch verpflichtend. Des Weiteren spiegelt dieses Instrumentarium nicht die offiziellen Standpunkte der Europäischen Kommission wider und ist nicht dazu gedacht, die Einhaltung bestehender oder zukünftiger EU-Rechtsvorschriften zu gewährleisten.



Profile zur Sensibilisierung für die Cybersicherheit

Profil I: Alle Beschäftigten im Verkehrssektor. Der erste Pfad richtet sich an alle Beschäftigten von Verkehrsorganisationen. Er enthält Informationen für ein besseres Verständnis der häufigsten Cyberbedrohungen für den Verkehr. Darüber hinaus wird erläutert, wie mit potenziellen Cyberbedrohungen umgegangen werden kann, einschließlich ihrer Feststellung, Meldung und Eindämmung durch bewährte Verfahren im Bereich der Cybersicherheit.

Profil II: Entscheidungsträger für die Cybersicherheit im Verkehrssektor. Der zweite Pfad richtet sich an Beschäftigte, die Entscheidungsbefugnisse in Bezug auf die Cybersicherheit in Verkehrsorganisationen haben. Hier werden bewährte Verfahren für die verschiedenen Verkehrsträger aufgezeigt. Insbesondere werden bewährte Verfahren für die Feststellung, Abwehr, Erkennung und Reaktion auf neue Cyberbedrohungen für Verkehrsorganisationen erläutert.

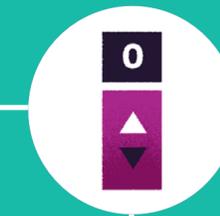


Instrumentarium für die Cybersicherheit im Verkehrssektor



Bedrohungslage im Verkehrssektor

Neue Bedrohungen der Cybersicherheit, die
verschiedene Verkehrsträger betreffen



Profile zur Sensibilisierung für die Cybersicherheit

Alternative, den verschiedenen Verkehrsprofilen
entsprechende Sensibilisierungspfade

Bedrohungslage im Verkehrssektor

Die Bedrohungslage durch Cyberangriffe ist dynamisch und verändert sich ständig. Dennoch ist es möglich, Cyberbedrohungen zu erkennen, denen alle Verkehrsträger ausgesetzt sind.





Angreifer

Einzelpersonen oder Organisationen, die potenziell die Sicherheit von Verkehrsdiensten und -systemen beeinträchtigen können



Neue Cyberbedrohungen

Ausgewählte Cyberbedrohungen, die möglicherweise Angriffsvektoren darstellen, die die Sicherheit von Verkehrsdiensten und -systemen beeinträchtigen können

Angreifer

Einzelpersonen oder Organisationen können absichtlich oder unabsichtlich Schwachstellen aufdecken und ausnutzen, die zu Cybervorfällen führen und die Verkehrsdienste einschließlich ihrer Sicherheit, ihrer Geschäftstätigkeit, ihrer Finanzen und ihres Ansehens beeinträchtigen können.

Cyberkriminelle, Insider, Nationalstaaten und **staatlich geförderte Gruppen** gehören zu den Hauptakteuren, die gezielt Verkehrsorganisationen angreifen.

Cyberkriminelle und andere Angreifer führen massive Angriffskampagnen durch und verfolgen dabei häufig finanzielle Ziele.

Insider kennen die Besonderheiten der Organisationen, für die sie tätig sind, und wissen oft sehr gut über versteckte Sicherheitslücken Bescheid. Bei den Insidern kann es sich

um unzufriedene Mitarbeiter, Lieferanten und einzelne Auftragnehmer handeln.

Im Zuge der sich weltweit verschärfenden geopolitischen Spannungen verfolgen **Nationalstaaten** und **staatlich geförderte Gruppen** langfristige strategische Ziele. Diese versuchen oftmals, unerkannt in die Systeme einer Organisation einzudringen, um dort an sensible Informationen zu gelangen. Sind die Systeme erst einmal infiltriert, versuchen staatlich unterstützte Angreifer, sich so zu positionieren, dass sie den größtmöglichen Schaden anrichten können.

nicht böswillige Akteure gelten **Insider**, deren unbeabsichtigte oder versehentliche Handlungen sicherheitsrelevante Ereignisse und im schlimmsten Fall Cybervorfälle verursachen können.



Neue Cyberbedrohungen

Es gibt zahlreiche Cyberbedrohungen für den Verkehrssektor: **Distributed Denial of Service**, **Denial of Service**, Datendiebstahl, Verbreitung von **Schadsoftware** („Malware“), **Phishing**, Softwaremanipulation, **unbefugter Zugriff**, zerstörerische Angriffe, Fälschung oder Umgehung des Entscheidungsprozesses des Sicherheitsdiensts, Verschleierung der Identität, Missbrauch von Zugriffsrechten, **Social Engineering**, Verunstaltung („Defacement“), Abhören, Missbrauch von Anlagen und Hardwaremanipulation.

Nach umfassender Literaturrecherche in öffentlich zugänglichen Dokumenten und Befragungen von Experten haben sich folgende neue Cyberbedrohungen für den Verkehrssektor als am dringlichsten erwiesen: Schadsoftware, (Distributed) Denial of Service, unbefugter Zugriff und Diebstahl sowie Softwaremanipulation.





Bedrohung Nr. 1: Schadsoftware

Schädliche Software, die potenziell Einzelpersonen oder Organisationen bei allen Verkehrsträgern beeinträchtigen kann



Bedrohung Nr. 2: (Distributed) Denial of Service

Cyberangriffe, die Einzelpersonen oder Organisationen den Zugang zu Diensten und Ressourcen verwehren



Bedrohung Nr. 3: Unbefugter Zugriff und Diebstahl

Unbefugter Zugriff, unbefugte Aneignung und Nutzung von kritischen Anlagen



Bedrohung Nr. 4: Software- manipulation

Cyberangriffe auf Software, um deren Verhalten zu ändern und gezielte Angriffe durchzuführen

Bedrohung Nr. 1: Schadsoftware

Bei Schadsoftware handelt es sich um schädliche Software, wie etwa Viren, Trojaner, Würmer, Ransomware, Kryptowährungsminer oder jede andere Software, die potenziell nachteilige Auswirkungen auf Organisationen oder Einzelpersonen bei allen Verkehrsträgern haben kann.

Die Eindämmung der Verbreitung von Schadsoftware, die gezielt zur Schädigung von Computern, Servern, Clients, Netzen oder allen diesen Elementen entwickelt wurde, gehört zu den wichtigsten Prioritäten der Cybersicherheit bei allen Verkehrsträgern. Ein typischer Angriffsvektor sind Phishing-E-Mails an Mitarbeiter. Aber auch technisch ausgefeilte Social-Engineering-Strategien, wie das Einstecken eines USB-Sticks in einen freien Anschluss (z. B. zum Aufladen

eines Mobiltelefons), stellen Angriffsvektoren dar. Durch das Anklicken von Links in verdächtigen E-Mails oder das Öffnen von Dateianhängen kann der Nutzer unwissentlich Schadsoftware installieren.

Der Cyberangriff mit der Ransomware „WannaCry“ zum Beispiel betraf mehr als 150 Länder und infizierte über 230 000 Systeme. Die dazu verwendete Ransomware wird in der Regel über Phishing-E-Mails mit schädlichen Anhängen oder Links verbreitet. Bei dieser Art von Angriffen wird Social Engineering böswillig ausgenutzt, um Systembenutzer dazu zu verleiten, eine bestimmte Schadsoftware zu installieren (oder zu aktivieren).

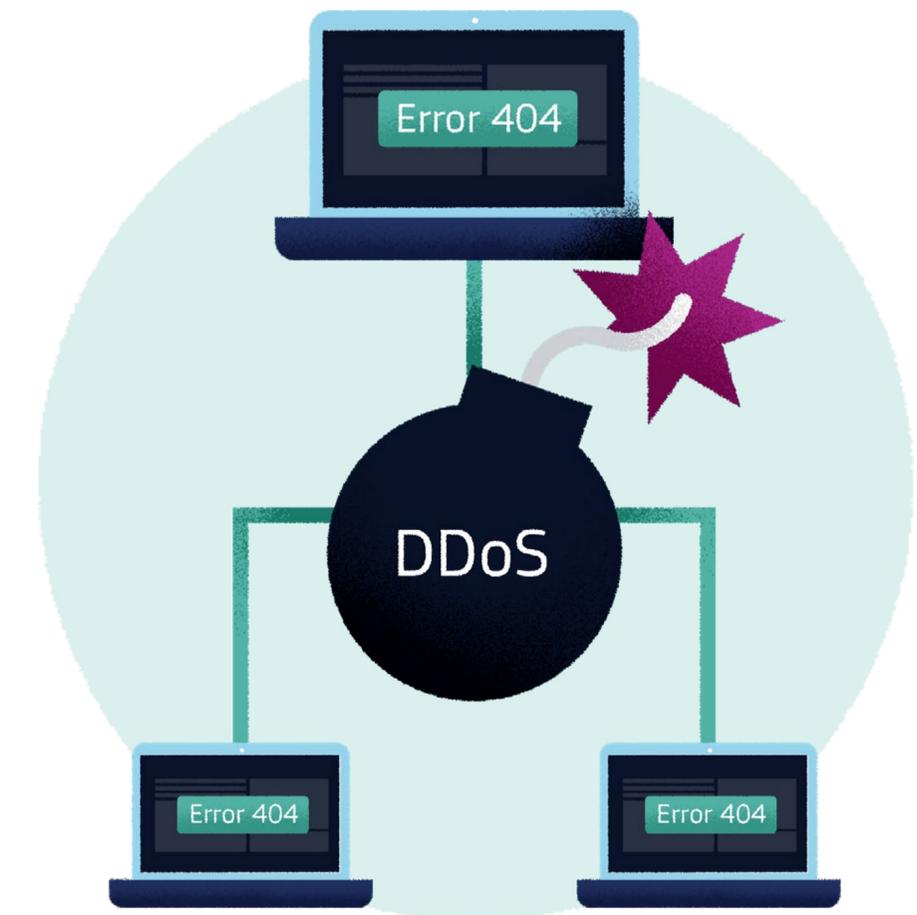


Bedrohung Nr. 2: (Distributed) Denial of Service

DDoS-Angriffe (*Distributed Denial of Service*) und DoS-Angriffe (*Denial of Service*) beeinträchtigen die Verfügbarkeit und Zugänglichkeit von Daten, Diensten, Systemen und anderen Ressourcen. Diese Arten von Angriffen können von unterschiedlicher Dauer sein und mehrere Dienste oder Systeme gleichzeitig betreffen. Bei DDoS-Angriffen werden mehrere Systeme (oder Angriffskanäle) eingesetzt, um die Zieldienste oder -systeme mit Anfragen zu überlasten. Bei einem erfolgreichen Angriff wird die Fähigkeit von Diensten und Systemen, mit der unerwarteten Menge an Anfragen umzugehen, beeinträchtigt. Dies führt dazu, dass der Zugang zu Diensten und Ressourcen verweigert wird.

Die von einem Angriff betroffenen Dienste und Systeme von Verkehrsorganisationen können aber auch für DDoS- und DoS-Angriffe auf bestimmte Systeme in anderen Betrieben oder Organisationen ausgenutzt werden.

Interne Informationssysteme (wie PCs und Geräte) können beispielsweise gezielt für den Zugriff auf operative Technik genutzt werden, falls diese mit dem Internet oder mit Netzen verbunden ist, um operative Daten übertragen zu können. Schnittstellen zwischen verschiedenen Systemen und Netzen (z. B. interne Netze, operative Technik und Fernwartungszugänge) können Schwachstellen darstellen, die für DDoS- oder DoS-Angriffe auf kritische Verkehrsdienste und -systeme genutzt werden können. So können DDoS- und DoS-Angriffe gängige Netzwerk- und Kommunikationsprotokolle wie Web Services Dynamic Discovery (WS-Discovery) zur automatischen Erkennung von IoT-Geräten in lokalen Netzen (LANs) ausnutzen. Wenn die IoT-Geräte Schwachstellen aufweisen, können Angreifer diese ausnutzen, um andere verbundene Geräte zu finden und DDoS- oder DoS-Angriffe durchzuführen.



Bedrohung Nr. 3: Unbefugter Zugriff und Diebstahl

Angreifer können sich ohne Berechtigung logischen oder physischen Zugriff auf ein Netz, ein System, eine Anwendung, auf Daten oder andere Ressourcen verschaffen, um böswillige Aktivitäten durchzuführen, wie z. B. den Diebstahl von sensiblen Daten oder Ressourcen (einschließlich physischer Ressourcen).

Die Bedrohung durch unbefugten Zugriff und Diebstahl betrifft vertrauliche und geschützte Güter (einschließlich personenbezogener Daten, Zugangsdaten für privilegierte Konten, Systeme und andere Arten von vertraulichen und geschützten Informationen). Für diese Bedrohungen können sowohl Schwachstellen in den Systemen als auch ahnungslose Personen ausgenutzt werden, die sensible Daten wie Zugangsdaten (z. B. Login, Passwort usw.) oder personenbezogene Daten (z. B. E-Mail-Adresse, Personalausweisnummer usw.) preisgeben.

In Verbindung mit einem unbefugten Zugriff bezieht sich Identitätsdiebstahl auf die unerlaubte Verwendung personenbezogener Daten oder spezifischer Identifikationsmerkmale, mit dem Ziel, die Identität von Personen, Diensten oder Systemen vorzutäuschen, um so Zugang zu privaten oder geschützten Ressourcen (einschließlich finanzieller und physischer Ressourcen) zu erhalten. Auch physische Anlagen der verschiedenen Verkehrsträger können von diesen Cybersicherheitsbedrohungen betroffen sein.

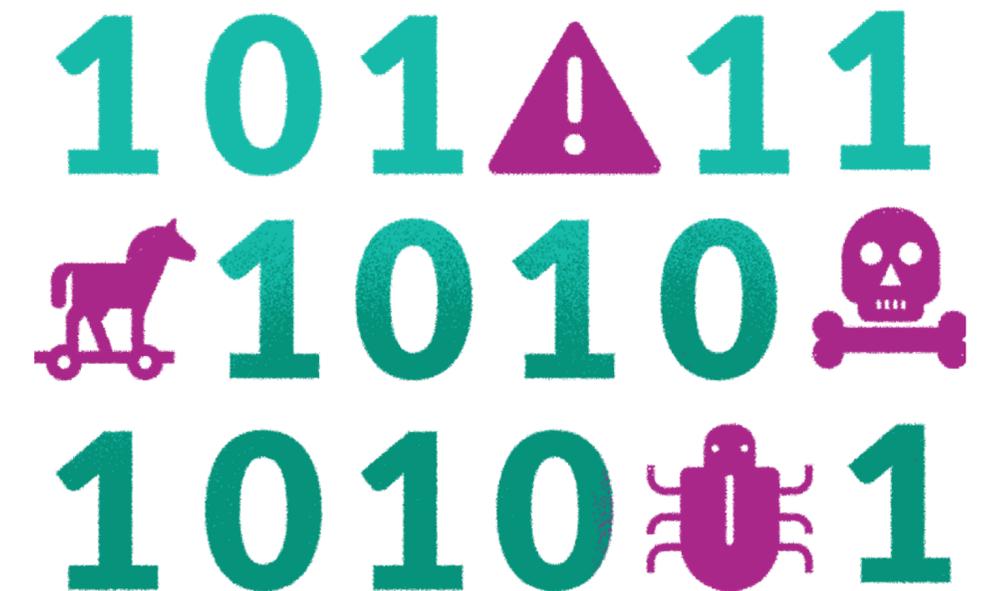


Bedrohung Nr. 4: Softwaremanipulation

Falsche Konfigurationen und Manipulationen von Software und zugehörigen Systemen oder Komponenten können sich unmittelbar auf die Sicherheitslage von Verkehrsdiensten und -systemen auswirken.

Bei Cyberangriffen mit einer manipulierten Software werden die Softwareeinstellungen geändert oder die Datenintegrität beeinträchtigt, um so das Verhalten von Systemen und Diensten zu beeinflussen. Angreifer können Software (oder Teile davon) absichtlich manipulieren, um sich damit Vorteile zu verschaffen (wie einen unbefugten Zugriff, Verhinderung des Zugriffs berechtigter Personen oder Systeme auf notwendige Ressourcen, Beschaffung sensibler Informationen, Änderung des Funktionsverhaltens usw.) und so Einfluss auf sensible Güter zu nehmen.

Beispielsweise können gezielt Kommunikationskanäle von Herstellern angegriffen werden, um schädliche Softwareupdates auf Dienste und Systeme (einschließlich operativer Technik) im Betrieb aufzuspielen. Mittels kompromittierter Zugangsdaten kann sich ein Angreifer Zugang zu einer gesicherten Schnittstelle eines Fernwartungsnetzes verschaffen, um so manipulierte Software zu installieren und andere zugängliche Dienste und Systeme zu kompromittieren. Der Angreifer installiert manipulierte Software, die die Zieldienste und -systeme weiter beeinträchtigt oder andere verbundene Dienste oder Systeme angreift.



Profile zur Sensibilisierung für die Cybersicherheit



1

Profil I: Alle Beschäftigten im Verkehrssektor

Der erste Pfad richtet sich an alle Beschäftigten in Verkehrsorganisationen, vom Personal im Verkehrsbetrieb bis hin zum Verwaltungspersonal. Ziel ist ein besseres Verständnis und eine verstärkte Sensibilisierung hinsichtlich der häufigsten Cyberbedrohungen. Darüber hinaus wird erläutert, wie mit potenziellen Cyberbedrohungen umgegangen werden kann, einschließlich ihrer Feststellung, Meldung und Eindämmung. Dieser Pfad ist für alle Verkehrsträger gleich.

2

Profil II: Entscheidungsträger für die Cybersicherheit im Verkehrssektor

Der zweite Pfad richtet sich an Beschäftigte, die Entscheidungsbefugnisse in Bezug auf die Sicherheit oder Cybersicherheit in Verkehrsorganisationen haben. Hier werden bewährte Verfahren für die verschiedenen Verkehrsträger aufgezeigt. Dabei werden bewährte Verfahren für die Feststellung, Abwehr, Erkennung und Reaktion auf neue Cyberbedrohungen für Verkehrsorganisationen erläutert.

Profil I: Alle Beschäftigten im Verkehrssektor

Dieser Teil richtet sich an alle Beschäftigten in Verkehrsorganisationen, vom Personal im Verkehrsbetrieb bis hin zum Verwaltungspersonal. Ziel ist ein besseres Verständnis und eine verstärkte Sensibilisierung hinsichtlich der häufigsten Cyberbedrohungen. Darüber hinaus wird erläutert, wie mit potenziellen Cyberbedrohungen umgegangen werden kann, einschließlich ihrer Feststellung, Meldung und Eindämmung.

Dieser Teil enthält empfohlene Verfahren und nützliche Tipps, die **für alle Verkehrsträger** relevant sind.



Bewährte Verfahren gegen Schadsoftware

Sie können zum Schutz Ihrer Organisation beitragen, indem Sie bewährte Verfahren zur **Feststellung von Schadsoftware und zur Verhinderung ihrer Verbreitung** einhalten, wie beispielsweise folgende:

- **Beachten Sie die Sicherheitsregeln.** Diese können beispielsweise beinhalten, dass Sie alle Speichermedien und Dateien auf Viren scannen, das Öffnen und Versenden bestimmter Dateitypen (z. B. ausführbare Dateien mit Dateiendungen wie .exe, .bat, .com usw.) vermeiden, ausschließlich zugelassene Software installieren und sicherstellen, dass die Software (einschließlich der Antivirensoftware) immer auf dem neuesten Stand ist und ordnungsgemäß funktioniert.
- **Sichern Sie Ihre Daten** regelmäßig auf sicheren (und zugelassenen) Datenspeichergeräten oder -diensten. Diese sollten Verschlüsselungsmechanismen unterstützen, sodass gespeicherte Daten geschützt sind und wiederhergestellt werden können.

- *Schützen Sie alle Systeme, einschließlich mobiler Geräte und Endgeräte, durch geeignete **Schutzmaßnahmen** (z. B. Passwort, Verschlüsselung usw.), und denken Sie daran, alle Systeme (physisch und digital) abzusperren, wenn sie unbeaufsichtigt sind.*
- *Öffnen Sie keine Anhänge und klicken Sie nicht auf Links, die in unangekündigten E-Mails und verdächtigen Webbrowser-Popups mit seltsamem Text oder von unbekanntem Absendern und Internetdomänen enthalten sind.*
- *Schließen Sie keine **nicht vertrauenswürdigen oder unbekanntem Wechselmedien** wie USB-Sticks, Festplatten und andere Speichermedien an Ihren Computer an.*
- *Deaktivieren Sie keine Schutzmaßnahmen gegen Schadsoftware (z. B. Antivirensoftware, Software zur Inhaltsfilterung, Firewall usw.)*

- **Aktualisieren Sie die installierte Software** regelmäßig auf die aktuell erhältlichen Versionen (die Informationssicherheitsbeauftragte oder Systemadministratoren mit regelmäßigen Updates freigeben können).
- *Verwenden Sie für reguläre Aktivitäten und Vorgänge keine privilegierten Konten (z. B. mit Administratorrechten) und Zugangsdaten.*
- *Melden Sie dem Informationssicherheitsbeauftragten oder Systemadministrator jede verdächtige E-Mail und jedes unerwartete Systemverhalten.*
- *Achten Sie bei der täglichen Routinearbeit auf die Informationssicherheit, damit Sie IT-Sicherheitsprobleme erkennen und entsprechend reagieren können.*

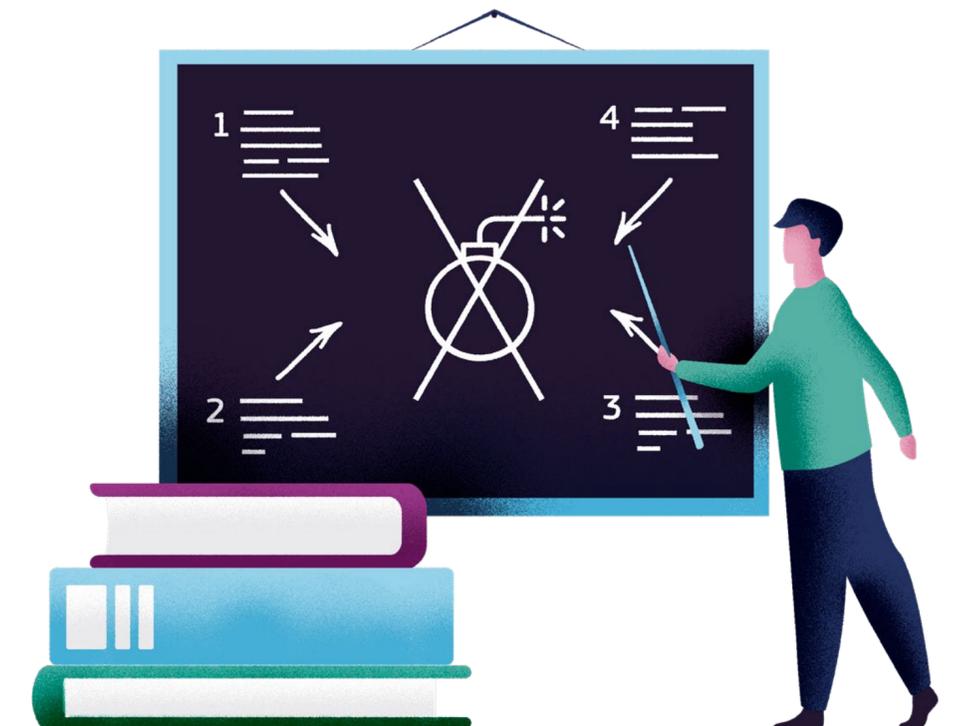
Bewährte Verfahren gegen DDoS-Angriffe

Sie können zum Schutz Ihrer Organisation beitragen, indem Sie **DDoS-Angriffe** (*Distributed Denial of Service*) und **DoS-Angriffe** (*Denial of Service*) erkennen. Sie sollten sich unverzüglich mit Ihrem Sicherheits- und IT-Team in Verbindung setzen, wenn Sie eines der folgenden Anzeichen für einen möglichen DDoS- oder DoS-Angriff auf Ihre Dienste oder Systeme entdecken:

- *Vermehrte Anfragen, die die Netzkapazität beanspruchen (erkennbar an verlangsamten Diensten und Antworten), und die schließlich zu Dienst- oder Systemausfällen aufgrund von Überlastung führen*
- *Steigender Bedarf an Speicherressourcen ohne ersichtlichen Grund*
- **Unerwartetes Verhalten von Diensten und Systemen**, häufige Abstürze und seltsame Fehlermeldungen

aufgrund böswilliger Inanspruchnahme von Rechenressourcen oder Netzverbindungen

- **Verschlechterte Leistung** der Geräte, lange Ausführungszeiten für einfache Funktionen und auffällige Aktivitäten (z. B. lauter Lüfter bei langsamer Geräteleistung)
- **Unerwartete Internetverbindungen oder Verbindungsabbrüche** zu Diensten und Systemen
- *Unauffällige Änderungen im Verhalten von Bedienelementen oder technischen Anlagen, die zu physischen Schäden führen*
- *Verweigerung des Zugriffs auf privilegierte Konten oder Administratorkonten, sodass Maßnahmen zur Wiederherstellung blockiert werden*



Bewährte Verfahren gegen unbefugten Zugriff und Diebstahl

Um Angriffe mit unbefugtem Zugriff und Diebstahl zu verhindern, müssen Grundsätze wie „*Kenntnis nur, wenn nötig*“ und „*Sicherheit und Schutz der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen*“ beachtet werden. In diesen Grundsätzen wird darauf hingewiesen, dass sensible und vertrauliche Güter (einschließlich personenbezogener und sensibler Daten, Verkehrssysteme usw.) nur denjenigen zugänglich sein sollten, die im Rahmen ihrer Aufgaben zugangsberechtigt sind. Sie können zum Schutz Ihrer Organisation beitragen, indem Sie bewährte Verfahren zur Feststellung und Verhinderung von unbefugtem Zugriff und Diebstahl einhalten, wie beispielsweise folgende:

- *Beachten Sie die Sicherheitsregeln Ihrer Organisation.*
- *Vermeiden Sie die Weitergabe und Veröffentlichung von Online-Zugangsdaten und personenbezogenen Daten, einschließlich Bildern, die diese Informationen enthalten könnten.*

- *Vermeiden Sie die Verwendung oder Übermittlung von Zugangsdaten und personenbezogenen Daten (und anderen sensiblen Daten) an nicht vertrauenswürdige und unsichere Netze, Geräte oder Webdienste (z. B. an Internetseiten, die unsichere Protokolle oder Adressen (<http://>) und keine sicheren (<https://>) verwenden.*

- **Geben Sie Ihre Zugangsdaten (z. B. Login und Passwort) niemals an andere Personen weiter**, auch nicht per E-Mail oder Telefon.

- *Schützen Sie sensible Daten, die auf Tastaturen eingegeben oder auf Bildschirmen (auch auf mobilen Geräten) angezeigt werden, vor unbefugten Personen und bringen Sie Sichtschutzvorrichtungen an. Arbeiten Sie nicht an öffentlichen Orten mit privaten Geräten, und lassen Sie ihre Geräte niemals ungesperrt und unbeaufsichtigt.*

- *Um unbefugte Zugriffe zu vermeiden, **verwenden Sie starke Passwörter** (z. B. ein ausreichend langes Passwort mit einer Kombination aus alphanumerischen Zeichen und*

Sonderzeichen) nach Maßgabe der Sicherheitsregeln Ihrer Organisation.

- **Ändern Sie die Standardpasswörter** von angeschlossenen Systemen und Geräten (z. B. Drucker, Router, Kameras, Smart Lock usw.).

- *Verwenden Sie nicht dieselben Zugangsdaten (z. B. Login und Passwort) für mehrere Dienste und Systeme, und achten Sie darauf, dass Sie nicht dieselben Zugangsdaten für Dienste und Systeme verwenden, die privilegierte Konten voraussetzen.*

- *Übermitteln Sie Passwörter und Schlüssel für übertragene geschützte Dateien (z. B. ZIP-Archive) nur über einen Out-of-Band-Kanal (z. B. SMS über GSM und Telefonanruf) und niemals per E-Mail.*

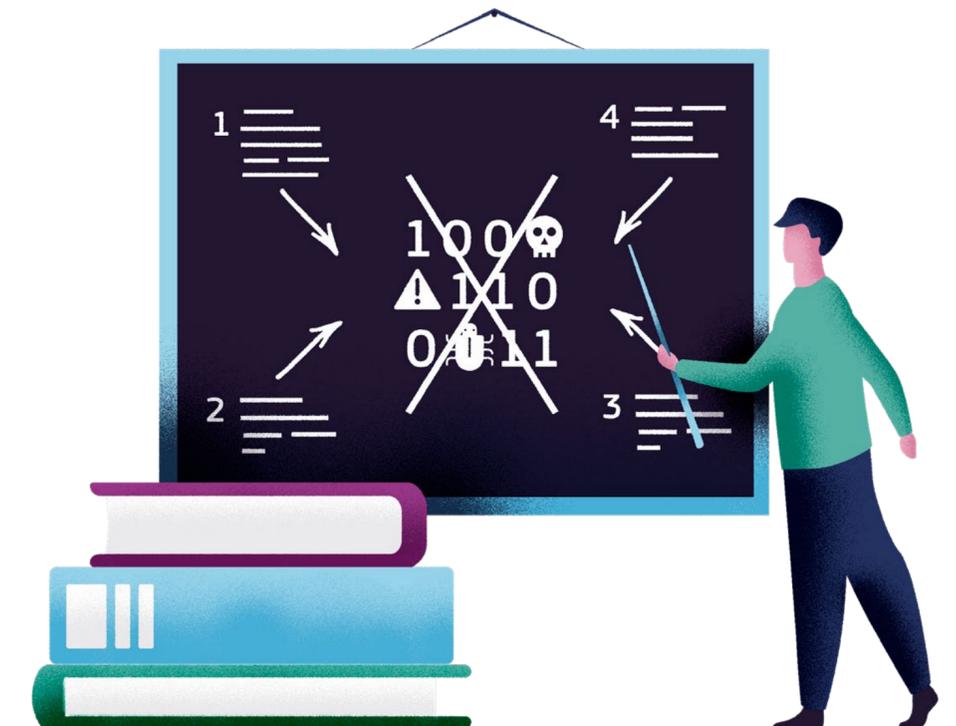
- *Aktivieren Sie, wenn möglich, die **Zwei-Faktor-Authentifizierung (2FA)** oder Multi-Faktor-Authentifizierung (MFA).*

Bewährte Verfahren gegen Softwaremanipulation

Sie können zum Schutz Ihrer Organisation beitragen, indem Sie bewährte Verfahren zur Feststellung und Verhinderung von Softwaremanipulation einhalten, wie beispielsweise folgende:

- *Installieren Sie keine Software auf Systemen und Geräten (einschließlich PCs, Servern, Peripheriegeräten, Netzwerkgeräten, Smartphones usw.), die nicht vertrauenswürdig ist.*
- *Installieren Sie ausschließlich Software und Updates, die von offiziellen Quellen und Internetseiten (z. B. von den Anbietern, internen Software-Bibliotheken usw.) bezogen werden.*
- *Laden Sie keine Software und Anwendungen (und keine Dateien) aus illegalen Quellen herunter.*

- *Deinstallieren Sie nicht mehr benötigte oder nicht mehr verwendete Software und deaktivieren Sie unnötige Verbindungen (z. B. Netzwerkprotokolle und -dienste), einschließlich des Zugriffs auf Remote-Dienste (z. B. Cloud-Speicherdienste).*
- *Scannen Sie jede Software und jedes Speichermedium mit einem zuverlässigen und aktuellen Antivirusprogramm.*
- *Laden Sie sichere Industriesoftware (z. B. Updates, Patches, neue Produkte usw.) von nur vertrauenswürdigen Anbietern herunter und überprüfen Sie diese vor einer Installation in einem isolierten Bereich.*
- *Aktualisieren Sie die gesamte installierte Software nach Maßgabe der Leitlinien und Verfahren der Organisation.*



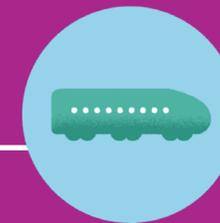
Profil II: Entscheidungsträger für die Cybersicherheit im Verkehrssektor

Dieser Teil richtet sich an Beschäftigte, die Entscheidungsbefugnisse in Bezug auf die Sicherheit oder Cybersicherheit in Verkehrsorganisationen haben. Hier werden bewährte Verfahren für die verschiedenen Verkehrsträger aufgezeigt. Insbesondere werden bewährte Verfahren für die Feststellung, Abwehr, Erkennung und Reaktion auf neue Cyberbedrohungen erläutert.





**Bewährte
Verfahren der
Cybersicherheit für
den Luftverkehr**

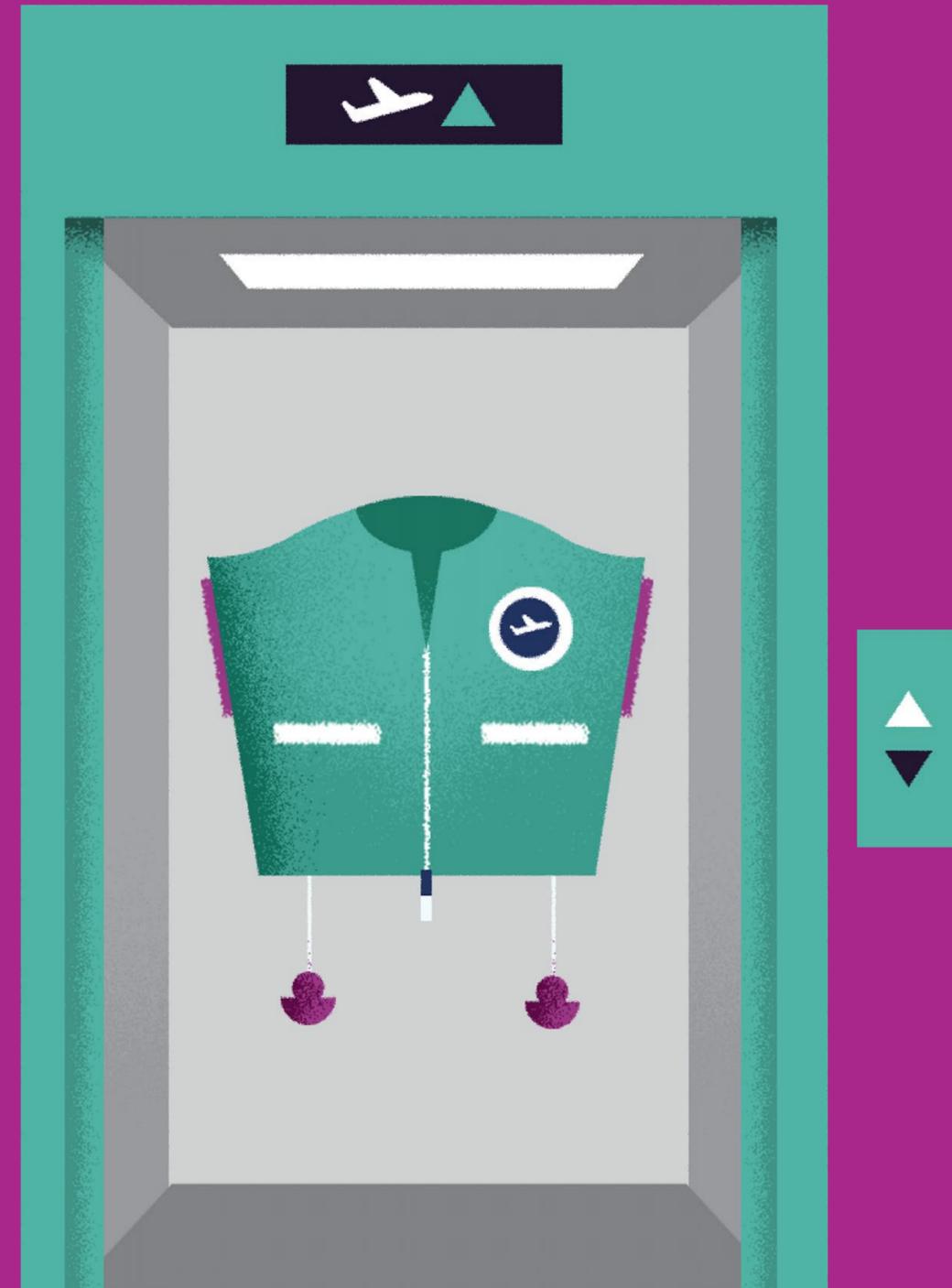


**Bewährte
Verfahren der
Cybersicherheit für
den Landverkehr**



**Bewährte
Verfahren der
Cybersicherheit für
den Seeverkehr**

Bewährte Verfahren und Schutzmaßnahmen für den Luftverkehr



Governance

Luftfahrtorganisationen benötigen genaue Kenntnisse über neue Bedrohungen, bevor sie Strategien und Verfahren zur Verbesserung der Cybersicherheit von Diensten und Systemen im Betrieb, einschließlich Informationstechnik (IT) und operativer Technik (OT), festlegen können.

Zu den bewährten Verfahren für Organisationen jeder Größe gehören:

- die Sicherstellung, dass die oberste Führungsebene Bedenken hinsichtlich der Cybersicherheit an die Geschäftsleitung und den Vorstand meldet, damit diese fundierte Entscheidungen über die Zuweisung von Ressourcen treffen können,
- die Ernennung eines leitenden Beauftragten, der sowohl für die Cybersicherheit als auch für die physische Sicherheit verantwortlich ist und die Gesamtverantwortung für die Sicherheit der Informationstechnik (IT) und der operativen Technik (OT) trägt, jedoch zur Vermeidung

von Interessenkonflikten nicht in den operativen Betrieb eingebunden ist,

- die eindeutige Festlegung von Funktionen, Verantwortlichkeiten, Zuständigkeiten und Freigaben im Zusammenhang mit der Cybersicherheit und deren Kommunikation an und Absprache mit den betreffenden Mitarbeitern; dies gilt insbesondere für Mitglieder von IT-Notfallteams (*Computer Emergency Response Teams – CERTs*),
- die Sicherstellung einer Governance im Bereich der Cybersicherheit für die gesamte Kette der Sicherheitsdienstleistungen, einschließlich der physischen und digitalen Schnittstellen, von den Technologieherstellern und Installationsbetrieben bis hin zu den Sicherheitsanbietern,
- die Festlegung von Maßnahmen und Kontrollen, einschließlich gemeinsamer Verantwortlichkeiten, zur Beherrschung von Cybersicherheitsrisiken und die

Gewährleistung, dass diese Verantwortlichkeiten während der gesamten Lebensdauer von Sicherheitslösungen und -diensten aufrechterhalten werden (z. B. durch Dienstleistungsverträge),

- die Festlegung von Governance-Mechanismen (z. B. Strategien) zur Einhaltung der Verpflichtungen aus den maßgeblichen Verordnungen und Richtlinien, wie z. B. der Verordnung (EU) 2018/1139 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt, der Durchführungsverordnung (EU) 2017/373 der Kommission zur Festlegung gemeinsamer Anforderungen an Flugverkehrsmanagementanbieter und Anbieter von Flugsicherungsdiensten sowie sonstiger Funktionen des Flugverkehrsmanagementnetzes und die Aufsicht hierüber und der NIS-Richtlinie (Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union).

Beispiele für Dienste und Systeme im Luftverkehr:

Beispiele für IT sind Geräte, die sowohl für das Personal (z. B. PCs, Mobiltelefone, Büroperipheriegeräte usw.) als auch für Passagiere/Fahrgäste (z. B. öffentliche Wi-Fi-Router und -Anschlüsse usw.) zugänglich sind. Beispiele für OT sind Prozesssteuerungs- und Datenerfassungssysteme (SCADA), Heizungs-, Lüftungs- und Klimaanlage, Sicherheitskontrollstellen für Handgepäck, Gepäckabfertigungssysteme, Zugangskontrollsysteme, Überwachungssysteme, Alarmsysteme, Durchleuchtungssysteme, Flugfeldbeleuchtungssysteme, Radarsysteme und Sensoren, globale Ortungssysteme (GPS), Flugverkehrsmanagementsysteme (ATM), Kommunikations-, Navigations- und Überwachungssysteme (CNS), Luftfahrtinformationssysteme, meteorologische Systeme, Systeme der Sicherheitszentrale, Bordsysteme der Fluggesellschaften sowie andere Systeme.



Feststellung von Bedrohungen der Cybersicherheit

Risikomanagement: Um die Risiken für die Cybersicherheit der Netz- und Informationssysteme, die für den Betrieb der wesentlichen Funktionen erforderlich sind, zu ermitteln, zu bewerten und richtig einzuschätzen, müssen Luftfahrtorganisationen geeignete Maßnahmen ergreifen.

Dies setzt einen organisationsweiten Risikomanagementansatz voraus, der Folgendes umfasst:

- *Bestandsaufnahme der verschiedenen Hardware- und Softwaresysteme, die für die Erbringung der verschiedenen Dienste eingesetzt werden: Im Luftverkehr umfassen diese Systeme sowohl die Informationstechnik (IT) als auch die operative Technik (OT).*

- **Bewertung der Risiken im Bereich der Cybersicherheit** unter Berücksichtigung neuer Bedrohungen, bekannter Schwachstellen und operativer Daten in Bezug auf die betroffenen Systeme:

Organisationen wie das IT-Notfallteam des europäischen Flugverkehrsmanagementsystems (EATM-CERT) und das Informationsaustausch- und Analysezentrum für den Luftverkehr (A-ISAC) können Informationen über Bedrohungen für den Luftverkehr bereitstellen.

- *Sicherstellung, dass die Risikobewertungen auch die Risiken im Zusammenhang mit dem beruflichen Alltag der Mitarbeiter berücksichtigen (z. B. Nutzung sozialer Medien, Nutzung persönlicher Geräte, Datenverarbeitung, Informationsaustausch usw.)*

- *Feststellung und Umsetzung von Maßnahmen zur Risikobeherrschung und von Plänen zur Eindämmung von Cybersicherheitsrisiken*

- *Einführung eines umfassenden **Managementsystems für Informationssicherheit** (Information Security Management System – ISMS) und eines*

Datenschutzmanagementsystems (Privacy Information Management System – PIMS), das mit anderen Managementsystemen abgestimmt ist: Diese Managementsysteme (d. h. ISMS und PIMS) umfassen die Umsetzung von Sicherheitskontrollen (sowie Kontrollen des Datenschutzes und des Schutzes der Privatsphäre), um neue Bedrohungen für die Sicherheit von Luftverkehrsdiensten und -systemen (einschließlich ihrer Daten) einzudämmen und zu verhindern.

- *Berücksichtigung aller Beschränkungen im Zusammenhang mit der **Anlagenverwaltung und Ressourcenplanung** (d. h. Beschränkungen, die sich auf die Bereitstellung, Wartung und Unterstützung kritischer Systeme für den Betrieb wesentlicher Funktionen im Luftverkehr auswirken können).*

Beispiele für Risikomanagementrahmen: Verschiedene Rahmen (z. B. die Normen der Reihe ISO/IEC 27000, der NIST-Rahmen für Cybersicherheit, der MITRE ATT&CK-Rahmen, der BSI IT-Grundschutz usw.) können als Grundlage für ein maßgeschneidertes Risikomanagementkonzept für den Luftverkehr dienen. Internationale Organisationen wie die IATA und die ICAO stellen Leitlinien für die Bewertung von Cybersicherheitsrisiken bereit. Weitere Informationen zu bewährten Verfahren für die Sicherheit von Flughäfen, Flugverkehrsmanagementanbietern und anderen Luftfahrtorganisationen sind unter anderem von der ENISA, EASA, Eurocontrol und dem Airports Council International (ACI) erhältlich. Das gemeinsame Unternehmen SESAR koordiniert und bündelt alle Forschungs- und Entwicklungstätigkeiten der EU im Bereich des Flugverkehrsmanagements, die auch Sicherheitsaspekte abdecken.



Schutz vor Bedrohungen durch Cyberkriminalität

Luftverkehrsorganisationen sollten angemessene und verhältnismäßige Schutzmaßnahmen treffen, um ihre Netz- und Informationssysteme – einschließlich Informationstechnik (IT) und operativer Technik (OT) – vor Cyberangriffen zu schützen. Zu den Schutzmaßnahmen gehören:

- **Sicherheitsregeln und -verfahren:** Festlegung, Umsetzung, Kommunikation und Durchsetzung geeigneter Sicherheitsregeln und -verfahren im Rahmen eines Gesamtkonzepts zum Schutz von Systemen und Daten, die für den Betrieb der wesentlichen Funktionen im Luftverkehr erforderlich sind. Diese Sicherheitsregeln und -verfahren (z. B. für Passwörter und Datenspeicherung) sollten auch das Management von Patches und Schwachstellen von Hardware- und Softwaresystemen (einschließlich IT und OT), das Management von Sicherheitsvorfällen sowie den Schutz von Systemen und Netzen umfassen.
- **Identitäts- und Zugangsmanagement:** Verständnis, Dokumentation und Verwaltung des Zugangs zu Netz- und Informationssystemen (einschließlich IT und OT), die für den

Betrieb der wesentlichen Funktionen im Luftverkehr erforderlich sind. Benutzer (oder automatisierte Funktionen), die auf Daten oder Systeme zugreifen können, werden in geeigneter Weise überprüft, authentifiziert und autorisiert. Dabei sollten auch die unterschiedlichen Funktionen und Verantwortlichkeiten für reguläre und privilegierte Konten berücksichtigt werden.

- **Daten- und Systemsicherheit:** Schutz von (gespeicherten und elektronisch übermittelten) Daten, kritischen Netz- und Informationssystemen (einschließlich IT und OT) vor Cyberangriffen. Die Organisationen sollten risikoorientierte Schutzmaßnahmen treffen, um die Möglichkeiten für Angreifer, Daten, Netze und Systeme zu kompromittieren, wirksam zu begrenzen. Diese Schutzmaßnahmen sollten auch Verschlüsselungsmechanismen und sichere Kommunikationsprotokolle umfassen, damit sowohl ruhende Daten als auch Daten während der Übertragung vor Bedrohungen der Cybersicherheit durch Man-in-the-Middle-Angriffe geschützt sind. Um den Zugang zu den Systemen zu schützen, müssen zudem physische Sicherheitsmaßnahmen

ergriffen werden (z. B. sollten die Systeme in abgeschlossenen Räumen mit beschränktem Zugang untergebracht werden).

- **Resilienz von Netzen und Systemen:** Stärkung der Resilienz von Netzen und Systemen (IT und OT) durch eine entsprechende Konzeption und Umsetzung der Netze und Systeme (einschließlich der operativen Verfahren), mit dem Ziel, den Auswirkungen von Cyberangriffen zu widerstehen und diese einzudämmen. Einige Beispiele für geeignete Maßnahmen, mit denen Netze und Systeme resilienter werden, sind formell verifizierte kritische Funktionen, redundante Systeme und Netze, getrennte Netze (insbesondere die Trennung von IT und OT), mehrschichtige Schutzmaßnahmen usw. Aus Sicht der Informationssicherheit können Sicherheitsdomänen, mit denen Netze und Systeme voneinander getrennt werden, eine geeignete Sicherheitslösung darstellen. Aus betrieblichen Gründen (z. B. Wartungsarbeiten, Datenübertragungen usw.) kann es jedoch erforderlich sein, verschiedene Sicherheitsdomänen (z. B. getrennte Systeme und Netze) zu umgehen oder diese miteinander zu verbinden, einschließlich der Verbindung von IT und OT.

Erkennen von Bedrohungen der Cybersicherheit

Die Organisationen sollten sicherstellen, dass die Schutzmaßnahmen wirksam bleiben, und alle Ereignisse im Bereich der Cybersicherheit erkennen, die die Sicherheitskontrollen sowie wesentliche Dienste und Systeme beeinträchtigen oder beeinträchtigen könnten. Um Bedrohungen der Cybersicherheit zu erkennen, sind entsprechende Schutzmaßnahmen erforderlich:

■ **Sicherheitsüberwachung:** Überwachung des Sicherheitsstatus von Netz- und Informationssystemen – einschließlich Informationstechnik (IT) und operativer Technik (OT) –, die für den Betrieb der wesentlichen Funktionen im Luftverkehr erforderlich sind. Bei der Sicherheitsüberwachung werden unter anderem die folgenden Daten berücksichtigt:

- Sicherheitsprotokolle
- Virenerkennungsprotokolle

- Protokolle zur Angriffserkennung
- Identifizierungs-, Authentifizierungs- und Autorisierungsprotokolle
- System- und Dienstprotokolle
- Protokolle über den Netzwerkdatenverkehr
- Datenverarbeitungsprotokolle

■ **Entdeckung von Sicherheitsereignissen:** Erkennung böswilliger Aktivitäten (d. h. von Sicherheitsereignissen), die die Sicherheit von Netz- und Informationssystemen (einschließlich IT und OT), die für den Betrieb der wesentlichen Funktionen im Luftverkehr erforderlich sind, beeinträchtigen oder beeinträchtigen können.

In diesem Zusammenhang kann der Einsatz besonderer Technik (z. B. Management von Sicherheitsinformationen und -ereignissen (SIEM), Angriffserkennungssystem (IDS) oder

Angriffsverhinderungssystem (IPS)) und die Einrichtung eines Sicherheitseinsatzzentrums (*Security Operations Centre – SOC*) oder ähnlicher Einrichtungen – erforderlich sein. Das bedeutet, dass vor Ort Instrumente zur Erkennung, Analyse, Reaktion und Wiederherstellung nach Cyberangriffen entwickelt werden.

Nationale CSIRTs (*Computer Security Incident Response Team*), sektorspezifische CERTs (wie das IT-Notfallteam des europäischen Flugverkehrsmanagementsystems (EATM-CERT) von Eurocontrol), kommerzielle CERTs von Fluggesellschaften oder das Informationsaustausch- und Analysezentrum für den Luftverkehr (A-ISAC) können Informationen über Cyberbedrohungen zur Sicherheitsüberwachung und Aufdeckung von Sicherheitsereignissen bereitstellen.

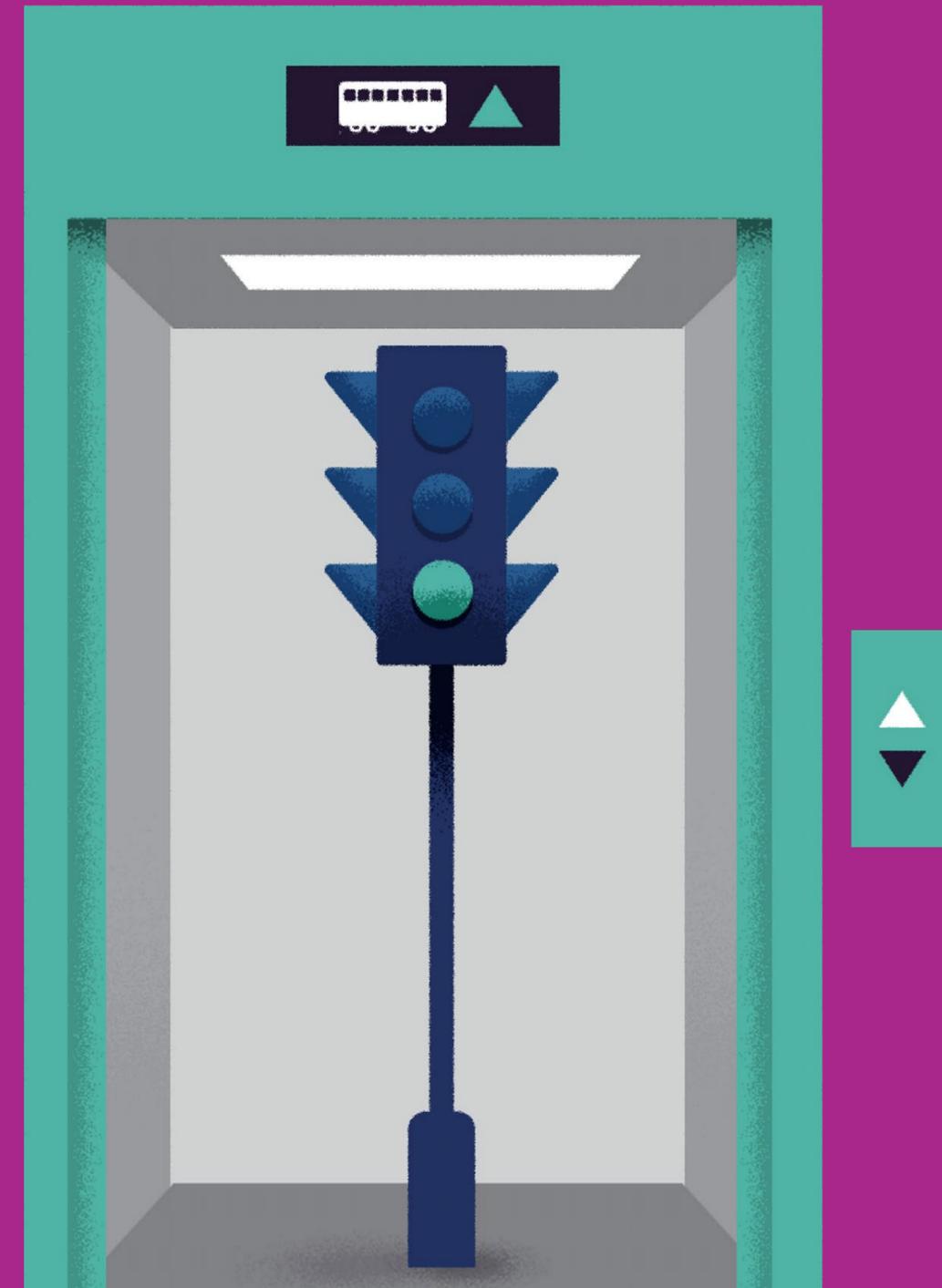
Reaktions- und Wiederherstellungsplanung

Die Organisationen sollten Verfahren für das Management von Vorfällen im Bereich der Cybersicherheit festlegen, umsetzen und testen, um die Kontinuität von Diensten und Systemen bei Vorfällen zu gewährleisten. Mit Maßnahmen zur Eindämmung sollen die Auswirkungen von Cybervorfällen eingedämmt oder begrenzt werden.

Bei der Reaktions- und Wiederherstellungsplanung sollten Schutzmaßnahmen berücksichtigt werden, die die Auswirkungen bestimmter Angriffe auf die Cybersicherheit eindämmen, wie zum Beispiel folgende:

- *Koordinierung und Zusammenarbeit mit nationalen CSIRTs, (öffentlichen und kommerziellen) CERTs und ISACs bei Cybervorfällen, Koordinierung von Vorfällen und Krisen auf gesamteuropäischer Ebene*
- *Informationsaustausch mit anderen Organisationen, auch mit Anbietern in der Lieferkette der Luftverkehrsdienstleistungen*
- *Durchführung regelmäßiger **Übungen für Cyberangriffe** (Planübungen, Koordinierungsübungen und technische Übungen) zur Bewertung der Schutzmaßnahmen und -verfahren sowie der Widerstandsfähigkeit der Organisation im Umgang mit Cybervorfällen*
- *Zugang zu Archivdaten oder Sicherungskopien für den Fall, dass die Integrität und Verfügbarkeit von Datenspeichern beeinträchtigt ist*
- ***Sicherheitskonzepte** mit detaillierten Verfahren für den Umgang mit Cybervorfällen und die Wiederherstellung der normalen Betriebsbedingungen für Dienste und Systeme*
- *Umleitung des Netzwerkdatenverkehrs auf redundante Dienste bei Denial-of-Service-Angriffen*
- *Manuelle Verfahren für den Betrieb von Diensten und Systemen in eingeschränktem Betriebsmodus*
- *Festlegung von Verfahren für den Umgang mit Datenschutzverletzungen, insbesondere solchen, die personenbezogene Daten betreffen, im Einklang mit der Datenschutzgrundverordnung (DSVGO) und anderen einschlägigen sektorspezifischen Verordnungen oder Richtlinien*
- *Abschluss einer **Versicherung gegen Cyberangriffe**, die das Risiko schwerer Cybervorfälle zumindest teilweise abdeckt*
- *Abschluss eines Vertrages mit einem oder mehreren auf die Bewältigung von Cybervorfällen spezialisierten Unternehmen, um bei einem Cybervorfall auf zusätzliche Kapazitäten und Fachkenntnisse zugreifen zu können*
- *Festlegung von Verfahren für den **Informationsaustausch über Cybervorfälle** mit relevanten Interessenträgern, einschließlich Verfahren für die Meldung von Vorfällen gemäß der NIS-Richtlinie (Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union)*

Bewährte Verfahren und Schutzmaßnahmen für den Landverkehr



Governance

Organisationen im Landverkehr (Schiene und Straße) benötigen genaue Kenntnisse über neue Bedrohungen, bevor sie Strategien und Verfahren zur Verbesserung der Cybersicherheit von Diensten und Systemen im Betrieb, einschließlich der Informationstechnik (IT) und operativer Technik (OT), festlegen können.

Zu den bewährten Verfahren für Organisationen jeder Größe gehören:

- *die Sicherstellung, dass die oberste Führungsebene Bedenken hinsichtlich der Cybersicherheit an die Geschäftsleitung und den Vorstand meldet, damit diese fundierte Entscheidungen über die Zuweisung von Ressourcen treffen können,*
- *die Ernennung eines leitenden Beauftragten, der sowohl für die Cybersicherheit als auch für die physische Sicherheit verantwortlich ist und die Gesamtverantwortung*

für die Sicherheit der Informationstechnik (IT) und der operativen Technik (OT) trägt, jedoch zur Vermeidung von Interessenkonflikten nicht in den operativen Betrieb eingebunden ist,

- *die eindeutige Festlegung von Funktionen, Verantwortlichkeiten, Zuständigkeiten und Freigaben im Zusammenhang mit der Cybersicherheit und deren Kommunikation an und Absprache mit den betreffenden Mitarbeitern; dies ist insbesondere für Mitglieder von IT-Notfallteams (CERTs) erforderlich,*
- *die Sicherstellung einer Governance im Bereich der Cybersicherheit für die gesamte Kette der Sicherheitsdienstleistungen, einschließlich der physischen und digitalen Schnittstellen, von den Technologieherstellern und Installationsbetrieben bis hin zu den Sicherheitsanbietern,*

- *die Festlegung von Maßnahmen und Kontrollen, einschließlich gemeinsamer Verantwortlichkeiten, zur Beherrschung von Cybersicherheitsrisiken und die Gewährleistung, dass diese Verantwortlichkeiten während der gesamten Lebensdauer von Sicherheitslösungen und -diensten aufrechterhalten werden (z. B. durch Dienstleistungsverträge),*
- *die Festlegung von Governance-Mechanismen (z. B. Strategien) zur Einhaltung der Verpflichtungen aus den maßgeblichen Verordnungen und Richtlinien. Diese umfassen eine Vielzahl von Strategien, die die einzelnen Verkehrsträger sowie verschiedene Arten von Interessenträgern (z. B. auch Hersteller von Fahrzeugen und Schienenverkehrssystemen) abdecken, sowie die NIS-Richtlinie (Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen).*

Beispiele für Dienste und Systeme im Landverkehr:

Beispiele für IT sind Geräte, die sowohl für das Personal (z. B. PCs, Mobiltelefone, Büroperipheriegeräte usw.) als auch für Passagiere/Fahrgäste (z. B. öffentliche Wi-Fi-Router und -Anschlüsse usw.) zugänglich sind. Beispiele für OT sind Prozesssteuerungs- und Datenerfassungssysteme (SCADA), Heizungs-, Lüftungs- und Klimaanlage, globale Ortungssysteme (GPS), Zugangskontroll-, Überwachungs-, Alarm- und Durchleuchtungssysteme. Spezifische Systeme für den Schienenverkehr sind beispielsweise operative Systeme (Zugsicherungs-, Zugsteuerungs- und Signalgebungssysteme), das Europäische Eisenbahnverkehrsleitsystem (ERTMS), fahrzeugseitige Systeme oder Instandhaltungssysteme.



Feststellung von Bedrohungen durch Cyberkriminalität

Risikomanagement: Um die Risiken für die Cybersicherheit der Netz- und Informationssysteme, die für den Betrieb der wesentlichen Funktionen erforderlich sind, festzustellen, zu bewerten und richtig einzuschätzen, müssen die Landverkehrsorganisationen geeignete Maßnahmen ergreifen. Dies setzt einen organisationsweiten Risikomanagementansatz voraus, der Folgendes umfasst:

- *Bestandsaufnahme der verschiedenen Hardware- und Softwaresysteme, die für die Erbringung der verschiedenen Dienste eingesetzt werden: Im Landverkehr umfassen diese Systeme sowohl die Informationstechnik (IT) als auch die operative Technik (OT).*

- **Bewertung der Risiken im Bereich der Cybersicherheit** unter Berücksichtigung neuer Bedrohungen, bekannter Schwachstellen und operativer Daten in Bezug auf die betroffenen Systeme. Zu den im Landverkehr eingesetzten Systemen gehören beispielsweise

Zahlungssysteme, Netz- und Kommunikationssysteme (z. B. Internet, Funk, WiFi usw.), Bordausrüstung, Betriebsleitstellen, Identitätsmanagementsysteme oder Sicherheitssysteme. Systeme für die Schienenverkehrsinfrastruktur sind beispielsweise Fahrzeuge, Teilsysteme für Verkehrsbetrieb und Verkehrsmanagement, fahrzeugseitige und streckenseitige Zugsteuerungs-, Zugsicherungs- und Signalgebungsteilsysteme.

- *Sicherstellung, dass die Risikobewertungen auch die Risiken im Zusammenhang mit dem beruflichen Alltag der Mitarbeiter berücksichtigen (z. B. Nutzung sozialer Medien, Nutzung persönlicher Geräte, Datenverarbeitung, Informationsaustausch usw.)*

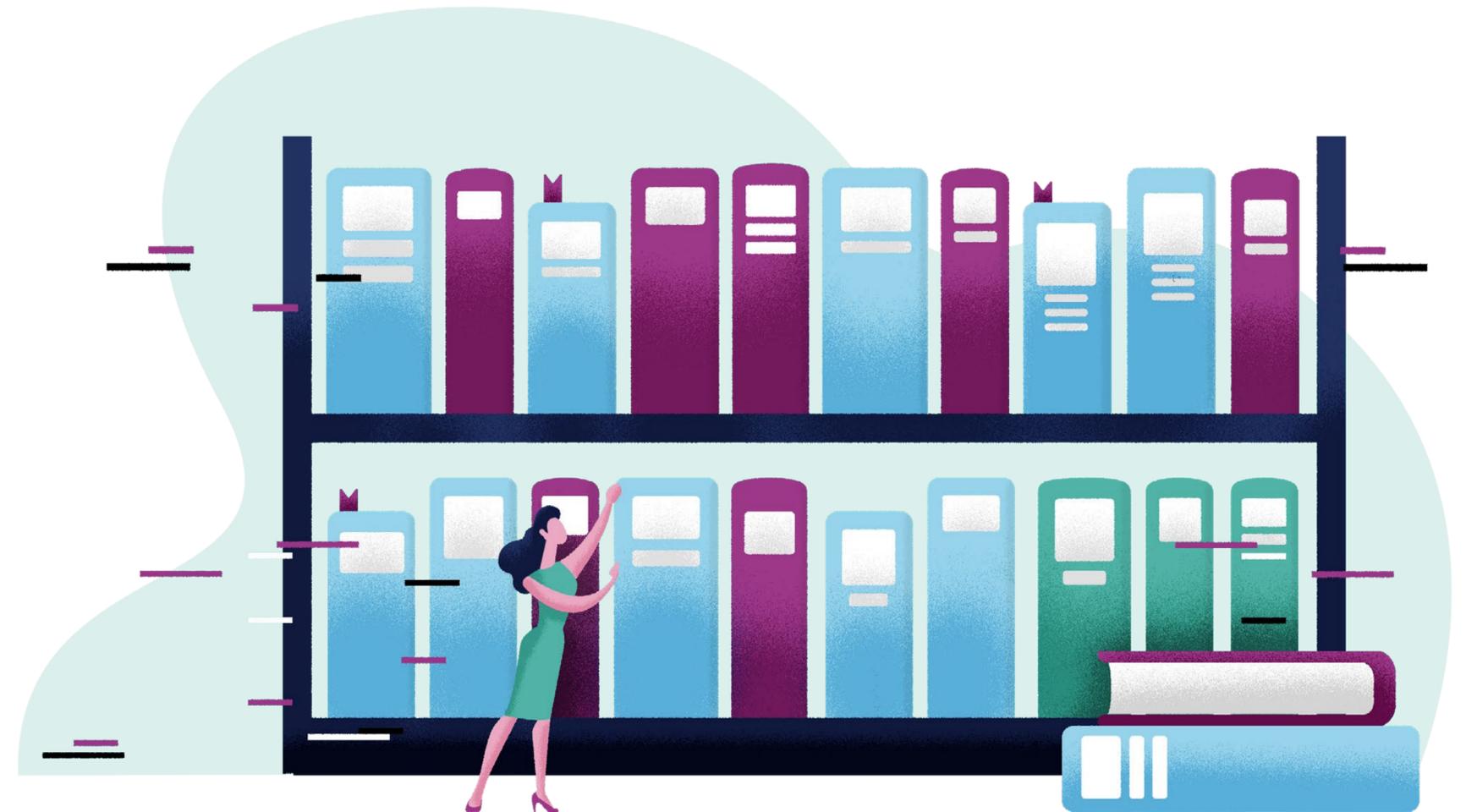
- *Feststellung und Umsetzung von Maßnahmen zur Risikobeherrschung und von Plänen zur Eindämmung von Cybersicherheitsrisiken, beispielsweise durch Einführung eines umfassenden **Managementsystems***

für Informationssicherheit (ISMS) und eines Datenschutzmanagementsystems (PIMS), das mit anderen Managementsystemen abgestimmt ist. Diese Managementsysteme (d. h. ISMS und PIMS) umfassen die Umsetzung von Sicherheitskontrollen (sowie Kontrollen des Datenschutzes und des Schutzes der Privatsphäre), um neue Bedrohungen für die Sicherheit von Diensten und Systemen im Landverkehr (einschließlich ihrer Daten) einzudämmen und zu verhindern.

- *Berücksichtigung aller Beschränkungen im Zusammenhang mit der **Anlagenverwaltung und Ressourcenplanung** (d. h. Beschränkungen, die sich auf die Bereitstellung, Wartung und Unterstützung kritischer Systeme für den Betrieb wesentlicher Funktionen im Landverkehr auswirken können).*

Beispiele für Risikomanagementrahmen: Verschiedene Rahmen (z. B. die Normen der Reihe ISO/IEC 27000, der NIST-Rahmen für Cybersicherheit, der MITRE ATT&CK-Rahmen, der BSI IT-Grundschutz usw.) können als Grundlage für ein maßgeschneidertes Risikomanagementkonzept für den Straßen- und Schienenverkehr dienen.

Organisationen wie die ENISA legen bewährte Verfahren für die Cybersicherheit von intelligenten Fahrzeugen und intelligenten öffentlichen Verkehrsmitteln fest, die den Herstellern und Verbänden der Branche (z. B. dem Europäischen Verband der Automobilhersteller – ACEA) zur Verfügung stehen. Die Eisenbahnagentur der Europäischen Union (ERA) legt für den Schienenverkehr Technische Spezifikationen für die Interoperabilität (TSI) fest, die zur Erfüllung der grundlegenden Anforderungen und zur Gewährleistung der Interoperabilität des Eisenbahnsystems der Europäischen Union von jedem Teilsystem oder Teilbereich des Teilsystems erfüllt werden müssen. Das gemeinsame Unternehmen Shift2Rail bringt zudem Innovationsinitiativen und -projekte (auch im Bereich der Cybersicherheit) für den Schienenverkehr voran.



Schutz vor Bedrohungen durch Cyberkriminalität

Organisationen im Landverkehr sollten angemessene und verhältnismäßige Schutzmaßnahmen treffen, um ihre Netz- und Informationssysteme – einschließlich Informationstechnik (IT) und operativer Technik (OT) – vor Cyberangriffen zu schützen. Zu den Schutzmaßnahmen gehören:

- **Sicherheitsregeln und -verfahren:** Festlegung, Umsetzung, Kommunikation und Durchsetzung geeigneter Sicherheitsregeln und -verfahren im Rahmen eines Gesamtkonzepts zum Schutz von Systemen und Daten, die für den Betrieb der wesentlichen Funktionen im Landverkehr erforderlich sind. Diese Sicherheitsregeln und -verfahren (z. B. für Passwörter und Datenspeicherung) sollten auch das Management von Patches und Schwachstellen von Hardware- und Softwaresystemen (einschließlich IT und OT), das Management von Sicherheitsvorfällen sowie den Schutz von Systemen und Netzen umfassen.
- **Identitäts- und Zugangsmanagement:** Verständnis, Dokumentation und Verwaltung des Zugangs zu Netz- und Informationssystemen (einschließlich IT und OT), die für den Betrieb der wesentlichen Funktionen im Landverkehr erforderlich

sind. Benutzer (oder automatisierte Funktionen), die auf Daten oder Systeme zugreifen können, werden in geeigneter Weise überprüft, authentifiziert und autorisiert. Dabei sollten auch die unterschiedlichen Funktionen und Verantwortlichkeiten für reguläre und privilegierte Konten berücksichtigt werden.

- **Daten- und Systemsicherheit:** Schutz von (gespeicherten und elektronisch übermittelten) Daten, kritischen Netz- und Informationssystemen (einschließlich IT und OT) vor Cyberangriffen. Die Organisationen sollten risikoorientierte Schutzmaßnahmen treffen, um die Möglichkeiten für Angreifer, Daten, Netze und Systeme zu kompromittieren, wirksam zu begrenzen. Diese Schutzmaßnahmen sollten auch Verschlüsselungsmechanismen und sichere Kommunikationsprotokolle umfassen, damit sowohl ruhende Daten als auch Daten während der Übertragung vor Bedrohungen der Cybersicherheit durch Man-in-the-Middle-Angriffe geschützt sind. Um den Zugang zu den Systemen zu schützen, müssen zudem physische Sicherheitsmaßnahmen ergriffen werden (z. B. sollten die Systeme in abgeschlossenen Räumen mit beschränktem Zugang untergebracht werden). Dies

ist besonders wichtig für Systeme, die für die Sicherheit des menschlichen Lebens von Bedeutung sein können.

- **Resilienz von Netzen und Systemen:** Stärkung der Resilienz von Netzen und Systemen (IT und OT) durch eine entsprechende Konzeption und Umsetzung der Netze und Systeme (einschließlich der operativen Verfahren), mit dem Ziel, den Auswirkungen von Cyberangriffen zu widerstehen und diese einzudämmen. Einige Beispiele für geeignete Maßnahmen, mit denen Netze und Systeme resilienter werden, sind formell verifizierte kritische Funktionen, redundante Systeme und Netze, getrennte Netze (insbesondere die Trennung von IT und OT), mehrschichtige Schutzmaßnahmen usw. Aus Sicht der Informationssicherheit können Sicherheitsdomänen, mit denen Netze und Systeme voneinander getrennt werden, eine geeignete Sicherheitslösung darstellen. Aus betrieblichen Gründen (z. B. Wartungsarbeiten, Datenübertragungen usw.) kann es jedoch erforderlich sein, verschiedene Sicherheitsdomänen (z. B. getrennte Systeme und Netze) zu umgehen oder diese miteinander zu verbinden, einschließlich der Verbindung von IT und OT.

Erkennen von Bedrohungen durch Cyberkriminalität

Die Organisationen sollten sicherstellen, dass die Schutzmaßnahmen wirksam bleiben, und alle Ereignisse im Bereich der Cybersicherheit erkennen, die die Sicherheitskontrollen sowie wesentliche Dienste und Systeme beeinträchtigen oder beeinträchtigen könnten. Um Bedrohungen der Cybersicherheit zu erkennen, sind entsprechende Schutzmaßnahmen erforderlich:

■ **Sicherheitsüberwachung:** Überwachung des Sicherheitsstatus von Netz- und Informationssystemen – einschließlich Informationstechnik (IT) und operativer Technik (OT) –, die für den Betrieb der wesentlichen Funktionen im Landverkehr erforderlich sind. Dies ist notwendig, um potenzielle Sicherheitsbedrohungen zu erkennen und die laufende Wirksamkeit der Schutzmaßnahmen zu überwachen. Bei der Sicherheitsüberwachung werden unter anderem die folgenden Daten berücksichtigt:

- Sicherheitsprotokolle
- Virenerkennungsprotokolle
- Protokolle zur Angriffserkennung
- Identifizierungs-, Authentifizierungs- und Autorisierungsprotokolle
- System- und Dienstprotokolle
- Protokolle über den Netzwerkdatenverkehr
- Datenverarbeitungsprotokolle

■ **Entdeckung von Sicherheitsereignissen:** Erkennung böswilliger Aktivitäten (d. h. von Sicherheitsereignissen), die die Sicherheit von Netz- und Informationssystemen (einschließlich IT und OT), die für den Betrieb der wesentlichen Funktionen erforderlich sind, beeinträchtigen oder beeinträchtigen können.

In diesem Zusammenhang kann der Einsatz besonderer Technik (z. B. Management von Sicherheitsinformationen und -ereignissen (SIEM), Angriffserkennungssystem (IDS) oder Angriffsverhinderungssystem (IPS)) und die Einrichtung eines Sicherheitseinsatzzentrums (Security Operations Centre – SOC) oder ähnlicher Einrichtungen erforderlich sein. Das bedeutet, dass vor Ort Instrumente zur Erkennung, Analyse, Reaktion und Wiederherstellung nach Cyberangriffen entwickelt werden.

Nationale CSIRTs, sektorspezifische und kommerzielle CERTs von Straßen- und Schienenwegbetreibern oder das europäische Informationsaustausch- und Analysezentrum für den Schienenverkehr (ER-ISAC) können Informationen über Cyberbedrohungen zur Sicherheitsüberwachung und Entdeckung von Sicherheitsereignissen bereitstellen.



Reaktions- und Wiederherstellungsplanung

Die Organisationen sollten Verfahren für das Management von Vorfällen im Bereich der Cybersicherheit festlegen, umsetzen und testen, um die Kontinuität von Diensten und Systemen bei Vorfällen zu gewährleisten.

Bei der Reaktions- und Wiederherstellungsplanung sollten Schutzmaßnahmen berücksichtigt werden, die die Auswirkungen bestimmter Angriffe auf die Cybersicherheit eindämmen, wie zum Beispiel folgende:

- *Koordinierung und Zusammenarbeit mit nationalen CSIRTs, (öffentlichen und kommerziellen) CERTs und ISACs bei Cybervorfällen, Koordinierung von Vorfällen und Krisen auf gesamteuropäischer Ebene*
- *Informationsaustausch mit anderen Organisationen, auch mit Anbietern in der Lieferkette der Landverkehrsdienstleistungen*
- *Durchführung regelmäßiger **Übungen für Cyberangriffe** (Planübungen, Koordinierungsübungen und*

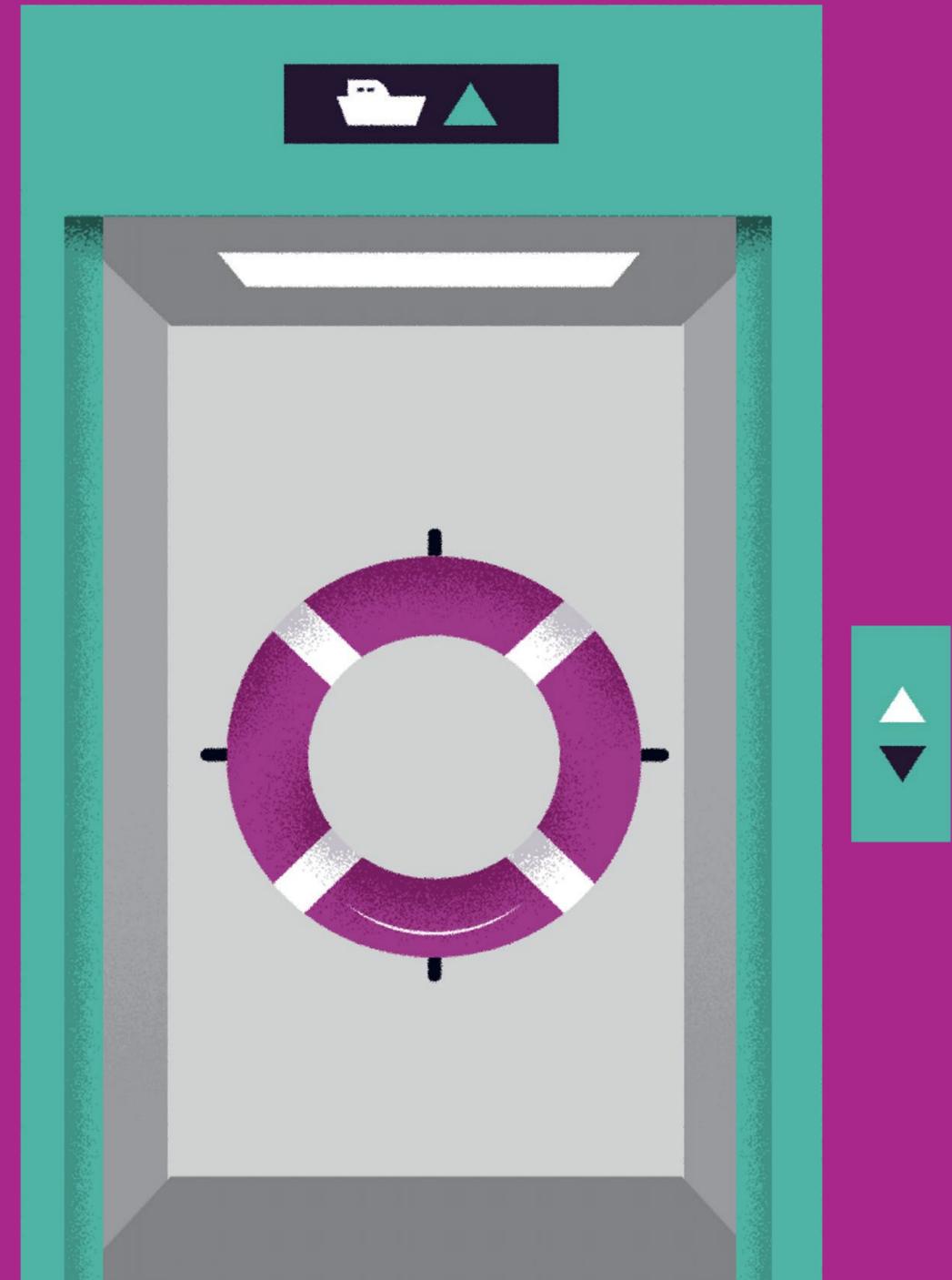
technische Übungen) zur Bewertung der Schutzmaßnahmen und -verfahren sowie der Widerstandsfähigkeit der Organisation im Umgang mit Cybervorfällen

- *Zugang zu Archivdaten oder Sicherungskopien für den Fall, dass die Integrität und Verfügbarkeit von Datenspeichern beeinträchtigt ist*
- ***Sicherheitskonzepte** mit detaillierten Verfahren für den Umgang mit Cybervorfällen und die Wiederherstellung der normalen Betriebsbedingungen für Dienste und Systeme*
- *Umleitung des Netzwerkdatenverkehrs auf redundante Dienste bei Denial-of-Service-Angriffen*
- *Manuelle Verfahren für den Betrieb von Diensten und Systemen in eingeschränktem Betriebsmodus*
- *Festlegung von Verfahren für den Umgang mit Datenschutzverletzungen, insbesondere solchen, die personenbezogene Daten betreffen, im Einklang mit*

der Datenschutzgrundverordnung (DSVGO) und anderen einschlägigen sektorspezifischen Verordnungen oder Richtlinien

- *Abschluss einer **Versicherung gegen Cyberangriffe**, die das Risiko schwerer Cybervorfälle zumindest teilweise abdeckt*
- *Abschluss eines Vertrages mit einem oder mehreren auf die Bewältigung von Cybervorfällen spezialisierten Unternehmen, um bei einem Cybervorfall auf zusätzliche Kapazitäten und Fachkenntnisse zugreifen zu können*
- *Festlegung von Verfahren für den Informationsaustausch über Cybervorfälle mit relevanten Interessenträgern, einschließlich Verfahren für die Meldung von Vorfällen gemäß der NIS-Richtlinie (Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union)*

Bewährte Verfahren und Schutzmaßnahmen im Seeverkehr



Governance

Organisationen im Seeverkehr benötigen genaue Kenntnisse über neue Bedrohungen, bevor sie Strategien und Verfahren zur Verbesserung der Cybersicherheit von Diensten und Systemen im Betrieb, einschließlich Informationstechnik (IT) und operativer Technik (OT), festlegen können.

Zu den bewährten Verfahren für Organisationen jeder Größe gehören:

- die Sicherstellung, dass die oberste Führungsebene Bedenken hinsichtlich der Cybersicherheit an die Geschäftsleitung und den Vorstand meldet, damit diese fundierte Entscheidungen über die Zuweisung von Ressourcen treffen können,
- die Ernennung eines leitenden Beauftragten mit der Gesamtverantwortung für die Sicherheit der Informationstechnik (IT) und der operativen Technik (OT), der sowohl für die Cybersicherheit als auch für die physische Sicherheit verantwortlich ist,
- die eindeutige Festlegung von Funktionen, Verantwortlichkeiten, Zuständigkeiten und Freigaben im Zusammenhang mit der Cybersicherheit, die Definition der

Entscheidungskompetenzen und Kommunikationswege des landseitigen und des bordseitigen Personals und Absprache mit den betreffenden Mitarbeitern. Dies ist insbesondere für die Mitglieder von IT-Notfallteams (CERTs) erforderlich. Mitarbeiter mit Funktionen im Zusammenhang mit den EU-Rechtsvorschriften zur Gefahrenabwehr im Seeverkehr, z. B. die Beauftragten für die Gefahrenabwehr in der Hafenanlage, die Beauftragten für die Gefahrenabwehr im Hafen oder die Beauftragten für die Gefahrenabwehr im Unternehmen oder die benannte Person an Land und der Kapitän an Bord, sollten zumindest mit den von der Organisation ergriffenen Cybersicherheitsmaßnahmen vertraut sein.

- die Sicherstellung einer Governance im Bereich der Cybersicherheit für die gesamte Kette der Sicherheitsdienstleistungen, einschließlich der physischen und digitalen Schnittstellen, von den Technologieherstellern und Installationsbetrieben bis hin zu den Sicherheitsanbietern,
- die Festlegung von Maßnahmen und Kontrollen, einschließlich gemeinsamer Verantwortlichkeiten, zur Beherrschung von Cybersicherheitsrisiken und die Gewährleistung, dass diese Verantwortlichkeiten während der

gesamten Lebensdauer von Sicherheitslösungen und -diensten aufrechterhalten werden (z. B. durch Dienstleistungsverträge),

- die Festlegung von Governance-Mechanismen (z. B. Strategien) zur Einhaltung der Verpflichtungen aus den maßgeblichen Verordnungen und Richtlinien, z. B. der Verordnung (EU) 2019/1239 zur Einrichtung eines europäischen Umfelds zentraler Meldeportale für den Seeverkehr (EMSWe), der Verordnung (EG) Nr. 725/2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen, der Richtlinie 2005/65/EG zur Erhöhung der Gefahrenabwehr in Häfen, der Verordnung (EG) Nr. 336/2006 zur Umsetzung des Internationalen Codes für Maßnahmen zur Organisation eines sicheren Schiffsbetriebs innerhalb der Gemeinschaft (ISM-Codes) und der Entschließung A.741 (18) zur Annahme des ISM-Codes für den sicheren Schiffsbetrieb und zur Verhütung der Meeresverschmutzung. In diesem Zusammenhang ist auch der Gemeinsame Informationsraum (CISE) zu erwähnen, eine EU-Initiative, die darauf abzielt, die Überwachungssysteme der EU und der Mitgliedstaaten interoperabel zu machen, damit alle betroffenen Behörden Zugang zu den als Verschlusssache eingestuft und nicht als Verschlusssache eingestuften Informationen erhalten, die sie zur Durchführung von Einsätzen auf See benötigen.

Beispiele für Dienste und Systeme im Seeverkehr:

Beispiele für IT sind Geräte, die sowohl für das Personal (z. B. PCs, Mobiltelefone, Büroperipheriegeräte usw.) als auch für Passagiere/Fahrgäste (z. B. öffentliche Wi-Fi-Router und -Anschlüsse usw.) zugänglich sind. Beispiele für OT sind Prozesssteuerungs- und Datenerfassungssysteme (SCADA), Heizungs-, Lüftungs- und Klimaanlage, globale Ortungssysteme (GPS), Zugangskontroll-, Überwachungs-, Alarm- und Durchleuchtungssysteme, Bordnavigationssysteme, SafeSeaNet, Brückensysteme, Frachtabfertigungs- und -managementsysteme, Systeme für Antriebs- und Maschinenmanagement und Leistungsregelung, Zugangskontrollsysteme, Passagierabfertigungs- und -managementsysteme, öffentliche Netze für Passagiere, Verwaltungssysteme und Systeme für die Schiffsbesatzung, Kommunikationssysteme usw.



Feststellung von Bedrohungen durch Cyberkriminalität

Risikomanagement: Seeverkehrsorganisationen müssen geeignete Schritte unternehmen, um Cybersicherheitsrisiken zu ermitteln, zu analysieren, zu bewerten und zu kommunizieren und diese Risiken zu akzeptieren, zu vermeiden, zu übertragen oder auf ein akzeptables Maß zu reduzieren. Dies setzt einen organisationsweiten Risikomanagementansatz voraus, der Folgendes umfasst:

- *Bestandsaufnahme der verschiedenen Hardware- und Softwaresysteme, die für die Erbringung der verschiedenen Dienste eingesetzt werden: Im Seeverkehr umfassen diese Systeme sowohl die Informationstechnik (IT) als auch die operative Technik (OT) und die Art und Weise, wie diese Systeme mit der Landseite, einschließlich Behörden, Hafenterminals und Stauereibetrieben, vernetzt und integriert werden.*
- *Ermittlung und Beurteilung wichtiger betrieblicher Vorgänge an Bord, die für Cyberangriffe anfällig sind, Durchführung von Risikobewertungen in Bezug auf die Cybersicherheit (einschließlich einer Bewertung der potenziellen betrieblichen Auswirkungen und der Eintrittswahrscheinlichkeit) unter Berücksichtigung neuer Bedrohungen, bekannter Schwachstellen und operativer Daten in Zusammenhang*

mit den betroffenen Systemen, dabei ist gegebenenfalls auf die Bewertungen zur Gefahrenabwehr zu verweisen, die für Schiffe (SSA), Hafenanlagen (PFSA) und Häfen (PSA) gemäß den EU-Rechtsvorschriften zur Gefahrenabwehr im Seeverkehr durchgeführt werden. Bei diesen Bewertungen werden mögliche Sicherheitsbedrohungen für die Hafeninfrastruktur und Schwachstellen in Bezug auf die Gefahrenabwehr ermittelt. Darüber hinaus können Seeverkehrsorganisationen wie die Internationale Seeschifffahrtsorganisation (IMO) und Informationsaustausch- und Analysezentren (ISACs) Informationen über Bedrohungen für den Seeverkehr bereitstellen.

- *Sicherstellung, dass die Risikobewertungen auch die Risiken im Zusammenhang mit dem beruflichen Alltag der Mitarbeiter berücksichtigen (z. B. Nutzung sozialer Medien, Nutzung persönlicher Geräte, Datenverarbeitung, Informationsaustausch usw.)*
- *Feststellung und Umsetzung von Maßnahmen zur Risikobeherrschung und von Plänen zur Eindämmung von Cybersicherheitsrisiken, beispielsweise durch Einführung eines umfassenden Managementsystems für Informationssicherheit*

(ISMS) und eines Datenschutzmanagementsystems (PIMS), die mit anderen Managementsystemen wie etwa einem Sicherheitsmanagementsystem (SMS) gemäß dem Internationalen Code für Maßnahmen zur Organisation eines sicheren Schiffsbetriebs (ISM-Code) abgestimmt sind. Diese Managementsysteme (d. h. ISMS und PIMS) umfassen die Umsetzung von Sicherheitskontrollen (sowie Kontrollen des Datenschutzes und des Schutzes der Privatsphäre), um neue Bedrohungen für die Sicherheit von Seeverkehrsdiensten und -systemen (einschließlich ihrer Daten) einzudämmen und zu verhindern.

- *Berücksichtigung aller Beschränkungen im Zusammenhang mit der **Anlagenverwaltung und Ressourcenplanung** (d. h. Beschränkungen, die sich auf die Bereitstellung, Wartung und Unterstützung kritischer Systeme für den Betrieb wesentlicher Funktionen im Seeverkehr auswirken können). Bei den Bewertungen ist gegebenenfalls auf die Anforderungen des ISM-Codes, der Sicherheitsmanagementsysteme (SMS) und der Pläne zur Gefahrenabwehr gemäß den EU-Rechtsvorschriften zur Sicherheit und Gefahrenabwehr im Seeverkehr zu verweisen.*

Beispiele für Risikomanagementrahmen: Verschiedene Rahmen (z. B. der ISM-Code die Normen der Reihe ISO/IEC 27000, der NIST-Rahmen für Cybersicherheit, der MITRE ATT&CK-Rahmen, der BSI IT-Grundschutz usw.) können als Grundlage für ein maßgeschneidertes Risikomanagementkonzept für den Seeverkehr dienen. Der NIST-Rahmen für Cybersicherheit ist auch auf die Cybersicherheit der Beförderung von flüssigem Massengut auf See, den Offshore-Betrieb und den Betrieb von Fahrgastschiffen zugeschnitten. Ferner hat der Baltic and International Maritime Council (BIMCO) Leitlinien für die Cybersicherheit an Bord von Schiffen („*The Guidelines on Cyber Security Onboard Ships*“) herausgegeben, und die Internationale Seeschiffahrtsorganisation (IMO) hat besondere Leitlinien für ein maritimes Cyberrisikomanagement („*Guidelines on maritime cyber risk management*“) (MSC-FAL.1/Circ.3) veröffentlicht. Die ENISA hat mehrere Studien über bewährte Verfahren für die Cybersicherheit im Seeverkehr, insbesondere für die Cybersicherheit in Hafenanlagen, durchgeführt. Die EMSA bietet Dienstleistungen für die Seeverkehrsgemeinschaft an, darunter auch Schulungen zum Thema Cybersicherheit. In Normen (z. B. IEC 61162-460:2018 über die Sicherheit von Navigations- und Funkkommunikationsgeräten und -systemen für die Seeschiffahrt, ISO 16425:2013 über Schiffe und Meerestechnik, IEC 62443-4-1:2018 über die Sicherheit von industriellen Automatisierungs- und Steuerungssystemen usw.) werden ebenfalls besondere Sicherheitsanforderungen für Systeme und Netze im Seeverkehr festgelegt.



Schutz vor Bedrohungen durch Cyberkriminalität

Organisationen im Seeverkehr sollten angemessene und verhältnismäßige Schutzmaßnahmen treffen, um ihre Netz- und Informationssysteme – einschließlich Informationstechnik (IT) und operativer Technik (OT) – vor Cyberangriffen zu schützen. Zu den Schutzmaßnahmen gehören:

■ **Sicherheitsregeln und -verfahren:** Festlegung, Umsetzung, Kommunikation und Durchsetzung geeigneter Sicherheitsregeln und -verfahren im Rahmen eines Gesamtkonzepts zum Schutz von Systemen und Daten, die für den Betrieb der wesentlichen Funktionen im Seeverkehr erforderlich sind. Die einschlägigen Pläne wie etwa das Sicherheitsmanagementsystem (SMS) oder der Plan zur Gefahrenabwehr für das Schiff (SSP) sollten Schutzmaßnahmen umfassen, die sowohl die Cybersicherheit als auch die physische Sicherheit betreffen. Diese Sicherheitsregeln und -verfahren (z. B. für Passwörter und Datenspeicherung) sollten auch das Management von Patches und Schwachstellen von Hardware- und Softwaresystemen (einschließlich IT und OT), das Management von Sicherheitsvorfällen sowie den Schutz von Systemen und Netzen umfassen.

■ **Identitäts- und Zugangsmanagement:** Verständnis, Dokumentation und Verwaltung des Zugangs zu Netz- und

Informationssystemen (einschließlich IT und OT), die für den Betrieb der wesentlichen Funktionen im Seeverkehr erforderlich sind. Benutzer (oder automatisierte Funktionen), die auf Daten oder Systeme zugreifen können, werden in geeigneter Weise überprüft, authentifiziert und autorisiert. Dabei sollten auch die unterschiedlichen Funktionen und Verantwortlichkeiten für reguläre und privilegierte Konten berücksichtigt werden.

■ **Daten- und Systemsicherheit:** Schutz von (gespeicherten und elektronisch übermittelten) Daten, kritischen Netz- und Informationssystemen (einschließlich IT und OT) vor Cyberangriffen. Die Organisationen sollten risikoorientierte Schutzmaßnahmen ergreifen, um die Möglichkeiten für Angreifer, Daten, Netze und Systeme zu kompromittieren, wirksam zu begrenzen. Diese Schutzmaßnahmen sollten auch Verschlüsselungsmechanismen und sichere Kommunikationsprotokolle umfassen, damit sowohl ruhende Daten als auch Daten während der Übertragung vor Bedrohungen der Cybersicherheit durch Man-in-the-Middle-Angriffe geschützt sind. Um den Zugang zu den Systemen zu schützen, müssen zudem physische Sicherheitsmaßnahmen ergriffen werden (z. B. sollten die Systeme in abgeschlossenen Räumen mit beschränktem Zugang untergebracht werden). Dies ist besonders wichtig für Systeme, die für die Sicherheit

des menschlichen Lebens von Bedeutung sein können (z. B. Navigations- und Funkkommunikationssysteme der Kategorien II und III).

■ **Resilienz von Netzen und Systemen:** Stärkung der Resilienz von Netzen und Systemen (IT und OT) durch eine entsprechende Konzeption und Umsetzung der Netze und Systeme (einschließlich der operativen Verfahren), mit dem Ziel, den Auswirkungen von Cyberangriffen zu widerstehen und diese einzudämmen. Einige Beispiele für geeignete Maßnahmen, mit denen Netze und Systeme resilienter werden, sind formell verifizierte kritische Funktionen, redundante Systeme und Netze, getrennte Netze (insbesondere die Trennung von IT und OT), mehrschichtige Schutzmaßnahmen usw. Aus Sicht der Informationssicherheit können Sicherheitsdomänen, mit denen Netze und Systeme voneinander getrennt werden, eine geeignete Sicherheitslösung darstellen. Aus betrieblichen Gründen (z. B. Wartungsarbeiten, Datenübertragungen usw.) kann es bei bestimmten Systemen (wie etwa bei autonomen Schiffen (MASS)) jedoch erforderlich sein, verschiedene Sicherheitsdomänen (z. B. getrennte Systeme und Netze) zu umgehen oder diese miteinander zu verbinden, einschließlich der Verbindung von IT und OT.

Erkennen von Bedrohungen durch Cyberkriminalität

Die Organisationen sollten sicherstellen, dass die Schutzmaßnahmen wirksam bleiben, und alle Ereignisse im Bereich der Cybersicherheit erkennen, die die Sicherheitskontrollen sowie wesentliche Dienste und Systeme beeinträchtigen oder beeinträchtigen könnten. Um Bedrohungen der Cybersicherheit zu erkennen, sind entsprechende Schutzmaßnahmen erforderlich:

■ **Sicherheitsüberwachung:** Überwachung des Sicherheitsstatus von Netz- und Informationssystemen – einschließlich Informationstechnik (IT) und operativer Technik (OT) –, die für den Betrieb der wesentlichen Funktionen im Seeverkehr erforderlich sind. Dies ist notwendig, um potenzielle Sicherheitsbedrohungen zu erkennen und die laufende Wirksamkeit der Schutzmaßnahmen zu überwachen. Bei der Sicherheitsüberwachung werden unter anderem die folgenden Daten berücksichtigt:

- Sicherheitsprotokolle
- Virenerkennungsprotokolle

- Protokolle zur Angriffserkennung
- Identifizierungs-, Authentifizierungs- und Autorisierungsprotokolle
- System- und Dienstprotokolle
- Protokolle über den Netzwerkdatenverkehr
- Datenverarbeitungsprotokolle

■ **Entdeckung von Sicherheitsereignissen:** Erkennung böswilliger Aktivitäten (d. h. von Sicherheitsereignissen), die die Sicherheit von Netz- und Informationssystemen (einschließlich IT und OT), die für den Betrieb der wesentlichen Funktionen im Seeverkehr erforderlich sind, beeinträchtigen oder beeinträchtigen können.

In diesem Zusammenhang kann der Einsatz besonderer Technik (z. B. Management von Sicherheitsinformationen und -ereignissen (SIEM), Angriffserkennungssystem (IDS) oder Angriffsverhinderungssystem (IPS)) und die Einrichtung eines Sicherheitseinsatzzentrums (*Security Operations Centre* – SOC) oder ähnlicher Einrichtungen– erforderlich sein. Das

bedeutet, dass auf lokaler Ebene Instrumente zur Erkennung, Analyse, Reaktion und Wiederherstellung nach Cyberangriffen entwickelt werden.

Nationale CSIRTs, sektorspezifische CERTs und kommerzielle CERTs von Seeverkehrsbetreibern oder Informationsaustausch- und Analysezentren (ISACs) für den Seeverkehr können Informationen über Cyberbedrohungen zur Sicherheitsüberwachung und Entdeckung von Sicherheitsereignissen bereitstellen.

Reaktions- und Wiederherstellungsplanung

Die Organisationen sollten Verfahren für das Management von Vorfällen im Bereich der Cybersicherheit festlegen, umsetzen und testen, um die Kontinuität von Diensten und Systemen bei Vorfällen zu gewährleisten.

Bei der Reaktions- und Wiederherstellungsplanung sollten Schutzmaßnahmen berücksichtigt werden, die die Auswirkungen bestimmter Angriffe auf die Cybersicherheit eindämmen, wie zum Beispiel folgende:

- *Umleitung des Netzwerkdatenverkehrs auf redundante Dienste bei Denial-of-Service-Angriffen*
- *Manuelle Verfahren für den Betrieb von Diensten und Systemen in eingeschränktem Betriebsmodus*
- *Einrichtung von Programmen für Schulungen und Übungen (z. B. Planübungen, Koordinierungsübungen, technische Übungen und Reaktionsübungen) zur Reaktion auf Cyberangriffe und Notfälle sowie zur Bewertung der Schutzmaßnahmen, Verfahren*

und der Widerstandsfähigkeit der Organisation gegenüber Cybervorfällen

- *Zugang zu Archivdaten oder Sicherungskopien für den Fall, dass die Integrität und Verfügbarkeit von Datenspeichern beeinträchtigt ist*
- *Koordinierung und Zusammenarbeit mit nationalen CSIRTs, (öffentlichen und kommerziellen) CERTs und ISACs bei Cybervorfällen, Koordinierung von Vorfällen und Krisen auf gesamteuropäischer Ebene*
- *Informationsaustausch mit anderen Organisationen, auch mit Anbietern in der Lieferkette der Seeverkehrsdienstleistungen*
- *Sicherheitskonzepte mit detaillierten Verfahren für den Umgang mit Cybervorfällen und die Wiederherstellung der normalen Betriebsbedingungen für Dienste und Systeme*
- *Festlegung von Verfahren für den Umgang mit Datenschutzverletzungen, insbesondere solchen, die*

personenbezogene Daten betreffen, im Einklang mit der Datenschutzgrundverordnung (DSVGO) und anderen einschlägigen sektorspezifischen Verordnungen oder Richtlinien

- *Abschluss einer Versicherung gegen Cyberangriffe, die das Risiko schwerer Cybervorfälle zumindest teilweise abdeckt*
- *Abschluss eines Vertrages mit einem oder mehreren auf die Bewältigung von Cybervorfällen spezialisierten Unternehmen, um bei einem Cybervorfall auf zusätzliche Kapazitäten und Fachkenntnisse zugreifen zu können*
- *Festlegung von Verfahren für den Informationsaustausch über Cybervorfälle (einschließlich Nichtkonformitäten, Unfälle und Gefahrensituationen) an relevante Interessenträger, einschließlich der Verfahren für die Meldung von Sicherheitsvorfällen gemäß der NIS-Richtlinie (Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union)*

Die in diesem Bericht dargelegten Informationen und Ansichten entsprechen denen des/der Verfasser(s) und geben nicht unbedingt die offizielle Meinung der Kommission wieder. Die Kommission übernimmt keine Gewähr für die Richtigkeit der in diesem Bericht enthaltenen Daten. Weder die Kommission noch in ihrem Namen handelnde Personen können für die Verwendung der in dieser Studie enthaltenen Informationen verantwortlich gemacht werden.

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2021

© Europäische Union, 2021

Die Weiterverwendung ist gestattet, sofern die Quelle angegeben wird und die ursprüngliche Bedeutung oder Aussage des Dokuments nicht verfälscht werden. Die Europäische Kommission haftet nicht für Folgen, die sich aus der Weiterverwendung dieser Veröffentlichung ergeben. Die Weiterverwendung von Dokumenten der Europäischen Kommission ist durch den Beschluss 2011/833/EU der Kommission vom 12. Dezember 2011 über die Weiterverwendung von Kommissionsdokumenten (ABl. L 330 vom 14.12.2011, S. 39) geregelt.

Für jede Verwendung oder Wiedergabe von Elementen, die nicht Eigentum der EU sind, muss gegebenenfalls direkt bei den jeweiligen Rechteinhabern eine Genehmigung eingeholt werden.

Print ISBN 978-92-76-40492-7 doi:10.2832/424826 MI-05-21-230-DE-C
PDF ISBN 978-92-76-40469-9 doi:10.2832/168040 MI-05-21-230-DE-N



Amt für Veröffentlichungen
der Europäischen Union