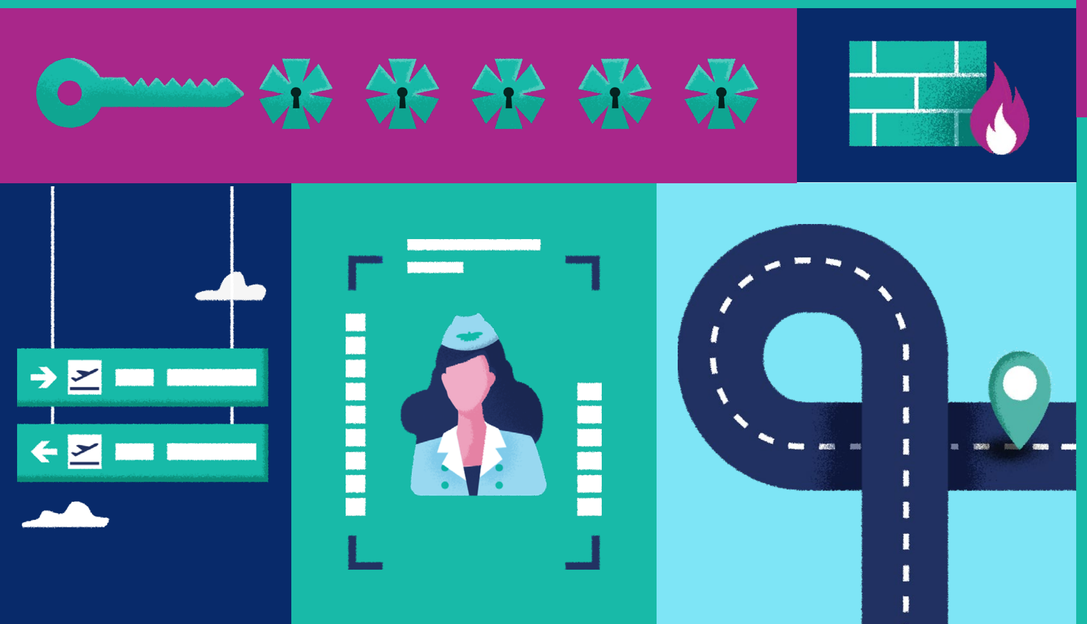
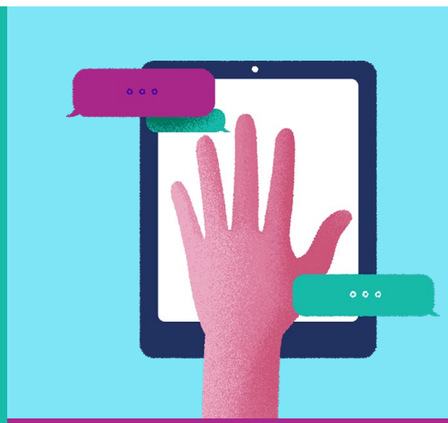
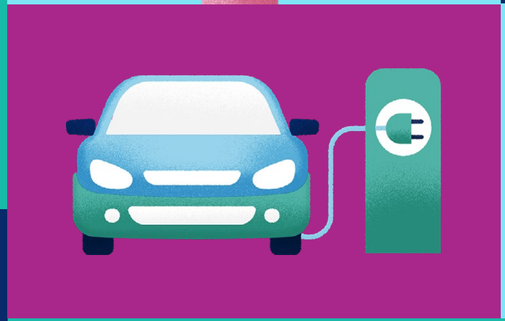
Comissão Europeia

Conjunto de ferramentas de cibersegurança para o setor dos transportes









Introdução

A Direção-Geral da Mobilidade e dos Transportes (DG MOVE) da Comissão Europeia encomendou a elaboração deste conjunto de ferramentas para reforçar a sensibilização e preparação das partes interessadas do setor dos transportes para as ciberameaças. Este fornece informações que permitem compreender as ciberameaças e reduzir o seu impacto. O conjunto de ferramentas fornece duas vias de sensibilização, que correspondem a diferentes perfis:

- Todo o pessoal dos transportes (fornecendo orientações e informação geral);
- Decisores em matéria de cibersegurança no setor dos transportes, nos diferentes modos de transporte.

As hiperligações ligam as diferentes partes que compõem o conjunto de ferramentas, a fim de facilitar a navegação.

As práticas indicadas neste conjunto de ferramentas são exclusivamente de carácter consultivo. Nenhuma das recomendações formuladas é vinculativa ou obrigatória. Além disso, o presente conjunto de ferramentas não representa as opiniões formais da Comissão Europeia e não visa fornecer meios de garantir o cumprimento de legislações atuais ou futuras da UE.

Perfis de sensibilização para a cibersegurança

Perfil I: Todos os agentes de transporte. A primeira via é dirigida a todo o pessoal de organizações de transporte e fornece informações para compreender melhor as ciberameaças mais comuns que visam os transportes. Além disso, aborda a forma de lidar com eventuais ciberameaças, nomeadamente a identificação, comunicação e atenuação das mesmas através de boas práticas no domínio da cibersegurança.

Perfil II: Decisores em matéria de cibersegurança no setor dos transportes. A segunda via dirige-se a pessoal responsável pela tomada de decisões em matéria de cibersegurança nas organizações de transporte. Esta via destaca boas práticas adaptadas aos diferentes modos de transporte. Em particular, fornece boas práticas para identificar, proteger, detetar e responder a ciberameaças emergentes que visam organizações de transporte.

Comissão Europeia

Conjunto de ferramentas de cibersegurança para o setor dos transportes

Cenário de ameaças no setor dos transportes

Ciberameaças emergentes que afetam diferentes modos de transporte

Perfis de sensibilização para a cibersegurança

Vias de sensibilização para a cibersegurança alternativas, que correspondem a diferentes perfis de transporte

Comissão Europeia

Cenário de ameaças no setor dos transportes

O cenário das ciberameaças é dinâmico e está em constante evolução. No entanto, é possível identificar ciberameaças que todos os modos de transporte enfrentam.

Comissão Europeia

Autores de ameaças

Indivíduos ou organizações que podem ter impacto na segurança e na proteção dos serviços e sistemas de transporte

Ciberameaças emergentes

Ciberameaças selecionadas que podem ter impacto na segurança e proteção dos serviços e sistemas de transporte

Autores de ameaças

Indivíduos ou organizações podem, intencional ou involuntariamente, expor e explorar vulnerabilidades suscetíveis de causar incidentes e afetar os serviços de transporte, nomeadamente a sua segurança, proteção, atividade, finanças e reputação.

Os principais agentes maliciosos que visam intencionalmente as organizações de transporte são **cibercriminosos**, **infiltrados**, **Estados-nação** e **grupos paraestatais**. Adversários como **cibercriminosos** realizam campanhas de ataque maciças e frequentemente agem motivados por intenções monetárias.

Os **infiltrados** conhecem as especificidades das organizações para as quais trabalham e frequentemente estão cientes de vulnerabilidades de segurança subtis.

Estes infiltrados podem ser funcionários descontentes, fornecedores e contratantes individuais.
À medida que as tensões geopolíticas internacionais se intensificam, os **Estados-nações** e os **grupos paraestatais** visam objetivos estratégicos a longo prazo. Frequentemente, procuram esconder-se nas profundezas dos sistemas das organizações e recolher informação sensível. Depois de se infiltrarem nos sistemas, os atacantes paraestatais procuram obter uma posição que permita causar o maior dano possível.

Os autores não maliciosos são **infiltrados**, que podem, intencional ou involuntariamente, realizar ações que resultam em eventos de cibersegurança e, no pior dos cenários, ciberincidentes.

Comissão Europeia

Ciberameaças emergentes

Existem várias ciberameaças que visam o setor dos transportes: **negação de serviço distribuída**, **negação de serviço**, roubo de dados, difusão de **programas maliciosos**, **mistificação da interface**, manipulação de *software*, **acesso não autorizado**, ataques destrutivos, falsificação ou contorno de processos deliberativos de operadores de segurança, disfarce de identidade, abuso de privilégios de acesso, **engenharia social**, desfiguração, interceção de mensagens, utilização indevida de ativos e manipulação de *hardware*.

Com base em investigação bibliográfica abrangente de documentos divulgados publicamente e entrevistas com especialistas, as ciberameaças emergentes mais prementes que afetam o setor dos transportes são: Programas maliciosos, (ataque distribuído de) negação de serviço, acesso não autorizado e roubo, e manipulação de *software*.

Comissão Europeia

Ameaça n.º 1: Programas maliciosos

Software mal-intencionado que pode afetar indivíduos ou organizações nos diferentes modos de transporte

Ameaça n.º 2: (Ataque distribuído de) negação de serviço

Ataques de cibersegurança que impedem os indivíduos ou as organizações de aceder a recursos ou serviços de transporte importantes

Ameaça n.º 3: Acesso não autorizado e roubo

Acesso não autorizado, apropriação e exploração de ativos críticos

Ameaça n.º 4: Manipulação de *software*

Ataques de cibersegurança que visam *software* para modificar o seu comportamento e realizar ataques específicos

Ameaça n.º 1: Programas maliciosos

Os programas maliciosos consistem em *software* mal-intencionado, que pode incluir diferentes tipos de aplicações de *software*, como vírus, cavalos de troia, vermes, *software* de sequestro, mineiros de criptomoedas ou qualquer *software* que possa ter um impacto adverso em organizações ou indivíduos nos diferentes modos de transporte.

Reduzir a difusão de programas maliciosos concebidos para danificar intencionalmente computadores, servidores, clientes, redes ou todos estes é uma das principais prioridades no domínio da cibersegurança em todos os modos de transporte. Um vetor de ataque típico pode envolver mensagens de correio eletrónico de *phishing* («ciberiscagem») dirigidos a funcionários. Outros vetores de ataque podem envolver diferentes estratégias de engenharia social sofisticadas, como introduzir uma memória USB numa porta livre (por exemplo, a entrada de carregamento do telemóvel). Ao clicar em hiperligações em mensagens de correio eletrónico suspeitas ou ao abrir ficheiros em anexo, o utilizador pode estar a instalar programas maliciosos inadvertidamente.

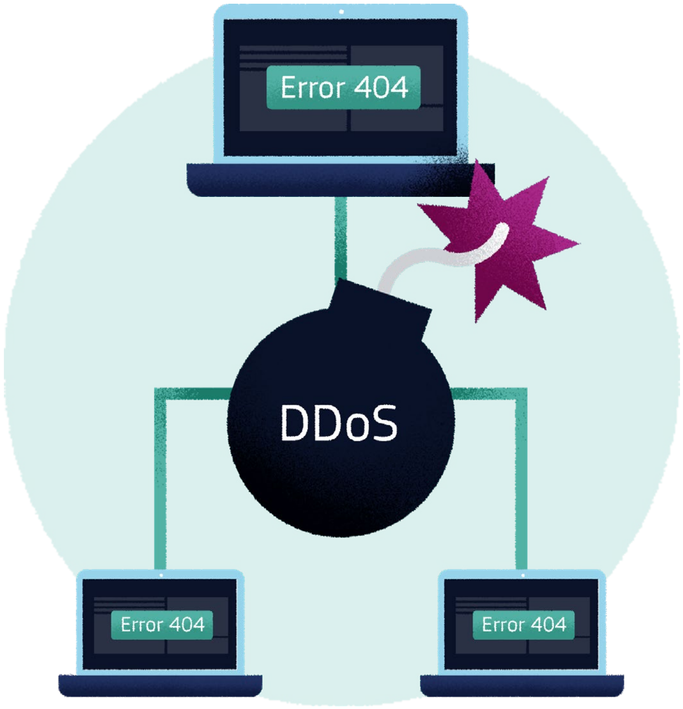
Por exemplo, o ciberataque do *software* de sequestro «WannaCry» afetou mais de 150 países e infetou mais de 230 000 sistemas. Este ataque utilizou um *software* de sequestro habitualmente difundido através de mensagens de correio eletrónico de *phishing* que contêm hiperligações ou anexos maliciosos. Este tipo de ataque explora a engenharia social de forma maliciosa, a fim de induzir os utilizadores do sistema a instalar (ou ativar) um programa malicioso específico.

Ameaça n.º 2: (Ataque distribuído de) negação de serviço

Os ataques distribuídos de negação de serviço (DDoS) e de negação de serviço (DoS) afetam a disponibilidade e a acessibilidade dos dados, serviços, sistemas e outros recursos. Estes tipos de ataque podem ter uma duração variável e visar vários serviços ou sistemas em simultâneo. Os ataques DDoS utilizam vários sistemas (ou canais de ataque) para sobrecarregar os serviços ou sistemas alvo com pedidos. Os ataques bem-sucedidos afetam a capacidade do serviço e do sistema para processar volumes de pedidos imprevistos, o que resulta na negação do acesso a serviços e recursos.

Importa salientar que os serviços e sistemas afetados que pertencem a organizações de transporte podem ser explorados para levar a cabo ataques DDoS e DoS em sistemas alvo específicos nas operações ou noutras organizações.

Por exemplo, os sistemas informáticos empresariais (como dispositivos e computadores pessoais) podem ser alvo de ataque para aceder a tecnologias de operação, que podem estar ligadas à Internet ou aceder a redes para transferir dados operacionais. As ligações entre diferentes sistemas e redes (como redes empresariais, tecnologias de operação e acesso a manutenção remota) podem representar vulnerabilidades suscetíveis de exploração para levar a cabo ataques DDoS ou DoS em serviços e sistemas de transporte críticos. Por exemplo, os ataques DDoS e DoS podem explorar protocolos de comunicação e de rede comuns, como o *Web Services Dynamic Discovery* (WS-Discovery), que os dispositivos da IdC podem utilizar para descobrir automaticamente cada nó nas redes locais (LAN). Se os dispositivos da IdC apresentarem vulnerabilidades, os atacantes podem explorá-las para descobrir outros dispositivos ligados e levar a cabo ataques DDoS e DoS.



Ameaça n.º 3: Acesso não autorizado e roubo

Os autores de ameaças podem procurar obter acesso lógico ou físico não autorizado a uma rede, sistema, aplicação, dados ou outro recurso, a fim de realizar atividades maliciosas, nomeadamente o roubo de dados sensíveis ou recursos (incluindo recursos físicos).
As ameaças de acesso não autorizado e roubo visam ativos confidenciais e proprietários (nomeadamente identidades pessoais, credenciais de contas privilegiadas, sistemas e outros tipos de informação confidencial e proprietária). Estas ameaças podem explorar as vulnerabilidades dos sistemas, bem como indivíduos desprevenidos que revelam dados sensíveis, tais como credenciais (por exemplo, dados de início de sessão, palavras-passe, etc.) ou dados pessoais (por exemplo, correio eletrónico, número de identificação pessoal, etc.).

Relativamente ao acesso não autorizado, o roubo de identidade é a utilização ilícita de dados pessoais ou identificadores únicos para se fazer passar por pessoas ou serviços e sistemas e obter acesso a recursos privados ou proprietários (por exemplo, recursos financeiros e físicos). Estas ciberameaças também podem visar ativos físicos nos diferentes modos de transporte.

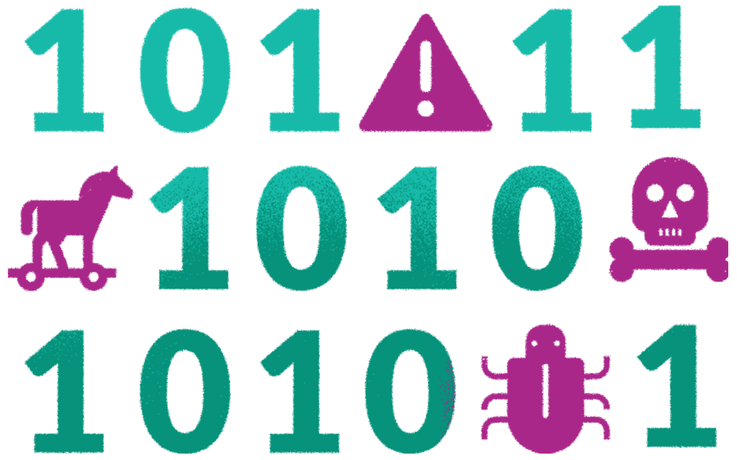
Comissão Europeia

Ameaça n.º 4: Manipulação de *software*

As configurações incorretas e as manipulações de *software* e sistemas ou componentes relacionados podem ter um impacto direto na postura de segurança dos serviços e sistemas de transporte.

Os ataques de cibersegurança que exploram manipulações de *software* modificam as definições do *software* ou afetam a integridade dos dados, a fim de alterar o comportamento de sistemas e serviços. Os atacantes podem intencionalmente manipular o *software* (ou parte do mesmo) para obter vantagens (por exemplo, obter acesso não autorizado, impedir que indivíduos ou sistemas legítimos acedam aos recursos necessários, recolher informações sensíveis, alterar comportamentos funcionais, etc.) em ativos sensíveis.

Por exemplo, os atacantes podem visar canais de comunicação de fabricantes para carregar atualizações de *software* maliciosas em serviços e sistemas (incluindo tecnologias operacionais). Um agente de ameaça utiliza credenciais de autorização comprometidas para aceder a uma interface de rede de manutenção remota segura, a fim de instalar *software* manipulado e comprometer outros serviços e sistemas acessíveis. O agente de ameaça instala *software* manipulado que compromete ainda mais os serviços e sistemas alvo, ou ataca outros serviços ou sistemas associados.



Comissão Europeia

Perfis de sensibilização para a cibersegurança

Comissão Europeia

1

Perfil I: Todos os agentes de transporte

A primeira via é dirigida a todo o pessoal de organizações de transporte, desde pessoal operacional a pessoal administrativo. Esta via fornece orientações para reforçar a compreensão e sensibilização para as ciberameaças mais comuns. Também aborda a forma de lidar com eventuais ciberameaças, nomeadamente como as identificar, comunicar e atenuar. Esta via é comum a todos os modos de transporte.

2

Perfil II: Decisores em matéria de cibersegurança no setor dos transportes

A segunda via dirige-se a pessoal responsável pela tomada de decisões em matéria de segurança ou cibersegurança nas organizações de transporte. Esta via fornece boas práticas adaptadas aos diferentes modos de transporte. Fornece igualmente boas práticas para identificar, proteger, detetar e responder a ciberameaças emergentes que visam organizações de transporte.

Comissão Europeia

Perfil I: Todos os agentes de transporte

Esta parte é dirigida a todo o pessoal de organizações de transporte, desde pessoal operacional a pessoal administrativo, e fornece orientações para reforçar a compreensão e sensibilização para as ciberameaças mais comuns. Também aborda a forma de lidar com eventuais ciberameaças, nomeadamente como as identificar, comunicar e atenuar.

Esta parte fornece práticas recomendadas e sugestões úteis, que são pertinentes **para todos os modos de transporte**.

Boas práticas contra programas maliciosos

Pode ajudar a proteger a sua organização ao seguir boas práticas para **identificar e prevenir a difusão de programas maliciosos**, tais como:

- ***Seguir as políticas de segurança**, como executar deteções de vírus nos suportes de armazenamento e nos ficheiros, evitar abrir e enviar por correio eletrónico determinados tipos de ficheiros (por exemplo, ficheiros executáveis com as extensões .exe, .bat, .com, etc.), instalar apenas software autorizado, assegurar que o software (incluindo o antivírus) está atualizado e a funcionar corretamente, entre outras políticas,*

- ***Realizar cópias de segurança dos dados** regularmente em serviços ou dispositivos de armazenamento de dados seguros (e autorizados), que devem ser compatíveis com mecanismos de encriptação, a fim de proteger dados inativos e garantir que estão disponíveis para procedimentos de recuperação de dados,*

- *Proteger todos os sistemas, nomeadamente dispositivos móveis e terminais, através de **medidas de segurança** adequadas (por exemplo, palavra-passe, encriptação, etc.), e não esquecer de bloquear (fisicamente e digitalmente) todos os sistemas deixados sem vigilância,*

- *Evitar abrir anexos e clicar em hiperligações presentes em mensagens de correio eletrónico inesperadas e janelas instantâneas suspeitas do navegador Web com texto estranho ou de domínios de Internet ou remetentes desconhecidos,*

- *Evitar introduzir no computador **dispositivos amovíveis não fidedignos ou desconhecidos**, como memórias USB, discos rígidos e outros dispositivos de armazenamento,*

- *Evitar desativar medidas de segurança contra programas maliciosos (por exemplo, o software antivírus, o software de filtragem de conteúdo, a barreira de segurança, etc.),*

- ***Atualizar o software instalado** regularmente para as versões mais recentes disponíveis (que os responsáveis pela segurança da informação ou administradores do sistema podem publicar com atualizações regulares),*

- *Evitar utilizar credenciais e contas privilegiadas (por exemplo, de nível de administrador) para atividades e operações normais,*

- *Comunicar aos responsáveis pela segurança da informação ou aos administradores do sistema qualquer mensagem de correio eletrónico suspeita ou comportamentos inesperados do sistema;*

- *Prestar atenção à segurança da informação durante o trabalho de rotina diário, a fim de reconhecer questões de segurança informática e responder em conformidade.*

Comissão Europeia

Boas práticas contra (ataques distribuídos de) negação de serviço

Pode ajudar a proteger a sua organização ao identificar ataques **distribuídos de negação de serviço (DDoS)** e de **negação de serviço (DoS)**. Deve contactar imediatamente as equipas de segurança e TI se detetar ou experienciar um dos seguintes indicadores de possíveis ataques DDoS e DoS em curso nos seus serviços ou sistemas:

- *Aumento de pedidos que consomem a capacidade da rede (percebido como lentidão dos serviços e das respostas), o que resulta em falhas no serviço ou sistema devido a sobrecarga,*
- *Aumento dos pedidos de utilização dos recursos de memória sem motivo aparente,*
- ***Comportamentos inesperados de serviços e sistemas**, paragens anormais frequentes e mensagens de erro estranhas devido a um consumo malicioso dos meios de computação ou ligações de rede,*
- ***Desempenho inferior** de dispositivos, execuções demoradas de tarefas triviais e atividades percetíveis (por exemplo, ruído da ventoinha quando os dispositivos têm um desempenho lento),*
- ***Ligações de Internet inesperadas ou perda de ligação** a serviços e sistemas,*
- *Alterações de comportamento subtis nos comandos ou tecnologias de operação que resultam em danos físicos,*
- *Negação de acesso a contas privilegiadas ou administrativas para bloquear a recuperação de procedimentos de resposta a incidentes.*

Boas práticas contra acesso não autorizado e roubo

A fim de prevenir ataques que envolvam acesso não autorizado e roubo, é necessário seguir princípios como a «*necessidade de tomar conhecimento*» e a «*segurança e privacidade por defeito*», que salientam que os ativos sensíveis e confidenciais (nomeadamente, dados pessoais e sensíveis, sistemas de transporte, etc.) só devem estar acessíveis a quem tenha esse direito no desempenho das suas funções. Pode ajudar a proteger a sua organização ao seguir boas práticas para identificar e prevenir o acesso não autorizado e roubo, tais como:

- *Seguir as políticas de segurança da organização,*

- *Evitar partilhar e publicar credenciais e dados pessoais em linha, nomeadamente imagens que possam conter essas informações,*

- *Evitar utilizar ou transmitir credenciais e dados pessoais (e outros dados sensíveis) em redes, dispositivos ou serviços Web não fidedignos e não seguros (por exemplo, sítios Web que utilizam protocolos inseguros ou endereços http:// e não https://),*

- ***Nunca revelar a ninguém as suas credenciais** (por exemplo, dados de início de sessão e palavras-passe), mesmo por correio eletrónico ou telefone,*

- *Proteger dados sensíveis introduzidos através de teclados ou apresentados em ecrãs (nomeadamente em dispositivos móveis) de indivíduos não autorizados, instalar ecrãs de privacidade, evitar trabalhar em espaços públicos com dispositivos privados e evitar deixar qualquer dispositivo desbloqueado e sem vigilância,*

- ***Utilizar palavras-passe complexas** (por exemplo, suficientemente longas e que combinem carateres alfanuméricos e especiais) que cumpram as políticas de segurança pertinentes da organização para prevenir o acesso não autorizado,*

- ***Alterar as palavras-passe predefinidas** de sistemas e dispositivos ligados (por exemplo, impressoras, encaminhadores, câmaras, Smart Lock, etc.),*

- *Evitar utilizar as mesmas credenciais (por exemplo, dados de início de sessão e palavras-passe) em vários serviços e sistemas e evitar utilizar as mesmas credenciais em serviços e sistemas que exigem contas privilegiadas,*

- *Apenas enviar palavras-passe e chaves para transferência através de ficheiros protegidos (por exemplo, arquivos ZIP) através de um canal fora de banda (por exemplo, SMS por GSM e chamada telefónica) e nunca por correio eletrónico,*

- ***Ativar a autenticação de dois fatores (2FA)** ou a autenticação multifator (MFA), se possível.*

Comissão Europeia

Boas práticas contra manipulação de *software*

Pode ajudar a proteger a sua organização ao seguir boas práticas para identificar e prevenir a manipulação de *software*, tais como:

- *Evitar instalar software não fidedigno em sistemas e dispositivos (nomeadamente, computadores pessoais, servidores, periféricos, dispositivos de rede, telemóveis inteligentes, etc.),*
- *Instalar sempre software e atualizações a partir de fontes e sítios Web oficiais (por exemplo, fabricantes, repositórios empresariais, etc.),*
- *Evitar descarregar software e aplicações (e qualquer ficheiro) de fontes ilegais,*
- *Desinstalar software desnecessário ou não utilizado recentemente e desativar ligações desnecessárias (por exemplo, serviços e protocolos de rede), nomeadamente o acesso a serviços remotos (por exemplo, serviços de armazenamento na nuvem),*
- *Analisar o software ou dispositivos de armazenamento com um antivírus fiável e atualizado,*
- *Descarregar software industrial seguro (por exemplo, atualizações, correções, novos produtos, etc.) de fornecedores fidedignos utilizando o princípio de estação branca,*
- *Atualizar todo o software instalado em conformidade com as políticas e práticas da organização.*

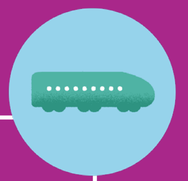
Comissão Europeia

Perfil II: Decisores em matéria de cibersegurança no setor dos transportes

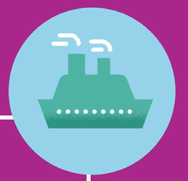
Esta parte dirige-se a pessoal responsável pela tomada de decisões em matéria de segurança ou cibersegurança nas organizações de transporte. Esta via destaca boas práticas adaptadas aos diferentes modos de transporte. Em particular, fornece boas práticas para identificar, proteger, detetar e responder a ciberameaças emergentes.

Comissão Europeia

Boas práticas de cibersegurança adaptadas ao transporte aéreo



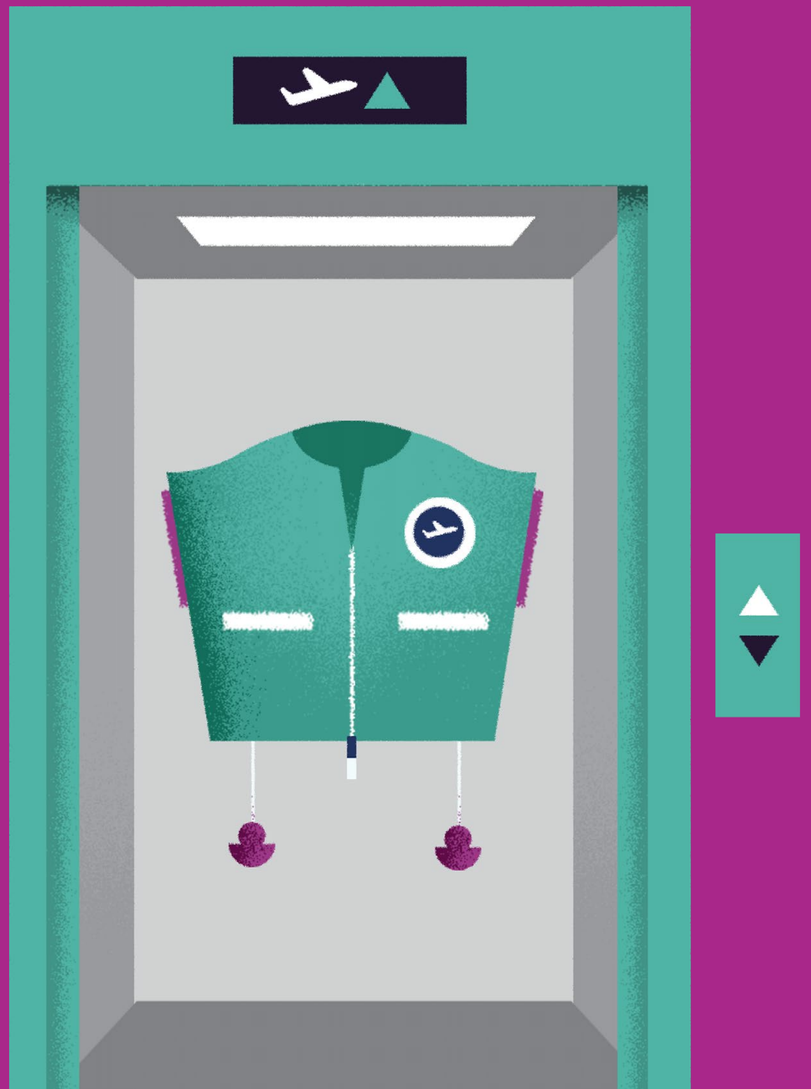
Boas práticas de cibersegurança adaptadas ao transporte terrestre



Boas práticas de cibersegurança adaptadas ao transporte marítimo

Comissão Europeia

Boas práticas e medidas de segurança adaptadas ao transporte aéreo



Governação

As organizações de aviação têm de compreender claramente as ameaças emergentes para definir políticas e processos de gestão que regulem as suas abordagens, a fim de reforçar a cibersegurança de serviços e sistemas nas operações, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO).

As boas práticas para organizações de qualquer dimensão incluem:

- Garantir que os quadros superiores de gestão comunicam questões de cibersegurança a membros executivos e dos conselhos de administração, que podem tomar decisões informadas sobre a atribuição de recursos,

- Designar um cargo sénior, responsável tanto pela cibersegurança como pela segurança física, com responsabilidades de gestão globais em matéria de segurança das tecnologias da informação (TI) e das tecnologias operacionais (TO), mas sem envolvimento nas operações, a fim de evitar conflitos de interesses,

- Definir claramente funções, responsabilidades, competências e autorizações em matéria de cibersegurança e comunicá-las e acordá-las com o pessoal em causa, em particular quando se trata de membros das Equipas de Resposta a Emergências Informáticas (CERT),

- Assegurar a governação da cibersegurança em toda a cadeia de prestação de serviços de segurança, incluindo tanto interfaces físicas como digitais, desde fabricantes e instaladores de tecnologia a prestadores de serviços de segurança,

- Acordar atividades e controlos, incluindo responsabilidades partilhadas, para gerir riscos de cibersegurança e assegurar que estas responsabilidades são mantidas durante todo o ciclo de vida (por exemplo, através de acordos de serviços) das soluções e dos serviços de segurança,

- Definir mecanismos de governação (por exemplo, políticas), a fim de cumprir as obrigações decorrentes de regulamentos e diretivas pertinentes, por exemplo, o Regulamento (UE) 2018/1139 relativo a regras comuns no domínio da aviação civil e o Regulamento de Execução (UE) 2017/373 da Comissão que estabelece requisitos comuns para os prestadores de serviços de gestão do tráfego aéreo/de navegação aérea e de outras funções de rede da gestão do tráfego aéreo e respetiva supervisão, bem como a Diretiva SRI [Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação].

Comissão Europeia

Exemplos de serviços e sistemas no transporte aéreo:
As TI são, por exemplo, as acessíveis aos funcionários (por exemplo, computadores pessoais, telemóveis, periféricos de escritório, etc.), bem como aos passageiros (por exemplo, ligações e encaminhadores Wi-Fi públicos, etc.). As TO são, por exemplo, sistemas de supervisão, controlo e aquisição de dados (SCADA), sistemas de aquecimento, ventilação e ar condicionado (AVAC), postos de controlo de segurança para bagagem de cabina, sistemas de assistência a bagagem (BHS), tecnologia de controlo de acesso, monitorização, vigilância, resposta a alarmes e rastreio, sistemas de controlo de iluminação das pistas, sensores e sistemas de radar, sistemas de posicionamento global (GPS), sistemas de gestão do tráfego aéreo (GTA), sistemas de Comunicações, Navegação e Vigilância (CNS), sistemas de informação aeronáutica, sistemas meteorológicos, sistemas de centros de operações de segurança, sistemas a bordo das companhias aéreas, entre outros.

Identificar ciberameaças

Gestão dos riscos: As organizações de aviação devem tomar medidas adequadas para identificar, avaliar e entender os riscos de cibersegurança para as redes e os sistemas de informação que apoiem as operações de funções essenciais.

Tal exige uma abordagem organizacional global da gestão do risco, que implica:

- *Garantir uma visão global clara dos vários sistemas de hardware e software utilizados para executar diferentes serviços. No contexto da aviação, estes sistemas envolvem tecnologias da informação (TI) e tecnologias operacionais (TO),*

- *Realizar **avaliações dos riscos de cibersegurança**, que têm em conta ameaças emergentes, vulnerabilidades conhecidas e dados operacionais relacionados com os sistemas em questão. Organizações como a Equipa de Resposta a Emergências Informáticas para a Gestão do Tráfego Aéreo Europeu (CERT-SESAR) e o centro de partilha e análise de informações no setor da aviação (ISAC-A) podem fornecer informações sobre ameaças que visam o transporte aéreo,*

- *Garantir que as avaliações dos riscos também abrangem riscos relacionados com atividades quotidianas do pessoal (por exemplo, utilização de redes sociais, utilização de dispositivos pessoais, tratamento de dados, partilha de informações, etc.),*

- *Identificar e aplicar medidas e planos de tratamento de riscos para atenuar riscos de cibersegurança,*

- *Pôr em prática um **sistema de gestão da segurança da informação** (SGSI) abrangente e um **sistema de gestão da privacidade da informação** (SGPI) harmonizados com outros sistemas de gestão. Estes sistemas de gestão (ou seja, SGSI e SGPI) envolvem a aplicação de controlos de segurança (bem como de proteção de dados e privacidade) para atenuar e prevenir ameaças emergentes que afetem a segurança de serviços e sistemas de aviação (incluindo os respetivos dados),*

- *Ter em conta quaisquer restrições relacionadas com a **gestão de ativos e planeamento de recursos** (ou seja, restrições que possam afetar o desempenho, manutenção e suporte de sistemas críticos para operações de funções essenciais no transporte aéreo).*

Exemplos de quadros de gestão de riscos: Os diferentes quadros (por exemplo, as normas da família ISO/IEC 27000, o quadro de referência para a cibersegurança do NIST, o quadro MITRE ATT&CK, o IT-Grundschutz da BSI, etc.) podem inspirar e apoiar uma abordagem de gestão de riscos adaptada ao transporte aéreo. Organizações internacionais como a IATA e a OACI fornecem orientações para avaliações de riscos de cibersegurança. A ENISA, a AESA, a EUROCONTROL e o Conselho Internacional dos Aeroportos (ACI), entre outros, destacam boas práticas para proteger aeroportos, prestadores de serviços de gestão do tráfego aéreo e outras organizações de aviação. A Empresa Comum SESAR coordena e concentra todas as atividades de investigação e desenvolvimento (I&D) da UE em matéria de gestão do tráfego aéreo, abrangendo também aspetos de segurança e proteção.

Comissão Europeia

Proteção contra ciberameaças

As organizações de transporte aéreo devem aplicar medidas de segurança adequadas e proporcionadas para proteger as suas redes e sistemas de informação, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO), contra ciberataques. As medidas de segurança incluem:

- ***Políticas e processos de segurança:*** *definir, aplicar, comunicar e executar políticas e processos adequados, que definem uma abordagem global para proteger sistemas e dados que apoiam operações de funções essenciais na aviação. Estas políticas de segurança (por exemplo, políticas de palavra-passe e armazenamento) também devem abranger correções e gestão de vulnerabilidades de sistemas de hardware e software (nomeadamente TI e TO), gestão de incidentes ou proteção de sistemas e redes.*

- ***Gestão da identidade e do acesso:*** *compreender, documentar e gerir o acesso a redes e sistemas de informação (nomeadamente TI e TO) que apoiem as operações de funções essenciais no transporte aéreo. Os utilizadores (ou funções automatizadas) que podem aceder aos dados ou sistemas são adequadamente verificados, autenticados e autorizados. Este processo também deve ter em conta as diferentes funções e responsabilidades para contas comuns e privilegiadas.*

- ***Segurança de dados e sistemas:*** *proteger dados (armazenados ou transmitidos eletronicamente) e redes e sistemas de informação críticos (nomeadamente TI e TO) contra ciberataques. Tendo em conta uma abordagem baseada em riscos, as organizações devem aplicar medidas de segurança para limitar de forma eficaz as possibilidades de os atacantes comprometerem dados, redes e sistemas. Estas medidas de segurança devem também incluir a adoção de protocolos de encriptação e comunicação segura, a fim de proteger dados inativos e em trânsito contra ciberameaças que resultem de ataques de interceção da comunicação. Além disso, é necessário combinar estas medidas com medidas de segurança físicas, a fim de proteger o acesso aos sistemas (por exemplo, os sistemas devem estar situados em salas fechadas com acesso restrito).*

- ***Resiliência de redes e sistemas:*** *reforçar a resiliência de redes e sistemas (nomeadamente TI e TO) concebendo-os e aplicando-os (bem como os respetivos procedimentos operacionais) de modo a prevenir e atenuar o impacto dos ciberataques. As soluções de conceção e aplicação que reforçam a resiliência incluem, por exemplo: funções críticas formalmente verificadas, redundância de sistemas e redes, segregação de redes (em particular, segregação de TI e TO), medidas de segurança multicamada, entre outras. Importa ter em conta que, do ponto de vista da segurança da informação, os domínios de segurança que aplicam segregações de redes e sistemas podem fornecer soluções de segurança adequadas. No entanto, as necessidades operacionais (por exemplo, atividades de manutenção, transferências de dados, etc.) dos sistemas podem exigir que se contorne ou ligue diferentes domínios de segurança (por exemplo, sistemas e redes segregados), nomeadamente ligando TI e TO.*

Detetar ciberameaças

As organizações devem assegurar que as medidas de segurança permanecem eficazes e detetar eventos de cibersegurança que afetem ou possam afetar os controlos de segurança, bem como os serviços e sistemas essenciais. As medidas de segurança pertinentes para detetar ciberameaças são as seguintes:

- ***Monitorização da segurança:*** *monitorizar o estado de segurança das redes e dos sistemas de informação, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO), para apoiar operações de funções essenciais nos serviços de transporte aéreo. A fim de apoiar a monitorização da segurança, importa ter em conta, por exemplo, os seguintes dados:*

  - *registos de segurança*
  - *registos de deteção de vírus*
  - *registos de deteção de intrusões*
  - *registos de identificação, autenticação e autorização*
  - *registos de sistemas e serviços*
  - *registos de tráfego na rede*
  - *registos de tratamento de dados*

- ***Deteção de eventos de segurança:*** *detetar atividades maliciosas (isto é, eventos de segurança) que afetem ou possam afetar a segurança das redes e dos sistemas de informação (nomeadamente TI e TO) que apoiem operações de funções essenciais nos serviços de transporte aéreo.*

Estas medidas podem exigir a adoção de tecnologias específicas (por exemplo, gestão de eventos e informação de segurança, sistema de deteção de intrusões, sistema de prevenção de intrusões, etc.) e a criação de um centro de operações de segurança (SOC) ou equivalente, isto é, desenvolver meios para detetar, analisar, responder e recuperar de ciberataques localmente.

Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) nacionais, CERT setoriais (por exemplo, a Equipa de Resposta a Emergências Informáticas para a Gestão do Tráfego Aéreo Europeu da EUROCONTROL – CERT-SESAR), CERT comerciais das companhias aéreas e o centro de partilha e análise de informações no setor da aviação (ISAC-A) podem fornecer informações sobre ciberameaças (CTI) que contribuem para a monitorização da segurança e a deteção.

Planeamento de resposta e recuperação

As organizações devem definir, aplicar e testar procedimentos de gestão de incidentes, que visam assegurar a continuidade operacional de serviços e sistemas em caso de incidentes de cibersegurança. As medidas de atenuação visam conter ou limitar o impacto dos incidentes de cibersegurança.

O planeamento de resposta e recuperação deve ter em conta medidas de segurança que atenuam o impacto de ataques de cibersegurança específicos, tais como:

- *Coordenação e colaboração com CSIRT nacionais, CERT (públicas e comerciais) e centros de partilha e análise de informações durante incidentes de cibersegurança, coordenação de incidentes e crises a nível pan-europeu,*

- *Partilha de informações com outras organizações, nomeadamente fornecedores na cadeia de abastecimento dos serviços de aviação,*

- *Realização de **exercícios de ciberataque** periódicos (exercícios teóricos de coordenação e técnicos) para avaliar medidas e procedimentos de segurança, bem como a resiliência da organização para lidar com ciberincidentes,*

- *Acesso a locais de armazenamento de arquivos ou cópias de segurança em caso de comprometimento da integridade e disponibilidade dos armazenamentos de dados,*

- ***Protocolos operacionais em matéria de segurança** com procedimentos pormenorizados para gerir incidentes de cibersegurança e repor os serviços e sistemas em condições de funcionamento normais,*

- *Redirecionamento do tráfego na rede para serviços redundantes durante ataques de negação de serviço,*

- *Procedimentos manuais para operar serviços e sistemas em modos de funcionamento degradados,*

- *Definição de procedimentos para lidar com violações de dados, nomeadamente procedimentos para lidar com violações de dados que afetem dados pessoais, em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e qualquer outro regulamento ou diretiva setorial pertinente,*

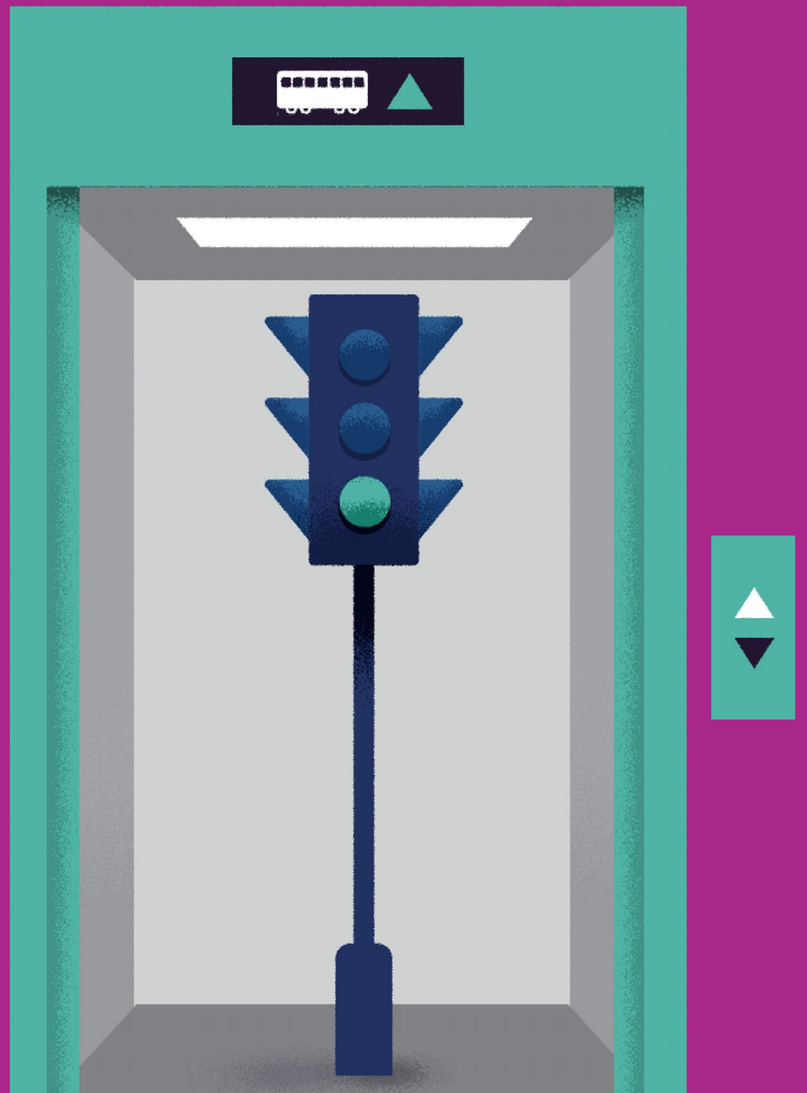
- *Subscrição de **ciberseguros** para cobrir parcialmente o risco associado a incidentes graves de cibersegurança,*

- *Celebração de um contrato de avença de resposta a incidentes com uma ou mais empresas especializadas para obter maior capacidade e experiência,*

- *Definição de procedimentos para a **partilha de informação de incidentes de cibersegurança** com partes interessadas, nomeadamente procedimentos para a notificação de incidentes em conformidade com a Diretiva SRI [Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União].*

Comissão Europeia

Boas práticas e medidas de segurança adaptadas ao transporte terrestre



Governação

As organizações de transporte terrestre (ferroviário e rodoviário) têm de compreender claramente as ameaças emergentes para definir políticas e processos de gestão que regulem as suas abordagens, a fim de reforçar a cibersegurança de serviços e sistemas nas operações, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO).

As boas práticas para organizações de qualquer dimensão incluem:

- *Garantir que os quadros superiores de gestão comunicam questões de cibersegurança a membros executivos e dos conselhos de administração, que podem tomar decisões informadas sobre a atribuição de recursos,*

- *Designar um cargo sénior, responsável tanto pela cibersegurança como pela segurança física, com responsabilidades de gestão globais em matéria de segurança das tecnologias da informação (TI) e das tecnologias operacionais (TO), mas sem envolvimento nas operações, a fim de evitar conflitos de interesses,*

- *Definir claramente funções, responsabilidades, competências e autorizações em matéria de cibersegurança e comunicá-las e acordá-las com o pessoal em causa. Tal é particularmente necessário quando se trata de membros das Equipas de Resposta a Emergências Informáticas (CERT),*

- *Assegurar a governação da cibersegurança em toda a cadeia de prestação de serviços de segurança, incluindo tanto interfaces físicas como digitais, desde fabricantes e instaladores de tecnologia a prestadores de serviços de segurança,*

- *Acordar atividades e controlos, incluindo responsabilidades partilhadas, para gerir riscos de cibersegurança e assegurar que estas responsabilidades são mantidas durante todo o ciclo de vida (por exemplo, através de acordos de serviços) das soluções e dos serviços de segurança,*

- *Definir mecanismos de governação (por exemplo, políticas) para cumprir obrigações decorrentes de regulamentos e diretivas pertinentes. Tal engloba um vasto conjunto de políticas que abrange modos de transporte específicos e diferentes tipos de partes interessadas (por exemplo, fabricantes de veículos e sistemas ferroviários), para além da Diretiva SRI [Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação].*

Exemplos de serviços e sistemas no transporte terrestre: As TI são, por exemplo, as acessíveis aos funcionários (por exemplo, computadores pessoais, telemóveis, periféricos de escritório, etc.), bem como aos passageiros (por exemplo, ligações e encaminhadores Wi-Fi públicos, etc.). As TO são, por exemplo, sistemas de supervisão, controlo e aquisição de dados (SCADA), sistemas de aquecimento, ventilação e ar condicionado (AVAC), sistemas de posicionamento global (GPS) e tecnologia de controlo de acesso, monitorização, vigilância, resposta a alarmes e rastreio. Os sistemas específicos para o transporte ferroviário incluem, por exemplo: sistemas operacionais (de controlo e comando), incluindo sistemas de sinalização, o Sistema Europeu de Gestão do Tráfego Ferroviário (ERTMS), sistemas a bordo de comboios, sistemas de manutenção, entre outros.

Identificação de ciberameaças

Gestão dos riscos: As organizações de transporte terrestre devem tomar medidas adequadas para identificar, avaliar e entender os riscos de cibersegurança para as redes e os sistemas de informação que apoiem as operações de funções essenciais. Tal exige uma abordagem organizacional global da gestão do risco, que implica:

- *Garantir uma visão global clara dos vários sistemas de hardware e software utilizados para executar diferentes serviços. No contexto do transporte terrestre, estes sistemas envolvem tecnologias da informação (TI) e tecnologias operacionais (TO),*

- *Realizar **avaliações dos riscos de cibersegurança**, que devem ter em conta ameaças emergentes, vulnerabilidades conhecidas e dados operacionais relacionados com os sistemas em questão. Os sistemas nos modos de transporte terrestre incluem, por exemplo: sistemas de pagamento, sistemas de rede e comunicação (por exemplo, Internet, comunicação por rádio, Wi-Fi, etc.), equipamento a bordo, centros de controlo operacional, sistemas de gestão de identidade, sistemas de proteção, entre outros. Para as estruturas ferroviárias, os sistemas incluem, por exemplo: material circulante, subsistemas de gestão de operações e de tráfego, comando de controlo e subsistemas de sinalização a bordo e na via, entre outros,*

- *Garantir que as avaliações dos riscos também abrangem riscos relacionados com atividades quotidianas do pessoal (por exemplo, utilização de redes sociais, utilização de dispositivos pessoais, tratamento de dados, partilha de informações, etc.),*

- *Identificar e aplicar medidas e planos de tratamento de riscos para atenuar riscos de cibersegurança. Por exemplo, pôr em prática um **sistema de gestão da segurança da informação** (SGSI) abrangente e um **sistema de gestão da privacidade da informação** (SGPI) harmonizados com outros sistemas de gestão. Estes sistemas de gestão (ou seja, SGSI e SGIPI) envolvem a aplicação de controlos de segurança (bem como de proteção de dados e privacidade) para atenuar e prevenir ameaças emergentes que afetem a segurança de serviços e sistemas de transporte terrestre (incluindo os respetivos dados),*

- *Ter em conta quaisquer restrições relacionadas com **gestão de ativos e planeamento de recursos** (ou seja, restrições que possam afetar o desempenho, manutenção e suporte de sistemas críticos para operações de funções essenciais no transporte terrestre).*

Exemplos de quadros de gestão de riscos: Os diferentes quadros (por exemplo, as normas da família ISO/IEC 27000, o quadro de referência para a cibersegurança do NIST, o quadro MITRE ATT&CK, o IT-Grundschutz da BSI, etc.) podem inspirar e apoiar uma abordagem de gestão de riscos adaptada ao transporte rodoviário e ferroviário. Organizações como a ENISA definem boas práticas para a cibersegurança de automóveis inteligentes e transportes públicos inteligentes, que informam fabricantes e associações do setor (por exemplo, a Associação dos Construtores Europeus de Automóveis — ACEA). Relativamente ao transporte ferroviário, a Agência Ferroviária da União Europeia (AFE) define especificações técnicas de interoperabilidade (ETI), que cada subsistema ou parte do subsistema deve satisfazer para cumprir os requisitos essenciais e assegurar a interoperabilidade do sistema ferroviário na União Europeia. A Empresa Comum Shift2Rail também promove iniciativas e projetos inovadores (nomeadamente em matéria de cibersegurança) para o transporte ferroviário.

Proteção contra ciberameaças

As organizações de transporte terrestre devem aplicar medidas de segurança adequadas e proporcionadas para proteger as suas redes e sistemas de informação, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO), contra ciberataques. As medidas de segurança incluem:

- ***Políticas e processos de segurança:*** *definir, aplicar, comunicar e executar políticas e processos adequados, que definem uma abordagem global para proteger sistemas e dados que apoiam operações de funções essenciais nos modos de transporte terrestres. Estas políticas de segurança (por exemplo, políticas de palavra-passe e armazenamento) também devem abranger correções e gestão de vulnerabilidades de sistemas de hardware e software (nomeadamente TI e TO), gestão de incidentes ou proteção de sistemas e redes.*

- ***Gestão da identidade e do acesso:*** *compreender, documentar e gerir o acesso a redes e sistemas de informação (nomeadamente TI e TO) que apoiem as operações de funções essenciais nos modos de transporte terrestre. Os utilizadores (ou funções automatizadas) que podem aceder aos dados ou sistemas são adequadamente verificados, autenticados e autorizados. Este processo também deve ter em conta as diferentes funções e responsabilidades para contas comuns e privilegiadas.*

- ***Segurança de dados e sistemas:*** *proteger dados (armazenados ou transmitidos eletronicamente) e redes e sistemas de informação críticos (nomeadamente TI e TO) contra ciberataques. Tendo em conta uma abordagem baseada em riscos, as organizações devem aplicar medidas de segurança para limitar de forma eficaz as possibilidades de os atacantes comprometerem dados, redes e sistemas. Estas medidas de segurança devem também incluir a adoção de protocolos de encriptação e comunicação segura, a fim de proteger dados inativos e em trânsito contra ciberameaças que resultem de ataques de interceção da comunicação. Além disso, é necessário combinar estas medidas com medidas de segurança físicas, a fim de proteger o acesso aos sistemas (por exemplo, os sistemas devem estar situados em salas fechadas com acesso restrito). Este aspeto é muito importante para sistemas que podem ter impacto na segurança da vida.*

- ***Resiliência de redes e sistemas:*** *reforçar a resiliência de redes e sistemas (nomeadamente TI e TO) concebendo-os e aplicando-os (bem como os respetivos procedimentos operacionais) de modo a prevenir e atenuar o impacto dos ciberataques. As soluções de conceção e aplicação que reforçam a resiliência incluem, por exemplo: funções críticas formalmente verificadas, redundância de sistemas e redes, segregação de redes (em particular, segregação de TI e TO), medidas de segurança multicamada, entre outras. Importa ter em conta que, do ponto de vista da segurança da informação, os domínios de segurança que aplicam segregações de redes e sistemas podem fornecer soluções de segurança adequadas. No entanto, as necessidades operacionais (por exemplo, atividades de manutenção, transferências de dados, etc.) dos sistemas podem exigir que se contorne ou ligue diferentes domínios de segurança (por exemplo, sistemas e redes segregados), nomeadamente ligando TI e TO.*

Deteção de ciberameaças

As organizações devem assegurar que as medidas de segurança permanecem eficazes e detetar eventos de cibersegurança que afetem ou possam afetar os controlos de segurança, bem como os serviços e sistemas essenciais. As medidas de segurança pertinentes para detetar ciberameaças são as seguintes:

- ***Monitorização da segurança:*** *monitorizar o estado de segurança das redes e dos sistemas de informação, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO), para apoiar operações de funções essenciais nos modos de transporte terrestre. Tal é necessário para detetar eventuais ameaças de segurança e monitorizar a eficácia contínua das medidas de segurança protetoras. A fim de apoiar a monitorização da segurança, importa ter em conta, por exemplo, os seguintes dados:*

  - *registos de segurança*
  - *registos de deteção de vírus*
  - *registos de deteção de intrusões*
  - *registos de identificação, autenticação e autorização*
  - *registos de sistemas e serviços*
  - *registos de tráfego na rede*
  - *registos de tratamento de dados*

- ***Deteção de eventos de segurança:*** *detetar atividades maliciosas (isto é, eventos de segurança) que afetem ou possam afetar a segurança das redes e dos sistemas de informação (nomeadamente TI e TO) que apoiem operações de funções essenciais.*

Estas medidas podem exigir a adoção de tecnologias específicas (por exemplo, gestão de eventos e informação de segurança, sistema de deteção de intrusões, sistema de prevenção de intrusões, etc.) e a criação de um centro de operações de segurança (SOC) ou equivalente, isto é, desenvolver meios para detetar, analisar, responder e recuperar de ciberataques localmente.
Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) nacionais, CERT setoriais e comerciais ou operadores rodoviários ou ferroviários, e o centro de partilha e análise de informações no setor ferroviário europeu (ISAC-ER) podem fornecer informações sobre ciberameaças (CTI) que contribuem para a monitorização da segurança e a deteção.

Planeamento de resposta e recuperação

As organizações devem definir, aplicar e testar procedimentos de gestão de incidentes, que visam assegurar a continuidade operacional de serviços e sistemas em caso de incidentes de cibersegurança.

O planeamento de resposta e recuperação deve ter em conta medidas de segurança que atenuam o impacto de ataques de cibersegurança específicos, tais como:

- *Coordenação e colaboração com CSIRT nacionais, CERT (públicas e comerciais) e centros de partilha e análise de informações durante incidentes de cibersegurança, coordenação de incidentes e crises a nível pan-europeu,*

- *Partilha de informações com outras organizações, nomeadamente fornecedores na cadeia de abastecimento dos serviços de transporte terrestre,*

- *Realização de **exercícios de ciberataque** periódicos (exercícios teóricos de coordenação e técnicos) para avaliar medidas e procedimentos de segurança, bem como a resiliência da organização para lidar com ciberincidentes,*

- *Acesso a locais de armazenamento de arquivos ou cópias de segurança em caso de comprometimento da integridade e disponibilidade dos armazenamentos de dados,*

- ***Protocolos operacionais em matéria de segurança** com procedimentos pormenorizados para gerir incidentes de cibersegurança e repor os serviços e sistemas em condições de funcionamento normais,*

- *Redirecionamento do tráfego na rede para serviços redundantes durante ataques de negação de serviço,*

- *Procedimentos manuais para operar serviços e sistemas em modos de funcionamento degradados,*

- *Definição de procedimentos para lidar com violações de dados, nomeadamente procedimentos para lidar com violações de dados que afetem dados pessoais, em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e qualquer outro regulamento ou diretiva setorial pertinente,*

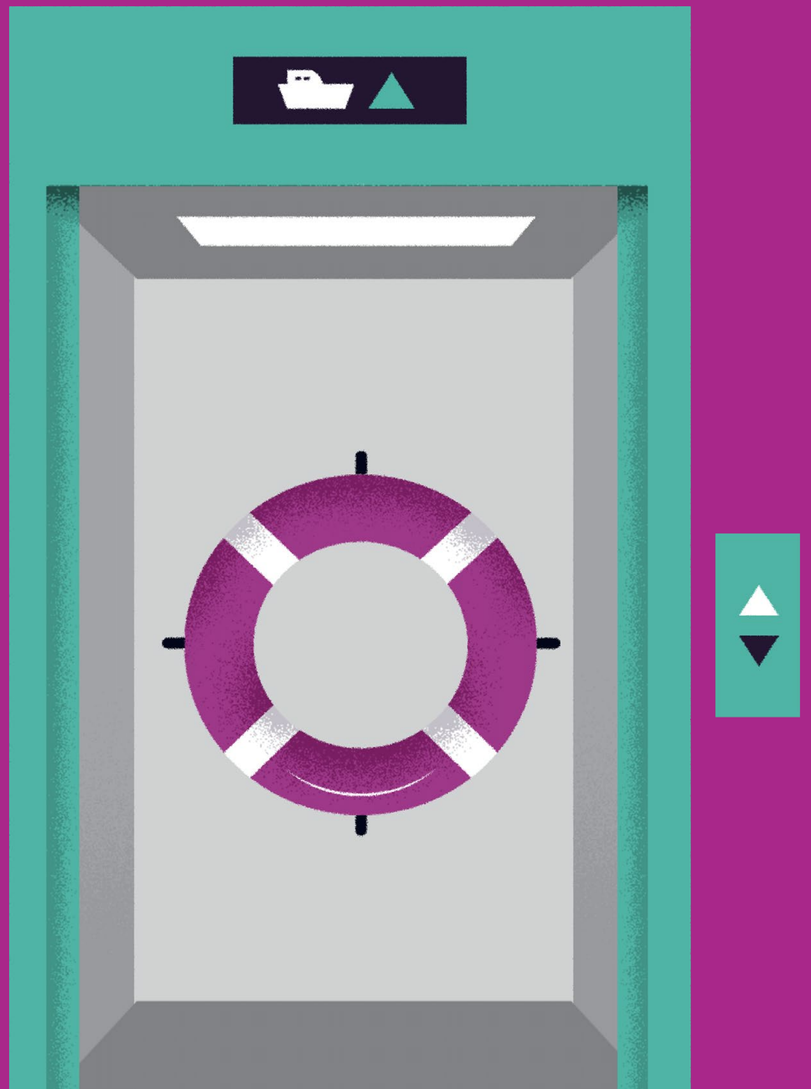
- *Subscrição de **ciberseguros** para cobrir parcialmente o risco associado a incidentes graves de cibersegurança,*

- *Celebração de um contrato de avença de resposta a incidentes com uma ou mais empresas especializadas para obter maior capacidade e experiência,*

- *Definição de procedimentos para a partilha de informação de incidentes de cibersegurança com partes interessadas, nomeadamente procedimentos para a notificação de incidentes em conformidade com a Diretiva SRI [Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União].*

Comissão Europeia

Boas práticas e medidas de segurança adaptadas ao transporte marítimo



Comissão Europeia

Governação

As organizações de transporte marítimo têm de compreender claramente as ameaças emergentes para definir políticas e processos de gestão que regulem as suas abordagens, a fim de reforçar a cibersegurança de serviços e sistemas em operações, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO).

As boas práticas para organizações de qualquer dimensão incluem:

- *Garantir que os quadros superiores de gestão comunicam questões de cibersegurança a membros executivos e dos conselhos de administração, que podem tomar decisões informadas sobre a atribuição de recursos,*

- *Nomear um cargo sénior com responsabilidades de gestão globais em matéria de segurança da tecnologia de informação (TI) e da tecnologia operacional (TO). Este cargo deve ser responsável tanto pela cibersegurança como pela segurança física,*

- *Definir claramente funções, responsabilidades, competências e autorizações em matéria de cibersegurança, definir níveis de autoridade e vias de comunicação para o pessoal de terra, para o pessoal de bordo e entre ambos e acordá-los com o pessoal em questão. Tal é particularmente necessário quando se trata de membros das Equipas de Resposta a Emergências Informáticas (CERT). O pessoal que desempenhe funções relacionadas com legislações da UE em matéria de proteção e segurança marítima, como agentes de segurança das instalações portuárias, agentes de segurança dos portos ou agentes de segurança de companhias, ou a pessoa em terra designada (DPA) e o comandante a bordo, devem estar familiarizados, pelo menos, com as medidas de cibersegurança tomadas pela organização,*

- *Assegurar a governação da cibersegurança em toda a cadeia de prestação de serviços de segurança, incluindo tanto interfaces físicas como digitais, desde fabricantes e instaladores de tecnologia a prestadores de serviços de segurança,*

- *Acordar atividades e controlos, incluindo responsabilidades partilhadas, para gerir riscos de cibersegurança e assegurar que estas responsabilidades são mantidas durante todo o ciclo de vida (por exemplo, através de acordos de serviços) das soluções e dos serviços de segurança,*

- *Definir mecanismos de governação (por exemplo, políticas), a fim de cumprir obrigações decorrentes de regulamentos e diretivas pertinentes, por exemplo, o Regulamento (UE) 2019/1239 que estabelece um ambiente europeu de plataforma única para o setor marítimo (EMSWe, do inglês European Maritime Single Window environment), o Regulamento (CE) n.º 725/2004 relativo ao reforço da proteção dos navios e das instalações portuárias, a Diretiva 2005/65/CE relativa ao reforço da segurança nos portos e o Regulamento (CE) n.º 336/2006 relativo à aplicação do Código Internacional de Gestão da Segurança (ISM), bem como a Resolução A.741(18) que adota o Código ISM para a Segurança da Exploração dos Navios e a Prevenção da Poluição. Neste contexto, cabe também mencionar o ambiente comum de partilha da informação (CISE), uma iniciativa da UE que visa tornar os sistemas de vigilância europeus e dos Estados-Membros interoperacionais para dar a todas as autoridades competentes acesso à informação confidencial e não confidencial de que necessitam para efetuar missões no mar.*

Exemplos de serviços e sistemas no transporte marítimo: As TI são, por exemplo, as acessíveis aos funcionários (por exemplo, computadores pessoais, telemóveis, periféricos de escritório, etc.), bem como aos passageiros (por exemplo, ligações e encaminhadores Wi-Fi públicos, etc.). As TO são, por exemplo, sistemas de supervisão, controlo e aquisição de dados (SCADA), sistemas de aquecimento, ventilação e ar condicionado (AVAC), sistemas de posicionamento global (GPS), tecnologia de controlo de acesso, monitorização, vigilância, resposta a alarmes e rastreio, sistemas de navegação a bordo, SafeSeaNet, sistemas de pontes, sistemas de gestão e manuseamento de carga, sistemas de propulsão e gestão de máquinas e de controlo de potência, sistemas de controlo de acesso, sistemas de gestão e serviço de passageiros, redes públicas para passageiros, sistemas de proteção social da tripulação e administrativos, sistemas de comunicação, entre outros.

Identificação de ciberameaças

Gestão dos riscos: As organizações marítimas devem tomar as medidas adequadas para identificar, analisar, avaliar e comunicar riscos de cibersegurança, bem como para os aceitar, prevenir, transferir ou diminuir para um nível aceitável. Tal exige uma abordagem organizacional global da gestão do risco, que implica:

- *Garantir uma visão global clara dos vários sistemas de hardware e software utilizados para executar diferentes serviços. No contexto do transporte marítimo, estes sistemas envolvem tecnologias da informação (TI) e tecnologias operacionais (TO), e a forma como estes sistemas se ligam e integram no lado de terra, nomeadamente com autoridades públicas, terminais marítimos e estivadores,*

- *Identificar e avaliar operações fundamentais a bordo de navios, que sejam vulneráveis a ciberataques, e realizar avaliações dos riscos de cibersegurança (nomeadamente, avaliar os eventuais impactos operacionais e a probabilidade de ocorrência), que devem ter em conta ameaças emergentes, vulnerabilidades conhecidas e dados operacionais relacionados com os sistemas em questão. Quando adequado, fazer a ligação com avaliações de segurança realizadas para navios (SSA), instalações portuárias (PFSA) e portos (PSA), conforme estabelecido na legislação em matéria de segurança marítima da UE. Estas avaliações identificam eventuais ameaças de segurança a infraestruturas portuárias e falhas de segurança. Adicionalmente, organizações marítimas como a Organização Marítima Internacional (OMI) e os centros de partilha e análise de informações do setor marítimo podem fornecer informações sobre ameaças que visam o transporte marítimo,*

- *Garantir que as avaliações dos riscos também abrangem riscos relacionados com atividades quotidianas do pessoal (por exemplo, utilização de redes sociais, utilização de dispositivos pessoais, tratamento de dados, partilha de informações, etc.),*

- *Identificar e aplicar medidas e planos de tratamento de riscos para atenuar riscos de cibersegurança. Por exemplo, pôr em prática um sistema de gestão da segurança da informação (SGSI) abrangente e um sistema de gestão da privacidade da informação (SGPI) harmonizados com outros sistemas de gestão, como sistemas de gestão de segurança (SGS), em conformidade com o Código Internacional de Gestão da Segurança (ISM). Estes sistemas de gestão (ou seja, SGSI e SGPI) envolvem a aplicação de controlos de segurança (bem como de proteção de dados e privacidade) para atenuar e prevenir ameaças emergentes que afetem a segurança de serviços e sistemas marítimos (incluindo os respetivos dados),*

- *Ter em conta quaisquer restrições relacionadas com a **gestão de ativos e planeamento de recursos** (ou seja, restrições que possam afetar o desempenho, manutenção e suporte de sistemas críticos para operações de funções essenciais no transporte marítimo). No que diz respeito às avaliações, fazer referências, quando adequado, aos requisitos do código ISM, aos sistemas de gestão de segurança (SGS) e aos planos de segurança elaborados em conformidade com a legislação da UE em matéria de segurança e proteção marítima.*

Exemplos de quadros de gestão de riscos: Os diferentes quadros (por exemplo, o Código ISM, as normas da família ISO/IEC 27000, o quadro de referência para a cibersegurança do NIST, o quadro MITRE ATT&CK, o IT-Grundschutz da BSI, etc.) podem inspirar e apoiar uma abordagem de gestão de riscos adaptada ao transporte marítimo. O quadro de referência para a cibersegurança do NIST também foi adaptado para abordar a cibersegurança de operações de transferência marítima de líquidos a granel (MBLT), operações ao largo e operações em embarcações de passageiros. Por sua vez, o Conselho Marítimo Báltico e Internacional (BIMCO) publicou *«The Guidelines on Cyber Security Onboard Ships»* (Orientações sobre cibersegurança a bordo de navios) e a Organização Marítima Internacional (OMI) publicou o documento específico *«Guidelines on maritime cyber risk management»* (Orientações sobre a gestão de ciber-riscos marítimos) (MSC-FAL.1/Circ.3). A ENISA realizou vários estudos relacionados com as boas práticas para a cibersegurança marítima, em particular, a cibersegurança dos portos. A EMSA presta serviços à comunidade marítima, nomeadamente formações de sensibilização para a cibersegurança. Algumas normas (por exemplo, IEC 61162-460:2018 sobre proteção e segurança de equipamento e sistemas de navegação e de radiocomunicação marítimas, ISO 16425:2013 sobre navios e tecnologia marítima, IEC 62443-4-1:2018 sobre segurança para sistemas de controlo e automação industrial, etc.) também definem requisitos específicos de proteção e segurança para sistemas e redes no transporte marítimo.

Proteção contra ciberameaças

As organizações de transporte marítimo devem aplicar medidas de segurança adequadas e proporcionadas para proteger as suas redes e sistemas de informação, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO). As medidas de segurança incluem:

- ***Políticas e processos de segurança:*** *definir, aplicar, comunicar e executar políticas e processos adequados, que definem uma abordagem global para proteger sistemas e dados que apoiam operações de funções essenciais no transporte marítimo. Devem ser incluídas medidas de segurança (nomeadamente medidas de segurança físicas e de cibersegurança) nos planos pertinentes, como o sistema de gestão de segurança (SGS) e o plano de proteção do navio (SSP). Estas políticas de segurança (por exemplo, políticas de palavra-passe e armazenamento) também devem abranger correções e gestão de vulnerabilidades de sistemas de hardware e software (nomeadamente TI e TO), gestão de incidentes ou proteção de sistemas e redes.*

- ***Gestão da identidade e do acesso:*** *compreender, documentar e gerir o acesso a redes e sistemas de informação (nomeadamente TI e TO) que apoiem as operações de funções essenciais no transporte marítimo. Os utilizadores (ou funções automatizadas) que podem aceder aos dados ou sistemas são adequadamente verificados, autenticados e autorizados. Este processo também deve ter em conta as diferentes funções e responsabilidades para contas normais e privilegiadas.*

- ***Segurança de dados e sistemas:*** *proteger dados (armazenados ou transmitidos eletronicamente) e redes e sistemas de informação críticos (nomeadamente TI e TO) contra ciberataques. Tendo em conta uma abordagem baseada em riscos, as organizações devem aplicar medidas de segurança para limitar de forma eficaz as possibilidades de os atacantes comprometerem dados, redes e sistemas. Estas medidas de segurança devem também incluir a adoção de protocolos de encriptação e comunicação segura, a fim de proteger dados inativos e em trânsito contra ciberameaças que resultem de ataques de interceção da comunicação. Além disso, é necessário combinar estas medidas com medidas de segurança físicas, a fim de proteger o acesso aos sistemas (por exemplo, os sistemas devem estar situados em salas fechadas com acesso restrito). Este aspeto é muito importante para sistemas que podem ter impacto na segurança da vida (por exemplo, sistemas de navegação e de comunicação por rádio de categoria II e III).*

- ***Resiliência de redes e sistemas:*** *reforçar a resiliência de redes e sistemas (nomeadamente TI e TO) concebendo-os e aplicando-os (bem como os respetivos procedimentos operacionais) de modo a prevenir e atenuar o impacto dos ciberataques. As soluções de conceção e aplicação que reforçam a resiliência incluem, por exemplo: funções críticas formalmente verificadas, redundância de sistemas e redes, segregação de redes (em particular, segregação de TI e TO), medidas de segurança multicamada, entre outras. Importa ter em conta que, do ponto de vista da segurança da informação, os domínios de segurança que aplicam segregações de redes e sistemas podem fornecer soluções de segurança adequadas. No entanto, as necessidades (por exemplo, atividades de manutenção, transferências de dados, etc.) dos sistemas (por exemplo, veículos marítimos de superfície autónomos) podem exigir que se contorne ou ligue diferentes domínios de segurança (por exemplo, sistemas e redes segregados), nomeadamente ligando TI e TO.*

Deteção de ciberameaças

As organizações devem assegurar que as medidas de segurança permanecem eficazes e detetar eventos de cibersegurança que afetem ou possam afetar os controlos de segurança, bem como os serviços e sistemas essenciais. As medidas de segurança pertinentes para detetar ciberameaças são as seguintes:

- ***Monitorização da segurança:*** *monitorizar o estado de segurança das redes e dos sistemas de informação, nomeadamente tecnologias da informação (TI) e tecnologias operacionais (TO), para apoiar operações de funções essenciais nos serviços de transporte marítimo. Tal é necessário para detetar eventuais ameaças de segurança e monitorizar a eficácia contínua das medidas de segurança protetoras. A fim de apoiar a monitorização da segurança, importa ter em conta, por exemplo, os seguintes dados:*

  - *registos de segurança*
  - *registos de deteção de vírus*
  - *registos de deteção de intrusões*
  - *registos de identificação, autenticação e autorização*
  - *registos de sistemas e serviços*
  - *registos de tráfego na rede*
  - *registos de tratamento de dados*

- ***Deteção de eventos de segurança:*** *detetar atividades maliciosas (isto é, eventos de segurança) que afetem ou possam afetar a segurança das redes e dos sistemas de informação (nomeadamente TI e TO) que apoiem operações de funções essenciais nos serviços de transporte marítimo.*

Estas medidas podem exigir a adoção de tecnologias específicas (por exemplo, gestão de eventos e informação de segurança, sistema de deteção de intrusões, sistema de prevenção de intrusões, etc.) e a criação de um centro de operações de segurança (SOC) ou equivalente, isto é, desenvolver meios para detetar, analisar, responder e recuperar de ciberataques localmente.

Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) nacionais, CERT setoriais e CERT comerciais de operadores marítimos, bem como os centros de partilha e análise de informações do setor marítimo, podem fornecer informações sobre ciberameaças (CTI) que contribuem para a monitorização da segurança e a deteção.

Comissão Europeia

Planeamento de resposta e recuperação

As organizações devem definir, aplicar e testar procedimentos de gestão de incidentes, que visam assegurar a continuidade operacional de serviços e sistemas em caso de incidentes de cibersegurança.
O planeamento de resposta e recuperação deve ter em conta medidas de segurança que atenuam o impacto de ataques de cibersegurança específicos, tais como:

- *Redirecionamento do tráfego na rede para serviços redundantes durante ataques de negação de serviço,*

- *Procedimentos manuais para operar serviços e sistemas em modos de funcionamento degradados,*

- *Criar programas para simulações e exercícios (por exemplo, exercícios teóricos de coordenação e técnicos e simulações de resposta) para responder a ciberataques e situações de emergência e avaliar medidas e procedimentos de segurança, bem como a resiliência da organização para lidar com ciberincidentes,*

- *Acesso a locais de armazenamento de arquivos ou cópias de segurança em caso de comprometimento da integridade e disponibilidade dos armazenamentos de dados,*

- *Coordenação e colaboração com CSIRT nacionais, CERT (públicas e comerciais) e centros de partilha e análise de informações durante incidentes de cibersegurança, coordenação de incidentes e crises a nível pan-europeu,*

- *Partilha de informações com outras organizações, nomeadamente fornecedores na cadeia de abastecimento de serviços no transporte marítimo,*

- *Protocolos operacionais em matéria de segurança com procedimentos pormenorizados para gerir incidentes de cibersegurança e repor os serviços e sistemas em condições de funcionamento normais,*

- *Definição de procedimentos para lidar com violações de dados, nomeadamente procedimentos para lidar com violações de dados que afetem dados pessoais, em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e qualquer outro regulamento ou diretiva setorial pertinente,*

- *Subscrição de ciberseguros para cobrir parcialmente o risco associado a incidentes graves de cibersegurança,*

- *Celebração de um contrato de avença de resposta a incidentes com uma ou mais empresas especializadas para obter maior capacidade e experiência,*

- *Definição de procedimentos para a partilha de informação de incidentes de cibersegurança (incluindo não conformidades, acidentes e situações perigosas) com partes interessadas, nomeadamente procedimentos para a notificação de incidentes em conformidade com a Diretiva SRI [Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União].*

Luxemburgo: Serviço das Publicações da União Europeia, 2021

Print	ISBN 978-92-76-40507-8	doi:10.2832/187199	MI-05-21-230-PT-C
PDF	ISBN 978-92-76-40500-9	doi:10.2832/364	MI-05-21-230-PT-N

Serviço das Publicações
da União Europeia