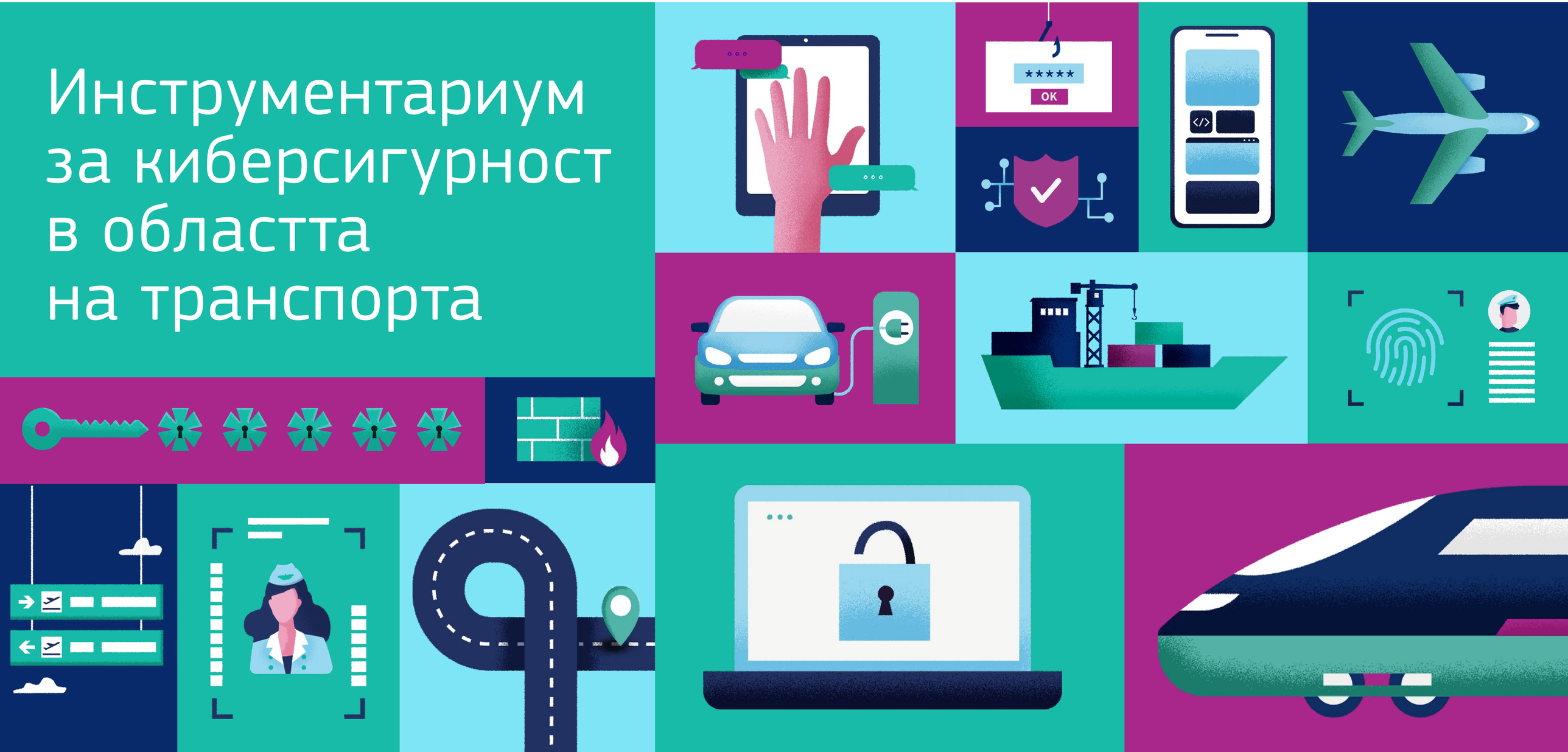
Европейска комисия

Инструментариум за киберсигурност в областта на транспорта



Въведение

Генерална дирекция „Мобилност и транспорт“ на Европейската комисия (ГД „Мобилност и транспорт“) възложи разработването на настоящия инструментариум, за да повиши осведомеността и готовността на заинтересованите страни в областта на транспорта по отношение на киберзаплахите. В него е предоставена информация за разбирането на киберзаплахите и намаляването на тяхното въздействие върху транспортните услуги, системи и операции. В настоящия инструментариум са представени алтернативни пътища за повишаване на осведомеността, насочени към различни профили в областта на транспорта:

- всички работещи в сектора на транспорта (предоставящи обща информация и насоки);
- лица, вземащи решения относно киберсигурността в различните видове транспорт.

Различните части на инструментариума са свързани посредством хипервръзки, което подпомага навигирането по пътищата за повишаване на осведомеността, адаптирани към конкретните профили в областта на транспорта.

Практиките, изброени в настоящия инструментариум, имат само препоръчителен характер. Нито една формулирана препоръка не е задължителна, нито обвързваща. Освен това настоящият инструментариум не представлява официално становище на Европейската комисия и няма за цел да осигури средства за спазване на съществуващи или бъдещи законодателни актове на ЕС.



Профили, чиято кибернетична осведоменост трябва да бъде повишена

Профил I: всички работещи в сектора на транспорта. Първият път е насочен към целия персонал на организациите в сектора на транспорта — от служителите, извършващи транспортни услуги, до административния персонал. Той предоставя насоки за постигане по-добро разбиране и повишена осведоменост относно най-често срещаните киберзаплахи, насочени към транспортните услуги и системи. Освен това предоставя информация за справяне с потенциални киберзаплахи, включително тяхното установяване, докладване и смекчаване чрез добри практики в областта на киберсигурността.

Профил II: лица, вземащи решения относно киберсигурността в сектора на транспорта. Вторият път е насочен към служителите с правомощия за вземане на решения относно киберсигурността в организациите в сектора на транспорта. При този път се подчертават добрите практики, съобразени с различните видове транспорт, за подобряване на състоянието на киберсигурността на организациите в сектора на транспорта. По-специално той предоставя добри практики за установяване, защита, разкриване и реагиране на възникващи киберзаплахи, насочени към организациите в сектора на транспорта.



Европейска комисия

Инструментариум за киберсигурност в областта на транспорта



Картина на заплахите в сектора на транспорта

Възникващи киберзаплахи, засягащи различните видове транспорт



Профили, чиято кибернетична осведоменост трябва да бъде повишена

Алтернативни пътища за повишаване на кибернетичната осведоменост, насочени към различните видове профили в сектора на транспорта

Европейска комисия

Картина на заплахите в сектора на транспорта



Картината на киберзаплахите в сектора на транспорта е динамична и се променя непрекъснато. Въпреки това е възможно да се установят киберзаплахи, които възникват във всички видове транспорт при експлоатацията на услуги и системи.

Европейска комисия



Участници в заплахи

Физически лица или организации, които потенциално могат да окажат въздействие върху безопасността и сигурността на транспортните услуги и системи



Възникващи киберзаплахи

Избрани киберзаплахи, които потенциално могат да представляват вектори на атаки, влияещи върху безопасността и сигурността на транспортните услуги и системи

Участници в заплахи

Физическите лица или организациите могат волно или неволно да разкрият и използват уязвими места, които могат да предизвикат инциденти и да засегнат транспортните услуги, включително тяхната безопасност, сигурност, работа, финанси и репутация. Сред участниците в заплахи са, наред с други, спонсорирани от държавата групи, киберпрестъпници, кибертерористи, хактивисти, хакери (включително хакери аматьори (скрипт-киди) и лица, злоупотребяващи с вътрешна информация (включително привилегировани такива лица).

Най-значимите злонамерени участници, които умишлено набелязват като своя мишена организации в сектора на транспорта, са **киберпрестъпниците**, **лицата, злоупотребяващи с вътрешна информация**, **националните държави** и **спонсорираните от държавата групи**.
Недоброжелателите, например **киберпрестъпниците**, провеждат масови кампании на кибератаки и често участват в играта заради парични възнаграждения.

Лицата, злоупотребяващи с вътрешна информация, познават особеностите на организациите, за които работят, и често са наясно с едва доловимите уязвими места по отношение на сигурността. Участниците във вътрешни заплахи може да са недоволни служители, доставчици и отделни изпълнители.
Със засилването на глобалното геополитическо напрежение **националните държави** и **спонсорираните от държавата групи** се насочват към стратегически дългосрочни цели. Те често се опитват да се потопят в дълбините на системите на организациите и да събират чувствителна информация. След като навлязат в системите, спонсорираните от държавата лица, извършващи кибератаки, се стремят да заемат позиция, която има потенциала да причини възможно най-големите щети. Например те може да се насочат към системите на други организации, като използват мрежовите им връзки.

Други участници в заплахи са **лицата, злоупотребяващи с вътрешна информация**, които може непреднамерено или случайно да извършат действия, водещи до събития, свързани с киберсигурността, а в най-лошия случай — до киберинциденти, засягащи безопасността и сигурността на транспортните услуги.



Възникващи киберзаплахи

Съществуват значителен брой киберзаплахи за транспорта: **разпределена атака тип „отказ от обслужване“**, **атака тип „отказ от обслужване“**, кражба на данни, **разпространение на малуер**, **фишинг**, манипулиране на софтуер, **неразрешен достъп**, разрушителни кибератаки, фалшифициране или заобикаляне на процеса на вземане на решения от оператора по сигурността, използване на фалшива самоличност, злоупотреба с привилегирован достъп, **социално инженерство**, подправяне на уебсайтове, прихващане на данни, злоупотреба с активи и манипулиране на хардуер.

Въз основа на задълбочено литературно проучване на публично достъпни документи и интервюта с експерти най-сериозните възникващи киберзаплахи, засягащи транспорта, са следните: малуер, (разпределена) атака тип „отказ от обслужване“, неразрешен достъп и кражба и манипулиране на софтуер.



Европейска комисия



Заплаха № 1: малуер

Зловреден софтуер, който потенциално може да засегне физически лица или организации в различните видове транспорт



Заплаха № 2: (разпределена) атака тип „отказ от обслужване“

Атаки срещу киберсигурността, които пречат на физически лица или организации да получат достъп до съответните транспортни услуги и ресурси



Заплаха № 3: неразрешен достъп и кражба

Неразрешен достъп, присвояване и използване на критични активи



Заплаха № 4: манипулиране на софтуер

Атаки срещу киберсигурността, насочени към софтуера, с цел да се промени неговото поведение и извършване на специфични кибератаки

Заплаха № 1: малуер

Малуерът е зловреден софтуер, който може да включва различни видове софтуерни приложения, като вируси, троянски коне, компютърни червеи, софтуер за изнудване, програми за добив на криптовалута или всякакъв друг софтуер, който може да има потенциално неблагоприятно въздействие върху организации или физически лица в различните видове транспорт.

Ограничаването на разпространението на зловреден софтуер, предназначен за умишлено увреждане на компютри, сървъри, клиенти, мрежи или на всички тях, е сред основните приоритети в областта на киберсигурността във всички видове транспорт. Типичният вектор на атака може да включва електронни писма за фишинг, насочени към служители. Други вектори на атака могат да включват различни и сложни стратегии за социално инженерство, като например включване на USB устройство в свободен порт (например при зареждане на мобилен телефон). Като щракне върху хипервръзки в подозрителни електронни писма или като отвори прикачени файлове, потребителят може несъзнателно да инсталира софтуер или съзнателно да застраши транспортните услуги и ресурси.

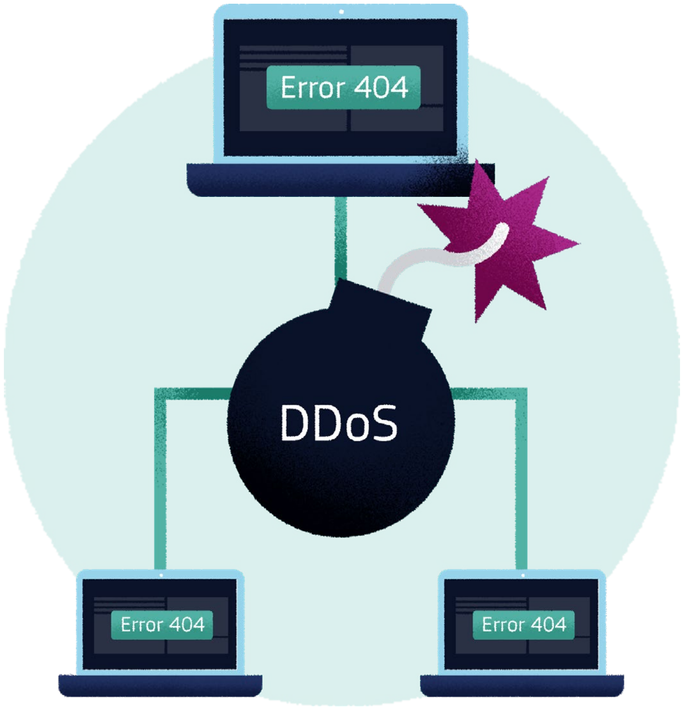
Например кибератаката със софтуер за изнудване WannaCry засегна повече от 150 държави и зарази над 230 000 системи. Това е софтуер за изнудване, който обикновено се разпространява чрез електронни писма с фишинг, съдържащи зловредни прикачени файлове или хипервръзки. При този вид атака се използва злонамерено социалното инженерство с цел подвеждане на потребителите на системата да инсталират (или да активират) определен зловреден софтуер.



Заплаха № 2: (разпределена) атака тип „отказ от обслужване“

Разпределените атаки тип „отказ от обслужване“ (DDoS атаки) и атаките тип „отказ от обслужване“ (DoS атаки) засягат наличието и достъпността на данни, услуги, системи и други ресурси. Тези видове атаки могат да бъдат с различна продължителност и да са насочени към повече от една услуга или система едновременно. При DDoS атаките се използват множество системи (или канали за атака) така, че целевите услуги или системи да се претоварят със заявки. Успешните атаки засягат възможностите на услугите и системите за справяне с неочакван обем заявки. Това води до отказ на достъп до услуги и ресурси.

Следва да се отбележи, че засегнати услуги и системи, принадлежащи на организации в сектора на транспорта, може да бъдат използвани за извършване на DDoS и DoS атаки срещу конкретни системи в експлоатация или други организации.
Може например да бъдат атакувани корпоративни информационни системи (като персонални компютри и устройства), за да се получи достъп до оперативни технологии, които може да бъдат свързани към интернет или мрежи за достъп с цел прехвърляне на оперативни данни. Връзките между различни системи и мрежи (например корпоративни мрежи, оперативни технологии и видове достъп за дистанционна поддръжка) може да представляват уязвими места за извършване на DDoS или DoS атаки срещу транспортни услуги и системи с критичен характер. Така например при DDoS и DoS атаки могат да се използват общи мрежови и комуникационни протоколи, като динамично откриване на уеб услуги (WS-Discovery), което може да се използва при устройства, базирани на интернет на предметите, с цел автоматично откриване на всеки възел в локалните мрежи (LAN). Ако устройствата, базирани на интернет на предметите, представляват уязвими места, лицата, извършващи кибератаки, може да ги използват, за да открият други свързани устройства и да извършат DDoS или DoS атаки.



Заплаха № 3: неразрешен достъп и кражба

Участниците в заплахи може да искат да получат логически или физически достъп без разрешение до мрежа, система, приложение, данни или друг ресурс, за да извършат злоумишлени действия, включително кражба на чувствителни данни или ресурси (включително физически ресурси). Заплахите от неразрешен достъп и кражба са насочени към поверителни и защитени активи (включително самоличности, идентификационни данни за привилегировани акаунти, системи и други видове поверителна и защитена информация). При тези заплахи може да се използват уязвимите места на системите, както и неосведомени лица, които разкриват чувствителни данни, като например идентификационни данни (например потребителско име, парола и др.) или лични данни (например електронна поща, личен идентификационен номер и др.).

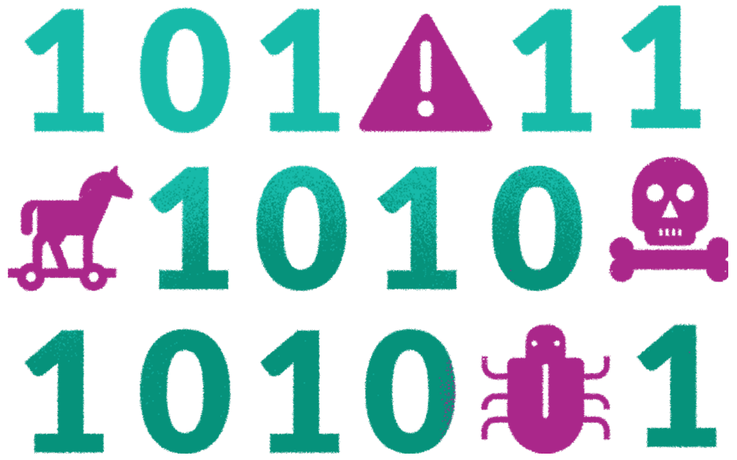
По отношение на неразрешения достъп кражбата на самоличност представлява незаконно използване на лични данни или уникални идентификатори с цел представяне за лица или имитиране на услуги и системи, за да се получи достъп до частни или защитени ресурси (например включително финансови и физически ресурси). Такива киберзаплахи може да бъдат насочени и към физически активи при различните видове транспорт.



Заплаха № 4: манипулиране на софтуер

Неправилното конфигуриране и манипулирането на софтуера и свързаните с него системи или компоненти могат да окажат пряко въздействие върху състоянието на киберсигурността на транспортните услуги и системи. Вследствие на атаките срещу киберсигурността, при които се използва манипулиране на софтуер, се променят настройките на софтуера или се засяга целостта на данните, за да се промени поведението на системите и услугите. Лицата, извършващи кибератаки, може умишлено да манипулират софтуера (или част от него), за да получат предимства (например получаване на неразрешен достъп, възпрепятстване на достъпа на правоимащи лица или системи до необходимите ресурси, събиране на чувствителна информация, промяна на функционалното поведение и т.н.) по отношение на чувствителни активи.

Например лицата, извършващи кибератаки, може да набележат комуникационни канали на производители, за да качат зловредни софтуерни актуализации на услуги и системи в експлоатация (включително оперативни технологии). Лицата, създаващи заплахи, използват идентификационни данни за разрешение с нарушена сигурност, за да получат достъп до защитен мрежов интерфейс за дистанционна поддръжка, с цел да инсталират манипулиран софтуер и да застрашат допълнително други достъпни услуги и системи. Те инсталират манипулиран софтуер, който допълнително застрашава сигурността на целевите услуги и системи, или атакуват други свързани услуги или системи.



Европейска комисия

Профили, чиято кибернетична осведоменост трябва да бъде повишена



Европейска комисия

1

Профил I: всички работещи в сектора на транспорта

Първият път е насочен към всички служители на организациите в сектора на транспорта — от оперативния до административния персонал. При този път се предоставят насоки за постигане на по-добро разбиране и повишена осведоменост относно най-често срещаните киберзаплахи, насочени към транспортните услуги. При него се предоставя и информация за справяне с потенциални киберзаплахи, включително тяхното установяване, докладване и ограничаване чрез добри практики в областта на киберсигурността. Този път е общ за всички видове транспорт.

2

Профил II: лица, вземащи решения относно киберсигурността в сектора на транспорта

Вторият път е насочен към служителите с правомощия за вземане на решения относно сигурността или киберсигурността в организациите в сектора на транспорта. При този път се предоставят добри практики, съобразени с различните видове транспорт. При него се предлагат добри практики за установяване, защита, разкриване и реагиране на възникващи киберзаплахи, насочени към организациите в сектора на транспорта.

Европейска комисия

Профил I: всички работещи в сектора на транспорта

Тази част е насочена към всички служители на организациите в сектора на транспорта — от оперативния до административния персонал. В нея се дават насоки за постигане на по-добро разбиране и повишена осведоменост относно най-често срещаните киберзаплахи, насочени към транспортните услуги. Предоставя се също информация за справяне с потенциални киберзаплахи, включително тяхното установяване, докладване и ограничаване чрез добри практики в областта на киберсигурността.
В тази част са представени препоръчителни практики и полезни съвети, които се отнасят за **всички видове транспорт**.



Добри практики за противодействие на малуер

Можете да помогнете за защитата на Вашата организация, като прилагате добри практики за **установяване и предотвратяване на разпространението на зловреден софтуер**, например:

- *като **спазвате политиките за сигурност**, например сканирате носителите на данни и файловете за наличие на вируси, избягвате отварянето и изпращането по електронна поща на определени видове файлове (например изпълними файлове с разширение .exe, .bat, .com и др.), инсталирате само разрешен софтуер, гарантирате, че софтуерът (включително антивирусният) е актуализиран и функционира правилно, и други политики;*

- *като **създавате редовно резервни копия на данните си** на сигурни (и разрешени) устройства или услуги за съхранение на данни, които следва да поддържат механизми за криптиране, за да се защитят данните в покой, и да бъдат достъпни за процедури за възстановяване на данни;*

- *като защитите с подходящи **мерки за сигурност** (например парола, криптиране и др.) всички системи, включително мобилните и крайните устройства, и не забравяте да заключвате по сигурен начин (физически и цифрово) всички системи, ако са оставени без надзор;*

- *като избягвате да отваряте прикачени файлове и да щракате върху хипервръзки, съдържащи се в неочаквани електронни писма и подозрителни изскачащи прозорци на уеб браузъра със странен текст или от непознати изпращачи и интернет домейни;*

- *като избягвате да поставяте в компютъра си **ненадеждни или непознати преносими устройства**, като USB устройства, твърди дискове и други устройства за съхранение;*

- *като избягвате да деактивирате мерките за защита от малуер (например антивирусен софтуер, софтуер за филтриране на съдържание, защитна стена и др.);*

- *като **актуализирате редовно инсталирания софтуер** с най-новите налични версии (които служителите, отговарящи за информационната сигурност, или системните администратори може да публикуват с редовни актуализации);*

- *като избягвате да използвате привилегировани акаунти (например на равнище администратор) и идентификационни данни за обикновени дейности и операции;*

- *като докладвате на служителите, отговарящи за информационната сигурност, или на системните администратори за подозрителни електронни писма или неочаквано поведение на системата;*

- *като при ежедневната си работа обръщате внимание на информационната сигурност, за да разпознавате проблеми, свързани с информационната сигурност, и да реагирате по подходящ начин.*

Добри практики за противодействие на (разпределена) атака тип „отказ от обслужване“

Можете да помогнете за защитата на Вашата организация, като откривате **разпределени атаки тип „отказ от обслужване“ (DDoS)** и **атаки тип „отказ от обслужване“ (DoS)**. Следва незабавно да се свържете с екипите по сигурността и ИТ екипите на Вашата организация, ако откриете или се сблъскате с някой от следните признаци за евентуални текущи DDoS и DoS атаки срещу Вашите услуги или системи:

- *увеличаване на заявките, които заемат капацитета на мрежата (възприемано като забавени услуги и отговори), което води до сривове в услугите или системата поради претоварване;*

- *увеличаване на потреблението на ресурсите на паметта без очевидна причина;*

- ***неочаквано поведение на услугите и системите**, чести сривове и странни съобщения за грешки поради злоумишлено използване на изчислителни ресурси или мрежови връзки;*

- ***влошени характеристики** на устройствата, продължително изпълнение на обикновени задачи и забележими дейности (например шумен вентилатор, докато устройствата работят бавно);*

- ***неочаквана интернет връзка или загуба на връзка** с услуги и системи;*

- *незабележими промени в поведението на мерките за контрол на управлението или технологиите за управление, които водят до физически повреди;*

- *отказ на достъп до привилегировани или административни акаунти с цел блокиране на възстановяването на процедурите за реагиране при инциденти.*



Добри практики за противодействие на неразрешен достъп и кражби

За да се предотвратят атаки, включващи неразрешен достъп и кражба, е необходимо да бъдат следвани принципи, като *принципа „необходимост да се знае“* и *принципа „сигурност и неприкосновеност на личния живот по подразбиране“*, при които се подчертава, че чувствителните и поверителните активи (включително лични и чувствителни данни, транспортни системи и т.н.) следва да бъдат достъпни само за онези, които имат право на достъп до тях, за да изпълняват задълженията си. Можете да помогнете за защитата на Вашата организация, като прилагате добри практики за установяване и предотвратяване на неразрешен достъп и кражба, например:

- *като спазвате политиките за сигурност на организацията;*
- *като избягвате да споделяте и публикувате онлайн идентификационни данни и лични данни, включително снимки, които могат да съдържат такава информация;*
- *като избягвате да използвате или предавате идентификационни данни и лични данни (и други чувствителни данни) на ненадеждни и несигурни мрежи, устройства или уеб услуги (например уебсайтове, които използват несигурни протоколи или адреси http:// вместо сигурните https://);*
- *като **никога не разкривате пред никого своите идентификационни данни** (например потребителско име и парола), дори по електронна поща или телефон;*
- *като защитавате чувствителните данни, въведени с клавиатурите или показвани на екраните (включително на мобилни устройства), от неоправомощени лица, като поставите върху екрана си защита срещу недискретни погледи и избягвате да работите на обществени места с лични устройства, както и като избягвате да оставяте устройството незаключено и без надзор;*
- *като **използвате сложни пароли** (например достатъчно дълга парола, която е съчетание от буквено-цифрени и специални знаци) съгласно съответните политики на организацията за сигурност, за да предотвратите неразрешен достъп;*
- *като **промените паролите по подразбиране** на свързани системи и устройства (например принтери, маршрутизатори, камери, интелигентни ключалки и др.);*
- *като избягвате да използвате едни и същи идентификационни данни (например потребителско име и парола) за множество услуги и системи и избягвате да използвате едни и същи идентификационни данни за услуги и системи, които изискват привилегировани акаунти;*
- *като изпращате пароли и ключове за прехвърлени защитени файлове (например ZIP архиви) само по канали извън мрежата (например чрез услуга за кратки съобщения (SMS) по GSM и телефонно обаждане) и никога по електронна поща;*
- *като **активирате двуфакторна автентификация (2FA)** или многофакторна автентификация (MFA), ако е възможно.*

Добри практики за противодействие на манипулиране на софтуер

Можете да помогнете за защитата на Вашата организация, като прилагате добри практики за установяване и предотвратяване на манипулиране на софтуер, например:

- *като избягвате да инсталирате ненадежден софтуер в системи и устройства (включително персонални компютри, сървъри, периферни устройства, мрежови устройства, смартфони и др.);*
- *като винаги инсталирате софтуер и актуализации от официални източници и уебсайтове (например производители, корпоративни хранилища и др.);*
- *като избягвате да теглите софтуер и приложения (и всякакви файлове) от незаконни източници;*
- *като деинсталирате ненужен или неизползван наскоро софтуер и деактивирате ненужни връзки (например мрежови протоколи и услуги), включително достъп до дистанционни услуги (например услуги за съхранение „в облак“);*
- *като проверявате софтуера или устройствата за съхранение с надеждна и актуализирана антивирусна програма;*
- *като теглите безопасен промишлен софтуер (например актуализации, корекции, нови продукти и т.н.) от надеждни доставчици на принципа на проверените източници;*
- *като актуализирате целия инсталиран софтуер в съответствие с политиките и практиките на организацията.*



Европейска комисия

Профил II: лица, вземащи решения относно киберсигурността в сектора на транспорта

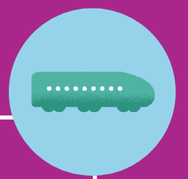
Тази част е насочена към служителите с правомощия за вземане на решения относно сигурността или киберсигурността в организациите в сектора на транспорта. При този път са очертани добри практики, съобразени с различните видове транспорт. По-специално при него се предлагат добри практики за установяване, защита, разкриване и реагиране на възникващи киберзаплахи.



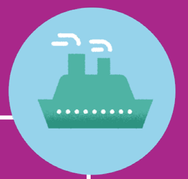
Европейска комисия



Добри практики в областта на киберсигурността за въздушния транспорт



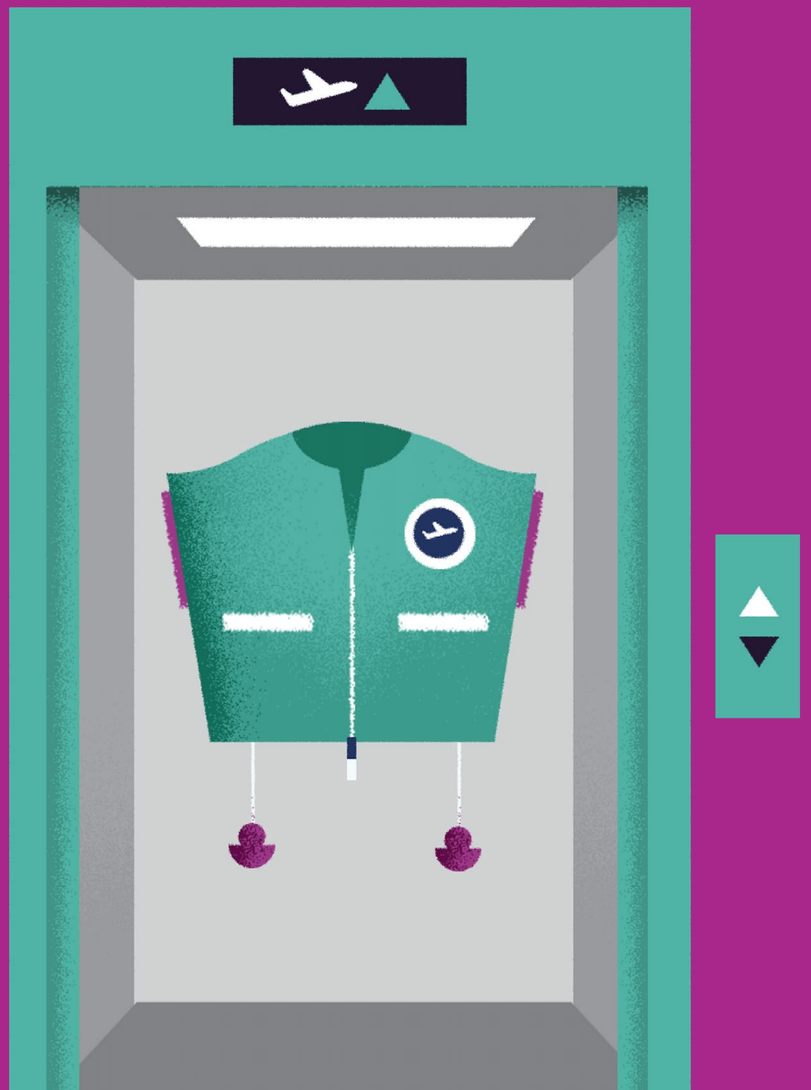
Добри практики в областта на киберсигурността за сухопътния транспорт



Добри практики в областта на киберсигурността за морския транспорт

Европейска комисия

Добри практики и мерки за сигурност, специално пригодени за въздушния транспорт



Управление

Организациите в сектора на въздухоплаването трябва да имат ясна представа за възникващите заплахи, за да определят политиките и процесите на управление, които да направляват подходите им с цел подобряване на киберсигурността на услугите и системите при операциите, включително информационните технологии (ИТ) и оперативните технологии (ОТ).

Добрите практики за организации от всякакъв мащаб включват следното:

- гарантиране, че висшите ръководители докладват за опасенията, свързани с киберсигурността, пред изпълнителното ръководство и управителните съвети, които могат да вземат информирани решения относно разпределението на ресурсите;

- назначаване на високопоставен служител, отговорен за киберсигурността, както и за физическата сигурност, който носи общи управленски отговорности за сигурността на информационните технологии (ИТ) и оперативните технологии (ОТ), но не участва в операциите, за да се избегнат конфликти на интереси;

- ясно определяне на длъжностните функции, отговорностите, компетентностите и разрешенията, свързани с киберсигурността, и съобщаването и съгласуването им със съответния персонал, по-конкретно за членовете на екипите за незабавно реагиране при компютърни инциденти (CERT);

- осигуряване на управление на киберсигурността по цялата верига на доставките на услуги в областта на сигурността, включително физически и цифрови интерфейси, от производителите на технологии и лицата, които ги инсталират, до доставчиците на услуги в областта на сигурността;

- договаряне на дейности и мерки за контрол, включително споделени отговорности, за управление на кибернетичните рискове и гарантиране, че тези отговорности се запазват през целия период на прилагане (например чрез споразумения за услуги) на решенията и услугите в областта на сигурността;

- определяне на механизми за управление (например политики) с цел спазване на задълженията, произтичащи от съответните регламенти и директиви, като например Регламент (ЕС) 2018/1139 относно общи правила в областта на гражданското въздухоплаване и Регламент за изпълнение (ЕС) 2017/373 на Комисията за определяне на общи изисквания за доставчиците на услуги и надзора при управлението на въздушното движение/аеронавигационното обслужване и други мрежови функции за управление на въздушното движение, както и Директивата за мрежова и информационна сигурност (МИС) (Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза).

Европейска комисия

Примери за услуги и системи при въздушния транспорт: примери за информационни технологии са ИТ на разположение на служителите (например персонални компютри, мобилни телефони, периферни офис устройства и т.н.), както и на пътниците (например обществено достъпни маршрутизатори и връзки за безжични локални мрежи (Wi-Fi) и т.н.). Примери за оперативни технологии са системи за надзорен контрол и събиране на данни (SCADA), системи за отопление, вентилация и климатизация (ОВК), пунктове за проверка за сигурност на ръчния багаж, системи за обработка на багажите (BHS), технологии за контрол на достъпа, мониторинг, наблюдение, реагиране на сигнали за тревога и проверки, системи за проверка на осветлението на летищата, радарни системи и сензори, глобални системи за определяне на местоположението (GPS), системи за управление на въздушното движение (УВД), системи за комуникации, навигация и наблюдение (CNS), аеронавигационни информационни системи, метеорологични системи, системи на центровете за оперативна сигурност, бордови системи на авиокомпаниите и др.



Установяване на киберзаплахи

Управление на риска: организациите в сектора на въздухоплаването трябва да предприемат подходящи стъпки за установяване, оценяване и разбиране на кибернетичните рискове за мрежата и информационните системи, подпомагащи изпълнението на основните функции.

За тази цел е необходим цялостен организационен подход за управление на риска, който включва следното:

- *осигуряване на ясна представа за различните хардуерни и софтуерни системи, използвани за предоставяне на различни услуги. В контекста на въздухоплаването тези системи включват информационни технологии (ИТ), както и оперативни технологии (ОТ);*

- *извършване на **оценки на кибернетичния риск**, при които се вземат предвид възникващите заплахи, известните уязвими места и оперативните данни във връзка със системите в тази област. Организации, като Европейският екип за незабавно реагиране при компютърни инциденти в областта на управлението на въздушното движение (EATM-CERT) и центърът за споделяне и анализ на информация в областта на въздухоплаването (A-ISAC), могат да предоставят информация за заплахите, насочени към въздушния транспорт;*

- *гарантиране, че оценките на риска обхващат и рисковете, свързани с ежедневните дейности на персонала (например използване на социални медии, използване на лични устройства, обработване на данни, споделяне на информация и др.);*

- *установяване и прилагане на мерки и планове за третиране на риска с цел намаляване на кибернетичните рискове;*

- *внедряване на цялостна **система за управление на сигурността на информацията** (ISMS) и **система за управление на неприкосновеността на личната информация** (PIMS), съгласувани с други системи за управление. Тези системи за управление (т.е. ISMS и PIMS) включват прилагане на мерки за контрол на сигурността (както и на защитата на данните и неприкосновеността на личния живот), за да се ограничат и предотвратят възникващите заплахи, засягащи сигурността на авиационните услуги и системи (включително на техните данни);*

- *отчитане на всички ограничения, свързани с **управлението на активите и планирането на ресурсите** (т.е. ограниченията, които могат да повлияят на доставката, поддръжката и подпомагането на критичните системи за изпълнение на основните функции в сектора на въздушния транспорт).*

Европейска комисия

Примери за рамки за управление на риска: различни рамки (например семейството стандарти ISO/IEC 27000, рамката за киберсигурност на Националния институт за стандарти и технологии на САЩ, рамката MITRE ATT&CK, BSI IT-Grundschutz и т.н.) може да предоставят информация и да подкрепят адаптиран подход за управление на риска в сектора на въздушния транспорт. Международни организации, като Международната асоциация за въздушен транспорт и Международната организация за гражданско въздухоплаване, предоставят насоки за оценка на кибернетичния риск. Агенцията на Европейския съюз за киберсигурност (ENISA), Агенцията за авиационна безопасност на Европейския съюз (ЕААБ), Евроконтрол и Международният съвет на летищата (ACI), наред с други, очертават добри практики за гарантиране на сигурността на летищата, доставчиците на услуги за управление на въздушното движение и други организации в сектора на въздухоплаването. Съвместното предприятие SESAR координира и обединява всички научноизследователски и развойни дейности (НИРД) на ЕС в областта на управлението на въздушното движение, като обхваща и аспектите на безопасността и сигурността.



Защита от киберзаплахи

Организациите в сектора на въздушния транспорт следва да прилагат подходящи и пропорционални мерки за сигурност, за да защитят от кибератаки мрежите си и информационните си системи, включително информационните технологии (ИТ) и оперативните технологии (ОТ). Мерките за сигурност включват следното:

- ***политики и процеси, свързани със сигурността:*** *определяне, внедряване, съобщаване и прилагане на подходящи политики и процеси, с които се определя цялостен подход към гарантирането на сигурността на системи и данни, подпомагащи изпълнението на основните функции в сектора на въздухоплаването. Тези политики (например политики за пароли и съхранение) и процедури за сигурност следва да обхващат също така управлението на корекциите и уязвимите места на хардуерните и софтуерните системи (включително ИТ и ОТ), управлението на инциденти, защитата на системите и мрежите;*

- ***управление на самоличността и достъпа:*** *разбиране, документиране и управление на достъпа до мрежи и информационни системи (включително ИТ и ОТ), подпомагащи изпълнението на основните функции в сектора на въздушния транспорт. Ползвателите (или автоматизираните функции), които могат да получат достъп до данни или системи, се проверяват, самоличността/автентичността им се удостоверява и им се предоставя разрешение по подходящ начин. При това следва да се вземат предвид и различните длъжностни функции и отговорности за обикновени и привилегировани акаунти;*

- ***сигурност на данните и системата:*** *защита на данните (съхранявани и предавани по електронен път), критичните мрежи и информационни системи (включително ИТ и ОТ) от кибератаки. Като вземат предвид подход, основан на риска, организациите следва да прилагат мерки за сигурност, за да могат ефективно да ограничат възможностите лицата, извършващи кибератаки, да застрашат сигурността на данни, мрежи и системи. Тези мерки за сигурност следва да включват и приемането на протоколи за криптиране и сигурни протоколи за комуникация, за да се защитят данните в покой и данните, които се предават, от киберзаплахи, водещи до атаки тип „човек по средата“. Освен това е необходимо тези мерки да се съчетаят с мерки за физическа сигурност, за да се защити достъпът до системите (например системите следва да бъдат разположени в затворени помещения с ограничен достъп);*

- ***устойчивост на мрежите и системите:*** *изграждане на устойчивост на мрежите и системите (включително ИТ и ОТ) на етапа на проектирането и внедряването им (и чрез техните оперативни процедури), за да се противостои на кибератаки и да се смекчи тяхното въздействие. Примерите за решения за проектиране и внедряване, повишаващи устойчивостта, включват следното: официално проверени критични функции, резервни системи и мрежи, разделяне на мрежите (по-специално разделяне на ИТ от ОТ), мерки за многослойна защита и много други. Следва да се има предвид, че от гледна точка на информационната сигурност областите на сигурност, в които се прилага разделяне на мрежите и системите, могат да предоставят подходящи решения за сигурност. Оперативните нужди (например дейности по поддръжка, прехвърляне на данни и т.н.) на системите обаче може да изискват заобикаляне или свързване на различни области на сигурност (например разделени системи и мрежи), включително свързване на ИТ и ОТ.*

Откриване на киберзаплахи

Организациите следва да гарантират, че мерките за сигурност остават ефективни, и да установяват всички събития, свързани с киберсигурността, които засягат или биха могли да засегнат контрола на сигурността, както и основните услуги и системи. Съответните мерки за сигурност за откриване на киберзаплахи са следните:

- ***наблюдение на сигурността:*** *наблюдение на нивото на сигурност на мрежите и информационните системи, включително информационните технологии (ИТ) и оперативните технологии (ОТ), подпомагащи изпълнението на основните функции при услугите за въздушен транспорт. Данните, които се вземат предвид с оглед подпомагане на наблюдението на сигурността, включват например:*

  - *регистри във връзка със сигурността,*
  - *регистри на откритите вируси,*
  - *регистри на откритите проникванията,*
  - *регистри на идентификациите, автентификациите и разрешенията,*
  - *регистри на системата и обслужването,*
  - *регистри на мрежовия трафик,*
  - *регистри на обработването на данни;*

- ***откриване на събития, свързани със сигурността:*** *откриване на злоумишлени действия (т.е. събития, свързани със сигурността), които засягат или биха могли да засегнат сигурността на мрежите и информационните системи (включително ИТ и ОТ), подпомагащи изпълнението на основните функции при услугите за въздушен транспорт.*

За тези мерки може да е необходимо внедряване на специфични технологии (например управление на информацията и събитията, свързани със сигурността, алармена система против проникване, система за предпазване от нежелани проникванията и т.н.) и създаване на ЦОС (центрове за оперативна сигурност) или еквивалентни на тях, т.е. разработване на средства за откриване, анализиране, реагиране и възстановяване от кибератаки на местно равнище.

Националните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), секторните екипи за незабавно реагиране при компютърни инциденти (например Европейският екип за незабавно реагиране при компютърни инциденти в областта на управлението на въздушното движение (EATM-CERT) на Евроконтрол), търговските екипи за незабавно реагиране при компютърни инциденти към авиокомпаниите и центърът за споделяне и анализ на информация в областта на въздухоплаването (A-ISAC) могат да предоставят разузнавателни данни за киберзаплахите, които да послужат за наблюдението на сигурността и за откриването на събития, свързани със сигурността.

Европейска комисия

Планиране на мерки за реагиране и възстановяване

Организациите следва да определят, да прилагат и да изпитват процедури за управление на инциденти, които са предназначени да гарантират непрекъснатост на дейността при услугите и системите в случай на инциденти в областта на киберсигурността. С мерките за смекчаване се цели овладяване или ограничаване на въздействието на инцидентите в областта на киберсигурността.

При планирането на мерки за реагиране и възстановяване следва да бъдат взети предвид мерки за сигурност, ограничаващи въздействието на конкретни атаки срещу киберсигурността, като например:

- *координация и сътрудничество с националните ЕРИКС, CERT (с обществена и търговска цел) и ISAC по време на инциденти в областта на киберсигурността, координиране във връзка с инциденти и кризи на паневропейско равнище;*

- *споделяне на информация с други организации, включително доставчици във веригата на доставките на авиационни услуги;*

- *провеждане на периодични **учения за реагиране на кибератаки** (координация при симулационно учение, както и техническа координация) с цел оценяване на мерките и процедурите за сигурност, както и устойчивостта на организацията за справяне с киберинциденти;*

- *достъп до места за съхранение на архивирани данни или на резервни копия в случай на нарушена цялост и наличност на хранилища на данни;*

- ***наръчници за сигурност** с подробни процедури за управление на инциденти в областта на киберсигурността и за връщане на услугите и системите към нормални условия на експлоатация;*

- *пренасочвания на мрежовия трафик към резервни канали за обслужване по време на атаки тип „отказ от обслужване“;*

- *процедури за ръчно обработване при работа с услуги и системи във влошен оперативен режим;*

- *определяне на процедури с цел справяне с нарушения на сигурността на данните, включително такива, които засягат лични данни, в съответствие с Общия регламент относно защитата на данните (ОРЗД) и други приложими секторни регламенти или директиви;*

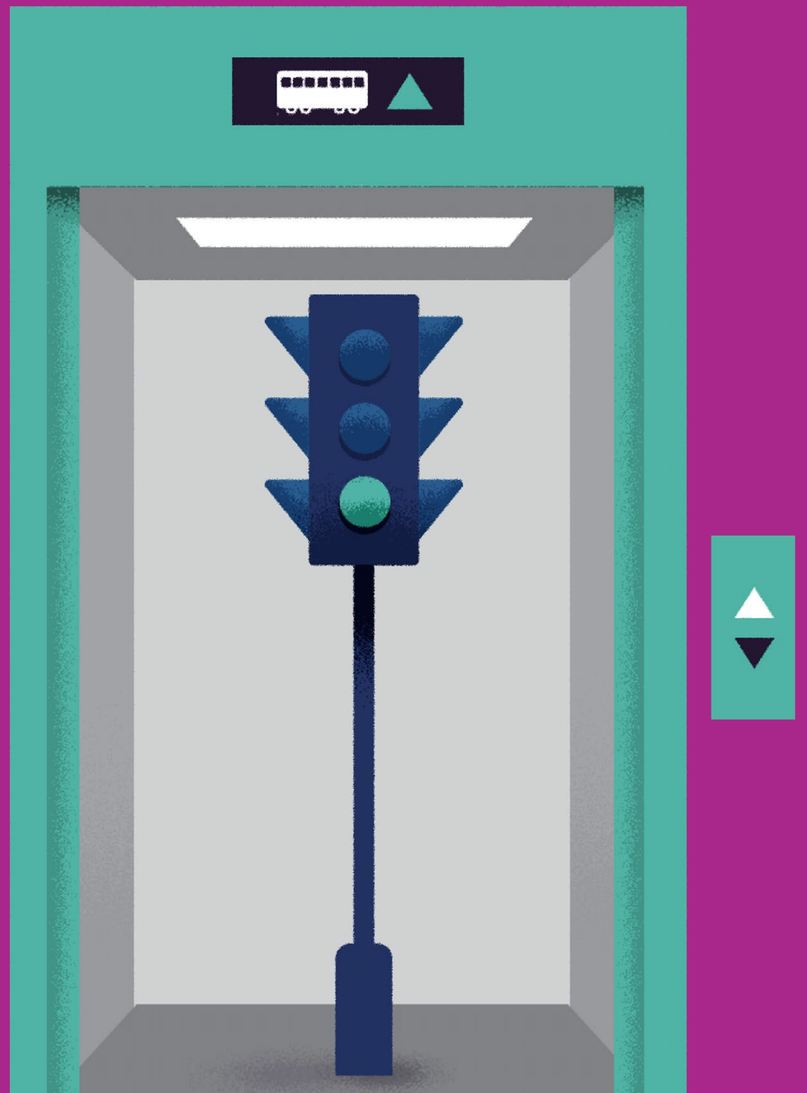
- *закупуване на **застраховка срещу киберинциденти** с цел отчасти да се компенсира рискът, свързан със сериозни киберинциденти;*

- *сключване на договор за предплатени услуги за реагиране при киберинциденти с една или повече специализирани фирми с цел осигуряване на повече капацитет и опит;*

- *определяне на процедури за **споделяне на информация относно инциденти в областта на киберсигурността** със съответните заинтересовани страни, включително процедури за уведомяване за инциденти в съответствие с Директивата за МИС (Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза).*

Европейска комисия

Добри практики и мерки за сигурност, специално пригодени за сухопътния транспорт



Управление

Организациите в сектора на сухопътния транспорт (железопътен и автомобилен) трябва да имат ясна представа за възникващите заплахи, за да определят политиките и процесите на управление, които да направляват подходите им с цел подобряване на киберсигурността на услугите и системите при операциите, включително информационните технологии (ИТ) и оперативните технологии (ОТ).

Добрите практики за организации от всякакъв мащаб включват следното:

- *гарантиране, че висшите ръководители докладват за опасенията, свързани с киберсигурността, пред изпълнителното ръководство и управителните съвети, които могат да вземат информирани решения относно разпределението на ресурсите;*

- *назначаване на високопоставен служител, отговорен за киберсигурността, както и за физическата сигурност, който носи общи управленски отговорности за сигурността на информационните технологии (ИТ) и оперативните технологии (ОТ), но не участва в операциите, за да се избегнат конфликти на интереси;*

- *ясно определяне на длъжностните функции, отговорностите, компетентностите и разрешенията, свързани с киберсигурността, и съобщаването и съгласуването им със съответния персонал. Това е необходимо по-конкретно за членовете на екипите за незабавно реагиране при компютърни инциденти (CERT);*

- *осигуряване на управление на киберсигурността по цялата верига на доставките на услуги в областта на сигурността, включително физически и цифрови интерфейси, от производителите на технологии и лицата, които ги инсталират, до доставчиците на услуги в областта на сигурността;*

- *договаряне на дейности и мерки за контрол, включително споделени отговорности, за управление на кибернетичните рискове и гарантиране, че тези отговорности се запазват през целия период на прилагане (например чрез споразумения за услуги) на решенията и услугите в областта на сигурността;*

- *определяне на механизми за управление (например политики) с цел спазване на задълженията, произтичащи от приложимите регламенти и директиви. Това включва широк кръг от политики, обхващащи конкретните видове транспорт, както и различни типове заинтересовани страни (например включително производители на превозни средства и железопътни системи), а също и Директивата за МИС (Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи).*

Европейска комисия

Примери за услуги и системи при сухопътния транспорт: примери за информационни технологии са ИТ на разположение на служителите (например персонални компютри, мобилни телефони, периферни офис устройства и т.н.), както и на пътниците (например обществено достъпни маршрутизатори и връзки за безжични локални мрежи и т.н.). Примери за оперативни технологии са системи за надзорен контрол и събиране на данни (SCADA), системи за отопление, вентилация и климатизация (ОВК), глобални системи за определяне на местоположението (GPS), технологии за контрол на достъпа, мониторинг, наблюдение, реагиране на сигнали за тревога и проверки. Специфични за железопътния транспорт системи са например следните: оперативни системи (системи за управление и контрол), в т.ч. системи за сигнализация, Европейската система за управление на железопътното движение (ERTMS), бордови системи на влаковете, системи за поддръжка и др.



Европейска комисия

Установяване на киберзаплахи

Управление на риска: организациите в сектора на сухопътния транспорт трябва да предприемат подходящи стъпки за установяване, оценяване и разбиране на кибернетичните рискове за мрежата и информационните системи, подпомагащи изпълнението на основните функции. За тази цел е необходим цялостен организационен подход за управление на риска, който включва следното:

- *осигуряване на ясна представа за различните хардуерни и софтуерни системи, използвани за предоставяне на различни услуги. В контекста на сухопътния транспорт тези системи включват информационни технологии (ИТ), както и оперативни технологии (ОТ);*

- *извършване на **оценки на кибернетичния риск**, при които следва да се вземат предвид възникващите заплахи, известните уязвими места и оперативните данни във връзка със системите в тази област. Примерите за системи при различните видове сухопътен транспорт включват следното: платежни системи, мрежови системи и комуникационни системи (например интернет, радиокомуникация, безжични локални мрежи и др.), бордово оборудване, центрове за оперативен контрол, системи за управление на самоличността, системи за безопасност и други. При железопътната инфраструктура примерите за системи включват следното: подсистеми за управление на подвижния състав, за експлоатация и управление на движението, подсистеми за контрол, управление и сигнализация на борда на влака и по железопътната линия и др.;*

- *гарантиране, че оценките на риска обхващат и рисковете, свързани с ежедневните дейности на персонала (например използване на социални медии, използване на лични устройства, обработване на данни, споделяне на информация и др.);*

- *установяване и прилагане на мерки и планове за третиране на риска с цел намаляване на кибернетичните рискове. Такива са например внедряването на цялостна **система за управление на сигурността на информацията** (ISMS) и **система за управление на неприкосновеността на личната информация** (PIMS), съгласувани с други системи за управление. Тези системи за управление (т.е. ISMS и PIMS) включват прилагане на мерки за контрол на сигурността (както и на защитата на данните и неприкосновеността на личния живот), за да се смекчат и предотвратят възникващите заплахи, засягащи сигурността на услугите и системите за сухопътен транспорт (включително техните данни);*

- *отчитане на всички ограничения, свързани с **управлението на активите и планирането на ресурсите** (т.е. ограниченията, които могат да повлияят на доставката, поддръжката и подпомагането на критичните системи за изпълнение на основните функции в сектора на сухоземния транспорт).*

Европейска комисия

Примери за рамки за управление на риска: различни рамки (например семейството стандарти ISO/IEC 27000, рамката за киберсигурност на Националния институт за стандарти и технологии на САЩ, рамката MITRE ATT&CK, BSI IT-Grundschutz и т.н.) могат да предоставят информация и да подкрепят адаптиран подход за управление на риска в секторите на автомобилния и железопътния транспорт. Организации като ENISA определят добри практики в областта на киберсигурността за интелигентни автомобили и интелигентен обществен транспорт, с които се предоставя информация на производителите и асоциациите от отрасъла (например Европейската асоциация на автомобилните производители — ACEA). В сектора на железниците Агенцията за железопътен транспорт на Европейския съюз определя технически спецификации за оперативна съвместимост (ТСОП), на които трябва да отговаря всяка подсистема или част от подсистема, за да бъдат спазени основните изисквания и да се гарантира оперативната съвместимост на железопътната система в Европейския съюз. Съвместното предприятие S2R (Shift2Rail) също дава тласък на иновативни инициативи и проекти (включително в областта на киберсигурността) за сектора на железопътния транспорт.



Защита от киберзаплахи

Организациите в сектора на сухопътния транспорт следва да прилагат подходящи и пропорционални мерки за сигурност, за да защитят от кибератаки мрежите си и информационните си системи, включително информационните технологии (ИТ) и оперативните технологии (ОТ). Мерките за сигурност включват следното:

- ***политики и процеси, свързани със сигурността:*** *определяне, внедряване, съобщаване и прилагане на подходящи политики и процеси, с които се определя цялостен подход към гарантиране на сигурността на системи и данни, подпомагащи изпълнението на основните функции при различните видове сухопътен транспорт. Тези политики (например политики за пароли и съхранение) и процедури за сигурност следва да обхващат също така управлението на корекциите и уязвимите места на хардуерните и софтуерните системи (включително ИТ и ОТ), управлението на инциденти, защитата на системите и мрежите;*

- ***управление на самоличността и достъпа:*** *разбиране, документиране и управление на достъпа до мрежи и информационни системи (включително ИТ и ОТ), подпомагащи изпълнението на основните функции при видовете сухопътен транспорт. Ползвателите (или автоматизираните функции), които могат да получат достъп до данни или системи, се проверяват, самоличността/автентичността им се удостоверява и им се предоставя разрешение по подходящ начин. При това следва да се вземат предвид и различните длъжностни функции и отговорности за обикновени и привилегировани акаунти;*

- ***сигурност на данните и системата:*** *защита на данните (съхранявани и предавани по електронен път), критичните мрежи и информационни системи (включително ИТ и ОТ) от кибератаки. Като вземат предвид подход, основан на риска, организациите следва да прилагат мерки за сигурност, за да могат ефективно да ограничат възможностите лицата, извършващи кибератаки, да застрашат сигурността на данни, мрежи и системи. Тези мерки за сигурност следва да включват и приемането на протоколи за криптиране и сигурни протоколи за комуникация, за да се защитят данните в покой и данните, които се предават, от киберзаплахи, водещи до атаки тип „човек по средата“. Освен това е необходимо тези мерки да се съчетаят с мерки за физическа сигурност, за да се защити достъпът до системите (например системите следва да бъдат разположени в затворени помещения с ограничен достъп). Това е много важно за онези системи, които може да дават отражение върху безопасността на човешкия живот;*

- ***устойчивост на мрежите и системите:*** *изграждане на устойчивост на мрежите и системите (включително ИТ и ОТ) на етапа на проектирането и внедряването им (и чрез техните оперативни процедури), за да се противостои на кибератаки и да се смекчи тяхното въздействие. Примерите за решения за проектиране и внедряване, повишаващи устойчивостта, включват следното: официално проверени критични функции, резервни системи и мрежи, разделяне на мрежите (по-специално разделяне на ИТ от ОТ), мерки за многослойна защита и много други. Следва да се има предвид, че от гледна точка на информационната сигурност областите на сигурност, в които се прилага разделяне на мрежите и системите, могат да предоставят подходящи решения за сигурност. Оперативните нужди (например дейности по поддръжка, прехвърляне на данни и т.н.) на системите обаче може да изискват заобикаляне или свързване на различни области на сигурност (например разделени системи и мрежи), включително свързване на ИТ и ОТ.*

Откриване на киберзаплахи

Организациите следва да гарантират, че мерките за сигурност остават ефективни, и да установяват всички събития, свързани с киберсигурността, които засягат или биха могли да засегнат контрола на сигурността, както и основните услуги и системи. Съответните мерки за сигурност за откриване на киберзаплахи са следните:

- ***наблюдение на сигурността:*** *наблюдение на нивото на сигурност на мрежите и информационните системи, включително информационните технологии (ИТ) и оперативните технологии (ОТ), подпомагащи изпълнението на основните функции при услугите за различните видове сухопътен транспорт. Това е необходимо, за да се откриват потенциални заплахи за сигурността и да се проследява текущата ефективност на защитните мерки за сигурност. Данните, които се вземат предвид с оглед подпомагане на наблюдението на сигурността, включват например:*

  - *регистри във връзка със сигурността,*
  - *регистри на откритите вируси,*
  - *регистри на откритите проникванията,*
  - *регистри на идентификациите, автентификациите и разрешенията,*
  - *регистри на системата и обслужването,*
  - *регистри на мрежовия трафик,*
  - *регистри на обработването на данни;*

- ***откриване на събития, свързани със сигурността:*** *откриване на злоумишлени действия (т.е. събития, свързани със сигурността), които засягат или биха могли да засегнат сигурността на мрежите и информационните системи (включително ИТ и ОТ), подпомагащи изпълнението на основните функции.*

За тези мерки може да е необходимо внедряване на специфични технологии (например управление на информацията и събитията, свързани със сигурността, алармена система против проникване, система за предпазване от нежелани проникванията и т.н.) и създаване на ЦОС (центрове за оперативна сигурност) или еквивалентни на тях, т.е. разработване на средства за откриване, анализиране, реагиране и възстановяване от кибератаки на местно равнище.
Националните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), секторните екипи и екипите с търговска цел за незабавно реагиране при компютърни инциденти или операторите на автомобилни или железопътни превози, както и центърът за споделяне и анализ на информация в областта на европейския железопътен транспорт (A-ISAC) могат да предоставят разузнавателни данни за киберзаплахите, които да послужат за наблюдението на сигурността и за откриването на събития, свързани със сигурността.



Планиране на мерки за реагиране и възстановяване

Организациите следва да определят, да прилагат и да изпитват процедури за управление на инциденти, които са предназначени да гарантират непрекъснатост на дейността при услугите и системите в случай на инциденти в областта на киберсигурността.

При планирането на мерки за реагиране и възстановяване следва да бъдат взети предвид мерки за сигурност, ограничаващи въздействието на конкретни атаки срещу киберсигурността, като например:

- *координация и сътрудничество с националните ЕРИКС, CERT (с обществена и търговска цел) и ISAC по време на инциденти в областта на киберсигурността, координиране във връзка с инциденти и кризи на паневропейско равнище;*

- *споделяне на информация с други организации, включително доставчици във веригата на доставките на услуги за сухопътен транспорт;*

- *провеждане на периодични **учения за реагиране на кибератаки** (координация при симулационно учение, както и техническа координация) с цел оценяване на мерките и процедурите за сигурност, както и устойчивостта на организациите за справяне с киберинциденти;*

- *достъп до места за съхранение на архивирани данни или на резервни копия в случай на нарушена цялост и наличност на хранилища на данни;*

- ***наръчници за сигурност** с подробни процедури за управление на инциденти в областта на киберсигурността и за връщане на услугите и системите към нормални условия на експлоатация;*

- *пренасочвания на мрежовия трафик към резервни канали за обслужване по време на атаки тип „отказ от обслужване“;*

- *процедури за ръчно обработване при работа с услуги и системи във вложен оперативен режим;*

- *определяне на процедури с цел справяне с нарушения на сигурността на данните, включително такива, които засягат лични данни, в съответствие с Общия регламент относно защитата на данните (ОРЗД) и други приложими секторни регламенти или директиви;*

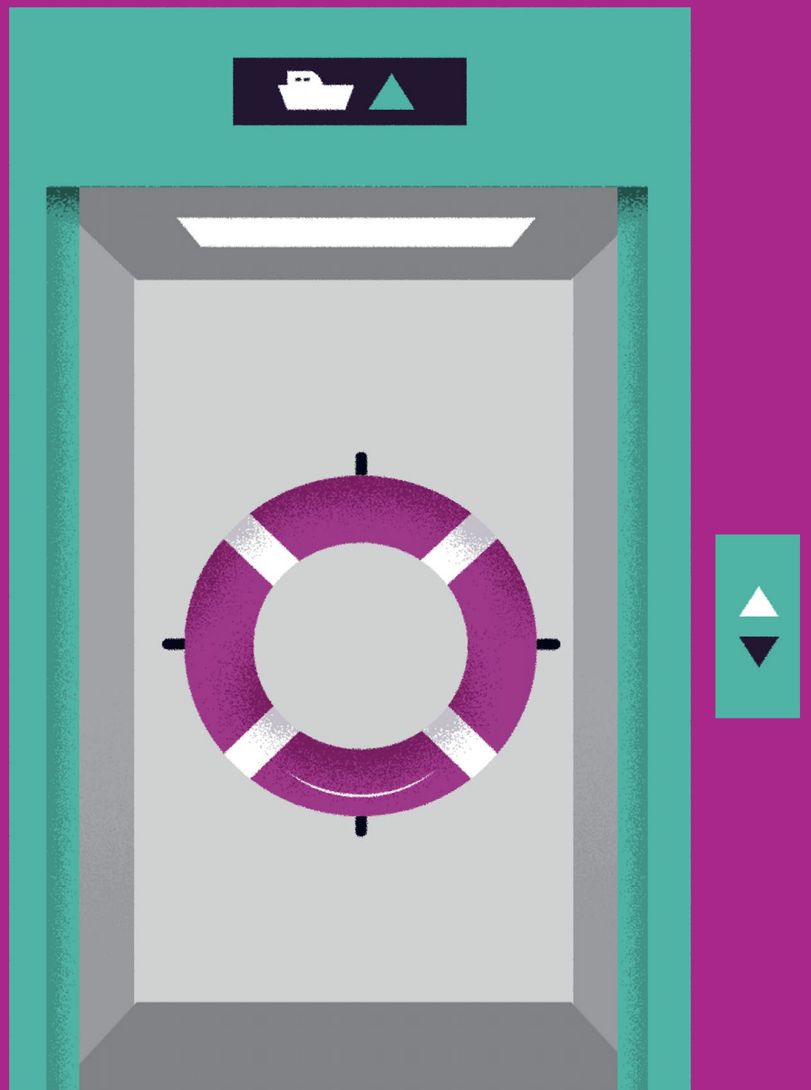
- *закупуване на **застраховка срещу киберинциденти** с цел отчасти да се компенсира рискът, свързан със сериозни киберинциденти;*

- *сключване на договор за предплатени услуги за реагиране при киберинциденти с една или повече специализирани фирми с цел осигуряване на повече капацитет и опит;*

- *определяне на процедури за споделяне на информация относно инциденти в областта на киберсигурността със съответните заинтересовани страни, включително процедури за уведомяване за инциденти в съответствие с Директивата за МИС (Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза).*

Европейска комисия

Добри практики и мерки за сигурност, специално пригодени за морския транспорт



Управление

Организациите в сектора на морския транспорт трябва да имат ясна представа за възникващите заплахи, за да определят политиките и процесите на управление, които да направляват подходите им с цел подобряване на киберсигурността на услугите и системите при операциите, включително информационните технологии (ИТ) и оперативните технологии (ОТ).

Добрите практики за организации от всякакъв мащаб включват следното:

- *гарантиране, че висшите ръководители докладват за опасенията, свързани с киберсигурността, пред изпълнителното ръководство и управителните съвети, които могат да вземат информирани решения относно разпределението на ресурсите;*

- *назначаване на високопоставен служител, който носи общи управленски отговорности за сигурността на информационните технологии (ИТ) и оперативните технологии (ОТ). Тази длъжностна функция следва да отговаря за киберсигурността, както и за физическата сигурност;*

- *ясно определяне на длъжностните функции, отговорностите, компетентностите и разрешенията, свързани с киберсигурността, определяне на равнища на правомощия и на канали за комуникация между персонала на брега и корабния персонал и съгласуването им между съответните служители; Това е необходимо по-конкретно за членовете на екипите за незабавно реагиране при компютърни инциденти (CERT). Персоналът, натоварен с функции във връзка със законодателството на ЕС в областта на морската сигурност и безопасност, като например служителите по сигурността на пристанищните съоръжения, служителите по сигурността на пристанището или служителите по сигурността на компанията, или упълномощеното лице на брега и капитанът, следва поне да са запознати с мерките за защита на киберсигурността, предприети от организацията;*

- *осигуряване на управление на киберсигурността по цялата верига на доставките на услуги в областта на сигурността, включително физически и цифрови интерфейси, от производителите на технологии и лицата, които ги инсталират, до доставчиците на услуги в областта на сигурността;*

- *договаряне на дейности и мерки за контрол, включително споделени отговорности, за управление на кибернетичните рискове и гарантиране, че тези отговорности се запазват през целия период на прилагане (например чрез споразумения за услуги) на решенията и услугите в областта на сигурността;*

- *определяне на механизми за управление (например политики) с цел спазване на задълженията, произтичащи от приложимите регламенти и директиви, например Регламент (ЕС) 2019/1239 за създаване на единна европейска среда за морско информационно обслужване, Регламент (ЕО) № 725/2004 относно подобряване на сигурността на корабите и на пристанищните съоръжения, Директива 2005/65/ЕО за повишаване на сигурността на пристанищата и Регламент (ЕО) № 336/2006 за прилагане на Международния кодекс за управление на безопасността (Кодекс за ISM) и Резолюция A.741(18) относно приемането на Международния кодекс за управление на безопасната експлоатация на кораби и предотвратяване на замърсяването. В този контекст е уместно също така да се спомене общата среда за обмен на информация (CISE) — инициатива на ЕС, насочена към постигане на оперативна съвместимост между системите за наблюдение на ЕС и на държавите членки, за да се осигури на всички съответни органи достъп до класифицираната и некласифицираната информация, която им е необходима за провеждане на мисии в морето.*

Примери за услуги и системи при морския транспорт: примери за информационни технологии са ИТ на разположение на служителите (например персонални компютри, мобилни телефони, периферни офис устройства и т.н.), както и на пътниците (например обществено достъпни маршрутизатори и връзки за безжични локални мрежи и т.н.). Примери за оперативни технологии са системи за надзорен контроли събиране на данни (SCADA), системи за отопление, вентилация и климатизация (ОВК), глобални системи за определяне на местоположението (GPS), технологии за контрол на достъпа, мониторинг, наблюдение, реагиране на сигнали за тревога и проверки, бордови навигационни системи, SafeSeaNet, мостови системи, системи за обработка и управление на товари, системи за управление на задвижващи модули и машини и контрол на мощността, системи за контрол на достъпа, системи за обслужване и организация на пътници, ориентирани към пътници обществени мрежи, системи за осигуряване на добри условия за административния персонал и екипажа, системи за комуникация и др.



Установяване на киберзаплахи

Управление на риска: организациите в сектора на морския транспорт трябва да предприемат подходящи стъпки за установяване, анализиране, оценяване и уведомяване за кибернетичните рискове и за приемането, избягването, прехвърлянето или ограничаването им до приемливо равнище. За тази цел е необходим цялостен организационен подход за управление на риска, който включва следното:

- *осигуряване на ясна представа за различните хардуерни и софтуерни системи, използвани за предоставяне на различни услуги. В контекста на морския транспорт тези системи включват информационни технологии (ИТ), както и оперативни технологии (ОТ), и начините на свързване и интегриране на тези системи със съоръженията на брега, включително публичните органи, морските терминали и операторите на терминали;*

- *установяване и оценяване на основните операции на борда на кораба, които са уязвими на кибератаки, и извършване на оценки на кибернетичния риск (включително оценяване на потенциалните оперативни въздействия и вероятността те да възникнат), при които следва да се вземат предвид възникващите заплахи, известните уязвими места и оперативните данни във връзка със системите в тази област. Когато е целесъобразно, да се направи връзка с оценките на сигурността, извършвани за кораби (оценка на сигурността на кораба), пристанищни съоръжения (оценка на сигурността на пристанищното съоръжение) и пристанища (оценка на сигурността на пристанището), както е посочено в законодателството на ЕС в областта на морската сигурност. Чрез тях се откриват възможни заплахи за сигурността на пристанищната инфраструктура и слабости по отношение на сигурността. Освен това морски организации, като Международната морска организация (ИМО) и морските центрове за споделяне и анализ на информация, могат да предоставят сведения относно заплахите, насочени към морския транспорт.*

- *гарантиране, че оценките на риска обхващат и рисковете, свързани с ежедневните дейности на персонала (например използване на социални медии, използване на лични устройства, обработване на данни, споделяне на информация и др.);*

- *установяване и прилагане на мерки и планове за третиране на риска с цел намаляване на кибернетичните рискове. Такива са например внедряването на цялостна система за управление на сигурността на информацията (ISMS) и система за управление на неприкосновеността на личната информация (PIMS), съгласувани с други системи за управление, като например системи за управление на безопасността, съответстващи на Международния кодекс за управление на безопасността (Кодекса за ISM). Тези системи за управление (т.е. ISMS и PIMS) включват прилагане на мерки за контрол на сигурността (както и на защитата на данните и неприкосновеността на личния живот), за да се смекчат и предотвратят възникващите заплахи, засягащи сигурността на услугите и системите за морски транспорт (включително техните данни);*

- *отчитане на всички ограничения, свързани с **управлението на активите и планирането на ресурсите** (т.е. ограниченията, които могат да повлияят на доставката, поддръжката и подпомагането на критичните системи за изпълнение на основните функции в сектора на морския транспорт). По отношение на оценките следва, когато е уместно, да се направи препратка към изискванията на Кодекса за ISM, системите за управление на безопасността и плановете за сигурност, изпълнявани съгласно законодателството на ЕС в областта на морската сигурност и безопасност.*

Примери за рамки за управление на риска: различни рамки (например Кодексът за ISM или семейството стандарти ISO/IEC 27000, рамката за киберсигурност на Националния институт за стандарти и технологии на САЩ, рамката MITRE ATT&CK, BSI IT-Grundschutz и т.н.) могат да предоставят информация и да подкрепят адаптиран подход за управление на риска в сектора на морския транспорт. Рамката за киберсигурност на Националния институт за стандарти и технологии на САЩ също така е специално адаптирана да обхваща киберсигурността при преноса на насипни течни товари с морски транспорт (Maritime Bulk Liquids Transfer — MBLT), дейностите в крайбрежни води и дейностите на пътнически кораби. По подобен начин Балтийският и международен морски съвет (BIMCO) е издал *„Насоки за киберсигурност на борда на кораби“ („The Guidelines on Cyber Security Onboard Ships“)*, а Международната морска организация (ИМО) е публикувала специални *„Насоки за управление на кибернетичния риск при морския транспорт“ („Guidelines on maritime cyber risk management“)* (MSC-FAL.1/Circ.3). ENISA е провела няколко проучвания, свързани с добрите практики в областта на морската киберсигурност, по-специално киберсигурността на пристанищата. Европейската агенция по морска безопасност (ЕАМБ) предоставя услуги на морската общност, включително обучения за повишаване на кибернетичната осведоменост. Също така специални изисквания за сигурност и безопасност за системите и мрежите на морския транспорт са определени в стандарти (например IEC 61162-460:2018 „Безопасност и сигурност на системи и съоръжения за морска навигация и радиосъобщения“, ISO 16425:2013 „Кораби и морски технологии“, IEC 62443-4-1:2018 „Сигурност на промишлени системи за автоматизация и управление“ и др.).



Защита от киберзаплахи

Организациите в сектора на морския транспорт следва да прилагат подходящи и пропорционални мерки за сигурност, за да защитят от кибератаки мрежите си и информационните си системи, включително информационните технологии (ИТ), като оперативните мерки за сигурност включват следното:

- ***политики и процеси, свързани със сигурността:*** *определяне, внедряване, съобщаване и прилагане на подходящи политики и процеси, с които се определя цялостен подход към гарантиране на сигурността на системи и данни, подпомагащи изпълнението на основните функции в сектора на морския транспорт. В съответните планове, като например системата за управление на безопасността, и в плана за сигурност на корабите следва да бъдат включени мерки за сигурност (в т.ч. мерки за киберсигурност и за физическа сигурност). Тези политики (например политики за пароли и съхранение) и процедури за сигурност следва да обхващат също така управлението на корекциите и уязвимите места на хардуерните и софтуерните системи (включително ИТ и ОТ), управлението на инциденти, защитата на системите и мрежите;*

- ***управление на самоличността и достъпа:*** *разбиране, документиране и управление на достъпа до мрежи и информационни системи (включително ИТ и ОТ), подпомагащи изпълнението на основните функции в сектора на морския транспорт. Ползвателите (или автоматизираните функции), които могат да получат достъп до данни или системи, се проверяват, самоличността/автентичността им се удостоверява и им се предоставя разрешение по подходящ начин. При това следва да се вземат предвид и различните длъжностни функции и отговорности за обикновени и привилегировани акаунти;*

- ***сигурност на данните и системата:*** *защита на данните (съхранявани и предавани по електронен път), критичните мрежи и информационни системи (включително ИТ и ОТ) от кибератаки. Като вземат предвид подход, основан на риска, организациите следва да прилагат мерки за сигурност, за да може ефективно да ограничат възможностите лицата, извършващи кибератаки, да застрашат сигурността на данни, мрежи и системи. Тези мерки за сигурност следва да включват и приемането на протоколи за криптиране и сигурни протоколи за комуникация, за да се защитят данните в покой и данните, които се предават, от киберзаплахи, водещи до атаки тип „човек по средата“. Освен това е необходимо тези мерки да се съчетаят с мерки за физическа сигурност, за да се защити достъпът до системите (например системите следва да бъдат разположени в затворени помещения с ограничен достъп). Това е много важно за онези системи, които може да дават отражение върху безопасността на човешкия живот (например навигационни системи и системи за радиокомуникация от категории II и III);*

- ***устойчивост на мрежите и системите:*** *изграждане на устойчивост на мрежите и системите (включително ИТ и ОТ) на етапа на проектирането и внедряването им (и чрез техните оперативни процедури), за да се противостои на кибератаки и да се смекчи тяхното въздействие. Примерите за решения за проектиране и внедряване, повишаващи устойчивостта, включват следното: официално проверени критични функции, резервни системи и мрежи, разделяне на мрежите (по-специално разделяне на ИТ от ОТ), мерки за многослойна защита и много други. Следва да се има предвид, че от гледна точка на информационната сигурност областите на сигурност, в които се прилага разделяне на мрежите и системите, могат да предоставят подходящи решения за сигурност. Въпреки това нуждите (например дейности по поддръжка, прехвърляне на данни и т.н.) на системите (например „Автономни морски надводни кораби“ (Maritime Autonomous Surface Ships — MASS) може да изискват заобикаляне или свързване на различни области на сигурност (например разделени системи и мрежи), включително свързване на ИТ и ОТ.*

Откриване на киберзаплахи

Организациите следва да гарантират, че мерките за сигурност остават ефективни, и да установяват всички събития, свързани с киберсигурността, които засягат или биха могли да засегнат контрола на сигурността, както и основните услуги и системи. Съответните мерки за сигурност за откриване на киберзаплахи са следните:

- ***наблюдение на сигурността:*** *наблюдение на нивото на сигурност на мрежите и информационните системи, включително информационните технологии (ИТ) и оперативните технологии (ОТ), подпомагащи изпълнението на основните функции при услугите за морски транспорт. Това е необходимо, за да се откриват потенциални заплахи за сигурността и да се проследява текущата ефективност на защитните мерки за сигурност. Данните, които се вземат предвид с оглед подпомагане на наблюдението на сигурността, включват например:*

  - *регистри във връзка със сигурността,*
  - *регистри на откритите вируси,*
  - *регистри на откритите прониквания,*
  - *регистри на идентификациите, автентификациите и разрешенията,*
  - *регистри на системата и обслужването,*
  - *регистри на мрежовия трафик,*
  - *регистри на обработването на данни;*

- ***откриване на събития, свързани със сигурността:*** *откриване на злоумишлени действия (т.е. събития, свързани със сигурността), които засягат или биха могли да засегнат сигурността на мрежите и информационните системи (включително ИТ и ОТ), подпомагащи изпълнението на основните функции при услугите за морски транспорт.*

За тези мерки може да е необходимо внедряване на специфични технологии (например управление на информацията и събитията, свързани със сигурността, алармена система против проникване, система за предпазване от нежелани прониквания и т.н.) и създаване на ЦОС (центрове за оперативна сигурност) или еквивалентни на тях, т.е. разработване на средства за откриване, анализиране, реагиране и възстановяване от кибератаки на местно равнище.

Националните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), секторните екипи за незабавно реагиране при компютърни инциденти (CERT) и търговските CERT на операторите на морски транспорт, центровете за споделяне и анализ на информация (ISAC) в областта на морския транспорт могат да предоставят разузнавателни данни за киберзаплахите, които да послужат за наблюдението на сигурността и за откриването на събития, свързани със сигурността.

Планиране на мерки за реагиране и възстановяване

Организациите следва да определят, да прилагат и да изпитват процедури за управление на инциденти, които са предназначени да гарантират непрекъснатост на дейността при услугите и системите в случай на инциденти в областта на киберсигурността.
При планирането на мерки за реагиране и възстановяване следва да бъдат взети предвид мерки за сигурност, ограничаващи въздействието на конкретни атаки срещу киберсигурността, като например:

- *пренасочвания на мрежовия трафик към резервни канали за обслужване по време на атаки тип „отказ от обслужване“;*
- *процедури за ръчно обработване при работа с услуги и системи във влошен оперативен режим;*
- *създаване на програми за тренировки и учения (например координация при симулационно учение, технически тренировки и тренировки за реагиране), за да се отговори на кибератаки и извънредни ситуации, а също и с цел оценяване на мерките и процедурите за сигурност, както и устойчивостта на организациите за справяне с киберинциденти;*
- *достъп до места за съхранение на архивирани данни или на резервни копия в случай на нарушена цялост и наличност на хранилища на данни;*
- *координация и сътрудничество с националните ЕРИКС, CERT (с обществена и търговска цел) и ISAC по време на инциденти в областта на киберсигурността, координиране във връзка с инциденти и кризи на паневропейско равнище;*
- *споделяне на информация с други организации, включително доставчици във веригата на доставките на услуги за морски транспорт;*
- *наръчници за сигурност с подробни процедури за управление на инциденти в областта на киберсигурността и за връщане на услугите и системите към нормални условия на експлоатация;*
- *определяне на процедури с цел справяне с нарушения на сигурността на данните, включително такива, които засягат лични данни, в съответствие с Общия регламент относно защитата на данните (ОРЗД) и други приложими секторни регламенти или директиви;*
- *закупуване на застраховка срещу киберинциденти с цел отчасти да се компенсира рискът, свързан със сериозни киберинциденти;*
- *сключване на договор за предплатени услуги за реагиране при киберинциденти с една или повече специализирани фирми с цел осигуряване на повече капацитет и опит;*
- *определяне на процедури за споделяне на информация относно инциденти в областта на киберсигурността (включително несъответствия, произшествия и опасни ситуации) със съответните заинтересовани страни, включително процедури за уведомяване за инциденти в съответствие с Директивата за МИС (Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза).*

Изложените в настоящата публикация информация и възгледи са тези на автора(ите) и не отразяват непременно официалното становище на Комисията. Комисията не гарантира точността на данните, включени в настоящата публикация. Нито Комисията, нито друго действащо от нейно име лице може да носи отговорност за евентуалната употреба на съдържащата се в нея информация.

Люксембург: Служба за публикации на Европейския съюз, 2021 г.

© Европейски съюз, 2021 г.
Повторната употреба е разрешена, при условие че се посочи източникът и оригиналното значение или послание на настоящия документ не е изкривено. Европейската комисия не носи никаква отговорност за каквито и да е последици от повторното използване на настоящата публикация. Политиката по отношение на повторната употреба на документи на Европейската комисия е уредена с Решение 2011/833/ЕС на Комисията от 12 декември 2011 г. относно повторната употреба на документи на Комисията (ОВ L 330, 14.12.2011 г., стр. 39).

За употребата или възпроизвеждането на елементи, които не са собственост на Европейския съюз, трябва да се поиска разрешение директно от носителите на авторските права.

Print ISBN 978-92-76-40483-5 doi:10.2832/478224 MI-05-21-230-BG-C
PDF ISBN 978-92-76-40503-0 doi:10.2832/519180 MI-05-21-230-BG-N

Служба за публикации на Европейския съюз