Il-Kummissjoni Ewropea

Sett ta’ Għodod għaċ-Ċibersigurtà tat-Trasport

Introduzzjoni

Id-Direttorat Ġenerali għall-Mobilità u t-Trasport tal-Kummissjoni Ewropea (DĠ Mobilità u Trasport) ikkuntratta l-iżvilupp ta' dan is-sett ta' għodod biex itejjeb is-sensibilizzazzjoni u t-tħejjija tal-partijiet ikkonċernati tat-trasport għat-theddid ċibernetiku. Dan jipprovdi għarfien għall-fehim tat-theddid ċibernetiku u l-mitigazzjoni tal-impatt tagħhom fuq is-servizzi, is-sistemi u l-operazzjonijiet tat-trasport. Dan is-sett ta' għodod jipprovdi mogħdijiet ta' sensibilizzazzjoni alternattivi mmirati lejn profili differenti tat-trasport:

- Il-persunal kollu tat-trasport (li jipprovdi informazzjoni u gwida ġenerali)
- Dawk li jieħdu d-deċiżjonijiet dwar it-trasport fiċ-ċibersigurtà fil-modi differenti tat-trasport.

L-iperlinks jgħaqqdu l-partijiet differenti li jiffurmaw is-sett ta' għodod sabiex jappoġġaw in-navigabbiltà tal-mogħdijiet ta' sensibilizzazzjoni mfassla għall-profili speċifiċi tat-trasport.

Il-prattiki elenkati f'dan is-sett ta' għodod huma ta' natura konsultattiva biss. Kwalunkwe rakkomandazzjoni li hija fformulata la hija vinkolanti u lanqas obbligatorja. Barra minn hekk, dan is-sett ta' għodod ma jirrappreżentax il-fehmiet formali tal-Kummissjoni Ewropea u ma huwiex maħsub biex jipprovdi mezzi ta' konformità mal-leġiżlazzjonijiet eżistenti jew futuri tal-UE.

Profili ta’ Sensibilizzazzjoni dwar iċ-Ċibersigurtà

Profil I: Il-persunal tat-trasport kollu. L-ewwel mogħdija għandha fil-mira l-persunal kollu tal-organizzazzjonijiet tat-trasport, mill-persunal fl-operazzjonijiet tas-servizzi tat-trasport sal-persunal amministrattiv. Dan jipprovdi gwida lejn fehim u sensibilizzazzjoni akbar dwar l-aktar theddid ċibernetiku komuni mmirat lejn is-servizzi u s-sistemi tat-trasport. Barra minn hekk, jipprovdi għarfien dwar kif għandhom jiġu indirizzati t-theddidiet ċibernetiċi potenzjali, inkluż l-identifikazzjoni, ir-rapportar, u l-mitigazzjoni tagħhom permezz ta’ prattiki tajbin taċ-ċibersigurtà.

Profil II: Dawk li jieħdu d-deċiżjonijiet fuq affarijiet relatati maċ-ċibersigurtà tat-trasport. It-tieni mogħdija hija mmirata lejn il-persunal li għandu responsabbiltajiet ta’ teħid ta’ deċiżjonijiet għaċ-ċibersigurtà fl-organizzazzjonijiet tat-trasport. Din il-mogħdija tenfasizza prattiki tajbin imfassla għall-modi differenti tat-trasport għat-tisħiħ tal-pożizzjoni taċ-ċibersigurtà tal-organizzazzjonijiet tat-trasport. Partikolarment, dan jipprovdi prattiki tajbin sabiex jidentifika, jipproteġi, isib u jirrispondi għat-theddid ċibernetiku emerġenti mmirat lejn l-organizzazzjonijiet tat-trasport.

Il-Kummissjoni Ewropea

Sett ta’ Għodod għaċ-Ċibersigurtà tat-Trasport

Xenarju ta’ Theddid għat-Trasport

Theddid ċibernetiku emerġenti li jaffettwa modi differenti ta’ trasport

Profili ta’ Sensibilizzazzjoni dwar iċ-Ċibersigurtà

mogħdijiet alternattivi ta’ sensibilizzazzjoni dwar iċ-ċibersigurtà mmirati lejn profili differenti tat-trasport

Il-Kummissjoni Ewropea

Xenarju tat-Theddid għat-Trasport

Ix-xenarju tat-theddid ċibernetiku huwa dinamiku u qed jevolvi kontinwament. Madankollu, huwa possibbli li jiġu identifikati t-theddidiet ċibernetiċi, li l-modi kollha tat-trasport jiffaċċjaw fl-operazzjonijiet tas-servizzi u tas-sistemi.

Il-Kummissjoni Ewropea

L-Awturi tat-Theddid

Individwi jew organizzazzjonijiet li jistgħu potenzjalment ikollhom impatt fuq is-sikurezza u s-sigurtà tas-servizzi u s-sistemi tat-trasport

Theddid Ċibernetiku Emerġenti

Theddid ċibernetiku magħżul li jista' potenzjalment jirrappreżenta vetturi ta' attakk li għandhom impatt fuq is-sikurezza u s-sigurtà tas-servizzi u s-sistemi tat-trasport

Awturi tat-Theddid

L-individwi jew l-organizzazzjonijiet jistgħu jesponu u jisfruttaw intenzjonalment jew mhux intenzjonalment vulnerabbiltajiet, li għandhom il-potenzjal li jikkawżaw aċċidenti u li jaffettwaw is-servizzi tat-trasport inkluż is-sikurezza, is-sigurtà, in-negozju, il-finanzi u r-reputazzjoni tagħhom. L-awturi tat-theddid jinvolvu, fost l-oħrajn, gruppi sponsorjati mill-Istat, kriminali ċibernetiċi, terroristi ċibernetiċi, hacktivisti, hackers (inkluż script kiddies), u persuni ta' ġewwa (inklużi persuni ta' ġewwa privileġġati).

L-aktar awturi malizzjużi sinifikanti li jimmiraw intenzjonalment organizzazzjonijiet tat-trasport huma **l-kriminali ċibernetiċi**, **il-persuni ta' ġewwa**, **l-istati nazzjon** u **l-gruppi sponsorjati mill-Istat**.
L-avversarji bħall-**kriminali ċibernetiċi** jwettqu kampanji ta' attakk enormi u spiss jagħmlu dan għal gwadanji monetarji.

Il-persuni ta' ġewwa, jafu l-karatteristiċi uniċi tal-organizzazzjonijiet li jaħdmu għalihom u spiss ikunu konxji sew ta' vulnerabbiltajiet tas-sigurtà sottili. L-awturi tat-theddid minn ġewwa jistgħu jinvolvu impjegati, fornituri u kuntratturi individwali mdejqin.
Hekk kif it-tensjonijiet ġeopolitiċi globali qegħdin jintensifikaw, **l-istati nazzjon** u **l-gruppi sponsorjati mill-Istat** għandhom fil-mira objettivi strateġiċi fit-tul. Spiss jippruvaw jaħbu lilhom infushom fil-fond tas-sistemi tal-organizzazzjonijiet u jiġbru informazzjoni sensittiva. Ladarba jistabbilixxu posthom fis-sistemi, l-attakkanti sponsorjati mill-Istat ifittxu li jiksbu pożizzjoni li għandha l-potenzjal li toħloq l-agħar ħsara possibbli. Pereżempju, dawn jistgħu jpoġġu fil-mira tagħhom sistemi ta' organizzazzjonijiet oħrajn billi jisfruttaw il-konnessjonijiet tan-network tal-organizzazzjonijiet.

Awturi oħrajn tat-theddid jinvolvu **persuni ta' ġewwa**, li jistgħu jwettqu azzjonijiet mhux intenzjonalment jew aċċidentali li jirriżultaw f'eventi taċ-ċibersigurtà u, fl-agħar każijiet, aċċidenti ċibernetiċi li jaffettwaw is-sikurezza u s-sigurtà tas-servizzi tat-trasport.

Theddid Ċibernetiku Emerġenti

Hemm għadd sostanzjali ta' theddid ċibernetiku mmirat lejn it-trasport: **ċaħda tas-servizzi distribwita**, **ċaħda tas-servizzi**, serq ta' *data*, **tixrid ta' malware**, **phishing**, manipulazzjoni tas-software, **aċċess mhux awtorizzat**, attakki qerrieda, falsifikazzjoni jew evitar tal-proċess tad-deċiżjoni tal-operatur tas-sigurtà, attakki maskarati fuq l-identità, abbuż tal-privileġġi tal-aċċess, **inġinerija soċjali**, defacement, interċettazzjoni, użu ħażin tal-assi, u manipulazzjoni tal-hardware.
Skont riċerka komprensiva fil-letteratura ta' dokumentazzjonijiet disponibbli għall-pubbliku u intervisti mal-esperti, l-aktar theddid ċibernetiku emerġenti urġenti li jaffettwa t-trasport huwa: Malware, Ċaħda ta' Servizz (Distribwita), Aċċess Mhux Awtorizzat u Serq, u Manipulazzjoni ta' Software.

Il-Kummissjoni Ewropea

Theddida #1: Malware

Software malizzjuż li jista' potenzjalment jaffettwa lill-individwi jew lill-organizzazzjonijiet fil-modi kollha tat-trasport

Theddida #2: Ċaħda tas-servizzi (distribwita)

Attakki fuq iċ-Ċibersigurtà li jipprevjenu lill-individwi jew lill-organizzazzjonijiet milli jaċċessaw servizzi u riżorsi tat-trasport rilevanti

Theddida #3: Aċċess mhux Awtorizzat u Serq

Aċċess, approprjazzjoni, u sfruttament mhux awtorizzati ta' assi kritiċi

Theddida #4: Manipulazzjoni tas-Software

Attakki fuq iċ-Ċibersigurtà mmirati lejn is-software sabiex jimmodifikaw l-imġiba tiegħu u jwettqu attakki speċifiċi

Theddida #1: Malware

Malware jikkonsisti f'software malizzjuż, li jista' jinkludi tipi differenti ta' applikazzjonijiet tas-software bħal viruses, trojans, worms, ransomwares, cryptocurrency-miners, jew kwalunkwe software li jista' jkollu impatti potenzjalment negattivi fuq organizzazzjonijiet jew individwi fil-modi kollha tat-trasport.

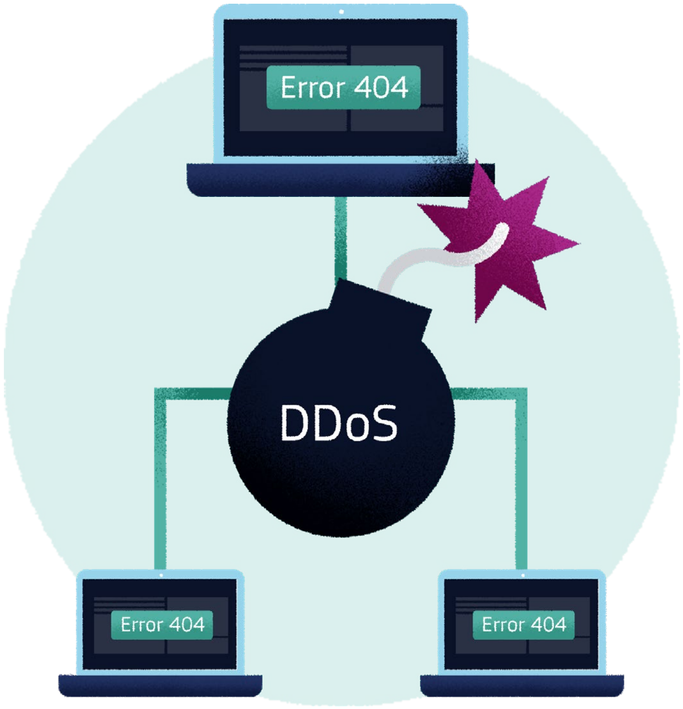
Il-mitigazzjoni tat-tixrid ta' malware iddisinjat biex jagħmel ħsara intenzjonalment lil kompjuters, servers, klijenti, networks, jew kollha kemm huma hija fost il-prijoritajiet ewlenin taċ-ċibersigurtà fil-modi kollha tat-trasport. Vettur tipiku ta' attakk jista' jinvolvi ittri elettroniċi ta' phishing immirati lejn l-impjegati. Vetturi oħrajn ta' attakk jistgħu jinvolvu strateġiji differenti u sofistikati ta' inġinerija soċjali bħall-użu ta' USB key f'port ħieles (eż. tal-iċċarġjar tal-mowbajl). Billi jikklikkja fuq iperlinks f'posta elettronika suspettuża jew billi jiftaħ fajls mehmuża, l-utent jista' jkun li mingħajr ma jkun jaf ikun qed jinstalla software jew jipperikola konxjement s-servizzi u r-riżorsi tat-trasport.

Pereżempju, l-attakk ċibernetiku tar-ransomware WannaCry affettwa lil aktar minn 150 pajjiż u infetta lil aktar minn 230,000 sistema. Dan kien jinvolvi ransomware li normalment jinfirex permezz ta' ittri elettroniċi ta' phishing li jkun fihom fajls mehmuża jew iperlinks malizzjużi. Dan it-tip ta' attakk jisfrutta malizzjożament l-inġinerija soċjali sabiex iqarraq lill-utenti tas-sistema biex iwettqu l-installazzjoni (jew l-attivazzjoni) ta' malware speċifiku.

Theddida #2: Ċaħda tas-Servizz (Distribwita)

Iċ-Ċaħda tas-Servizzi Distribwita (DDoS) u ċ-Ċaħda tas-Servizzi (DoS) jaffettwaw id-disponibbiltà u l-aċċessibbiltà tad-*data*, tas-servizzi, tas-sistemi, u ta' riżorsi oħrajn. Dawn it-tipi ta' attakki jistgħu jvarjaw fid-durata u jistgħu jkunu mmirati lejn aktar minn servizz jew sistema waħda f'ħin partikolari. L-attakki tad-DDoS jużaw diversi sistemi (jew mezzi ta' attakk) sabiex is-servizzi jew is-sistemi jiġu mgħobbija żżejjed bit-talbiet. L-attakki li jkunu ta' suċċess jaffettwaw il-kapaċitajiet tas-servizz u tas-sistema biex jindirizzaw volum mhux mistenni ta' talbiet. Dan jirriżulta fiċ-ċaħda tal-aċċess għas-servizzi u r-riżorsi.

Innota li servizzi u sistemi affettwati li jappartjenu għall-organizzazzjonijiet tat-trasport jistgħu jiġu sfruttati sabiex jitwettqu attakki DDoS u d-DoS fuq sistemi speċifiċi f'operazzjonijiet jew f'organizzazzjonijiet oħra wkoll. Pereżempju, is-sistemi ta' informazzjoni korporattiva (bħall-kompjuters u l-apparat personali) jistgħu jkunu fil-mira sabiex ikun hemm aċċess għat-teknoloġiji tal-operat, li jistgħu jkunu konnessi mal-internet jew aċċess għan-networks sabiex tiġi ttrasferita *data* operazzjonali. Il-konnessjonijiet bejn sistemi u networks differenti (bħan-networks korporattivi, it-teknoloġiji tal-operat u l-aċċessi għall-manutenzjoni mill-bogħod) jistgħu jirrappreżentaw vulnerabbiltajiet li jistgħu jiġu sfruttati għat-twettiq ta' attakki DDoS jew DoS fuq servizzi u fuq sistemi kritiċi tat-trasport. Pereżempju, l-attakki DDoS u DoS jistgħu jisfruttaw protokolli komuni tan-network u tal-komunikazzjoni bħall-Web Services Dynamic Discovery (WS-Discovery), li jista' juża l-apparat tal-IoT biex jiskopri awtomatikament kull nodu fuq in-Networks taż-Żona Lokali (LANs). Jekk l-apparat tal-IoT jippreżenta vulnerabbiltajiet, dawk li jwettqu l-attakki jistgħu jisfruttaw dan l-apparat sabiex jiskopru apparat ieħor konness u jwettqu attakki DDoS jew DoS.



Theddida #3: Aċċess Mhux Awtorizzat u Serq

L-awturi tat-theddid jistgħu jkunu jridu jiksbu aċċess loġiku jew fiżiku mingħajr permess għal network, sistema, applikazzjoni, *data*, jew riżorsa oħra sabiex iwettqu attivitajiet malizzjużi, inkluż is-serq ta' *data* jew riżorsi sensittivi (inklużi riżorsi fiżiċi).
It-theddid ta' aċċess mhux awtorizzat u serq għandu fil-mira tiegħu assi kunfidenzjali u proprjetarji (inkluż identitajiet personali, kredenzjali ta' kontijiet privileġġati, sistemi, u tipi oħrajn ta' informazzjoni kunfidenzjali u proprjetarja). Dan it-theddid jista' jisfrutta l-vulnerabbiltajiet tas-sistemi kif ukoll ta' individwi mhux konxji li jkunu qed jiżvelaw *data* sensittiva bħall-kredenzjali (eż. login, password, eċċ.) jew *data* personali (eż. posta elettronika, numru ta' identifikazzjoni personali, eċċ.).

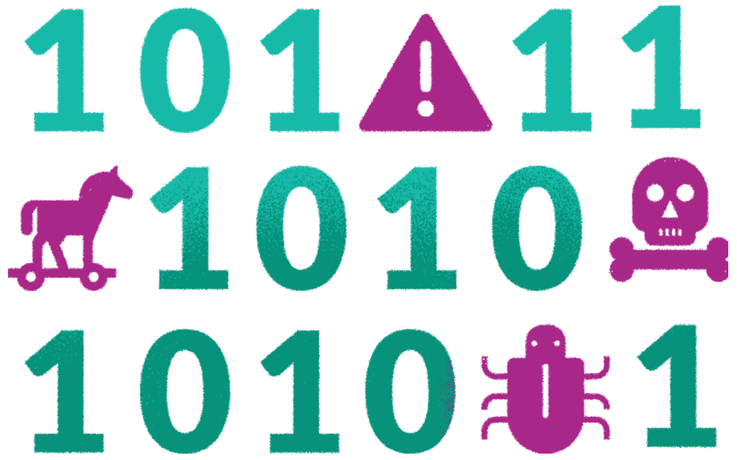
Fir-rigward ta' aċċess mhux awtorizzat, is-serq tal-identità huwa l-użu illeċitu ta' *data* personali jew ta' identifikaturi uniċi sabiex persuni jew servizzi u sistemi jiġu impersonati biex jinkiseb aċċess għal riżorsi privati jew proprjetarji (eż. inkluż riżorsi finanzjarji u fiżiċi). Tali theddid ċibernetiku jista' jkollu fil-mira tiegħu wkoll assi fiżiċi fil-modi kollha tat-trasport.

Theddida #4: Manipulazzjoni tas-Software

Il-konfigurazzjonijiet u l-manipulazzjonijiet ta' software u ta' sistemi jew komponenti relatati jista' jkollhom impatt dirett fuq il-pożizzjoni tas-sigurtà tas-servizzi u tas-sistemi tat-trasport.

L-attakki fuq iċ-ċibersigurtà li jisfruttaw il-manipulazzjonijiet tas-software jimmodifikaw is-settings tas-software jew jaffettwaw l-integrità tad-*data* sabiex tinbidel l-imġiba tas-sistemi u tas-servizzi. Dawk li jwettqu l-attakk jistgħu jimmanipulaw software (jew parti minnu) intenzjonalment sabiex jiksbu xi vantaġġi (eż. jiksbu aċċess mhux awtorizzat, jipprevjenu individwi jew sistemi leġittimi milli jaċċessaw ir-riżorsi meħtieġa, jiġbru informazzjoni sensittiva, ibiddlu l-imġiba funzjonali, eċċ.) fuq assi sensittivi.

Pereżempju, dawk li jwettqu l-attakk jistgħu jimmiraw lejn il-mezzi ta' komunikazzjoni tal-manifatturi sabiex itellgħu aġġornamenti tas-software malizzjużi fuq servizzi u sistemi (inkluż teknoloġiji operattivi) f'operazzjonijiet. Aġent ta' theddida juża kredenzjali ta' awtorizzazzjoni kompromessi biex jaċċessa interfaċċa sikura tan-network tal-manutenzjoni mill-bogħod sabiex jinstalla software manipulat u jikkompromett ulterjorment servizzi u sistemi aċċessibbli oħrajn. L-aġent tat-theddida jinstalla software manipulat li jikkompromett ulterjorment is-servizzi u s-sistemi, jew li jattakka servizzi jew sistemi konnessi oħrajn.



Il-Kummissjoni Ewropea

Profili ta’ Sensibilizzazzjoni dwar iċ-Ċibersigurtà

Il-Kummissjoni Ewropea

1

Profil I: Il-persunal kollu tat-trasport

L-ewwel mogħdija għandha fil-mira tagħha lill-persunal kollu tal-organizzazzjonijiet tat-trasport, minn persunal operazzjonali għal dak amministrattiv. Din il-mogħdija tipprovdi gwida lejn fehim u sensibilizzazzjoni akbar dwar l-aktar theddidiet ċibernetiċi komuni mmirati lejn is-servizzi tat-trasport. Tipprovdi wkoll għarfien dwar kif għandhom jiġu indirizzati t-theddidiet ċibernetiċi potenzjali, inkluż l-identifikazzjoni, ir-rapportar, u l-mitigazzjoni tagħhom permezz ta’ prattiki taċ-ċibersigurtà. Din il-mogħdija hija komuni għall-modi kollha tat-trasport.

2

Profil II: Dawk li jieħdu d-deċiżjonijiet fuq affarijiet relatati maċ-ċibersigurtà tat-trasport

It-tieni mogħdija hija mmirata lejn il-persunal li għandu r-responsabbiltà li jieħu deċiżjonijiet għas-sigurtà jew għaċ-ċibersigurtà fl-organizzazzjonijiet tat-trasport. Din il-mogħdija tipprovdi prattiki tajbin imfassla għall-modi differenti tat-trasport. Din tipprovdi prattiki tajbin għall-identifikazzjoni, għall-protezzjoni, għad-detezzjoni, u għar-rispons għat-theddid ċibernetiku emerġenti mmirat lejn l-organizzazzjonijiet tat-trasport.

Il-Kummissjoni Ewropea

Profil I: Il-persunal kollu tat-trasport

Din il-parti tpoġġi fil-mira tagħha lill-persunal kollu tal-organizzazzjonijiet tat-trasport, mill-persunal operazzjonali sal-persunal amministrattiv. Din tipprovdi gwida lejn fehim u sensibilizzazzjoni akbar dwar l-aktar theddidiet ċibernetiċi komuni mmirati lejn is-servizzi tat-trasport. Tipprovdi wkoll għarfien dwar kif għandhom jiġu indirizzati t-theddidiet ċibernetiċi potenzjali, inkluż l-identifikazzjoni, ir-rapportar, u l-mitigazzjoni tagħhom permezz ta’ prattiki taċ-ċibersigurtà.
Din il-parti tipprovdi prattiki rakkomandati u suġġerimenti utli, li huma rilevanti **fil-modi kollha tat-trasport**.

Prattiki tajbin kontra l-Malware

Inti tista' tgħin biex tipproteġi l-organizzazzjoni tiegħek billi ssegwi prattiki tajbin għall-**identifikazzjoni u għall-prevenzjoni tad-diffużjoni ta' malware**, bħal:

- ***Segwi politiki ta' sigurtà*** *bħall-iskennjar ta' mezzi tal-ħżin u fajls għall-virusijiet, filwaqt li tevita li tiftaħ jew tibgħat b'email tipi speċifiċi ta' fajls (eż. fajls eżegwibbli bħal .exe, .bat, .com, eċċ.), l-installazzjoni ta' software awtorizzat biss, l-iżgurar li s-software (inkluż l-antivirus) ikun aġġornat u jaħdem kif suppost, u politiki oħrajn*

- ***Agħmel backup tad-data tiegħek*** *regolarment f'apparat jew f'servizzi siguri (u awtorizzati) għall-ħżin tad-data, li jenħtieġ li jappoġġaw mekkaniżmi ta' kriptaġġ sabiex tiġi protetta d-data mistrieħa u li jenħtieġ li jkunu disponibbli għal proċeduri ta' rkupru tad-data*

- *Ipproteġi s-sistemi kollha b'**miżuri ta' sigurtà** xierqa (eż. password, kriptaġġ, eċċ.) inkluż apparat mobbli u apparat ta' punt ta' tmiem, u ftakar li għandek tillokkja (fiżikament u diġitalment) b'mod sikur is-sistemi kollha jekk tħallihom mingħajr superviżjoni*

- *Evita li tiftaħ fajls mehmuża u li tikklikkja fuq iperlinks li jkunu jinsabu f'emails mhux mistennija u "popups" tal-brawżer tal-web suspettużi b'test stramb jew mingħand persuni u dominji tal-internet li ma tafx*

- *Evita li ddaħħal fil-kompjuter tiegħek **apparat li jista' jitneħħa li ma jistax jiġi fdat jew li ma huwiex magħruf** bħal USB sticks, hard disks, u apparat ieħor għall-ħżin*

- *Evita li tiddiżattiva miżuri ta' sigurtà għal kontra l-malware (eż. software tal-antivirus, software għall-filtrazzjoni tal-kontenut, firewall, eċċ.)*

- ***Aġġorna s-software installat** regolarment għall-aħħar verżjonijiet disponibbli (li jistgħu joħorġu l-uffiċjali tas-sigurtà tal-informazzjoni jew amministraturi tas-sistema b'aġġornamenti regolari)*

- *Evita l-użu ta' kontijiet u kredenzjali privileġġati (eż. fil-livell ta' amministratur) għal attivitajiet u operazzjonijiet regolari*

- *Irrapporta lill-uffiċjali tas-sigurtà tal-informazzjoni jew lill-amministraturi tas-sistema kwalunkwe posta elettronika suspettuża jew imġiba tas-sistema mhux mistennija*

- *Oqgħod attent(a) għas-sigurtà tal-informazzjoni fix-xogħol ta' rutina ta' kuljum sabiex tagħraf tħassib dwar is-sigurtà tal-IT u tirrispondi kif xieraq.*

Prattiki tajbin kontra ċ-Ċaħda tas-Servizzi (Distribwita)

Tista’ tgħin fil-protezzjoni tal-organizzazzjoni tiegħek billi tidentifika **Ċaħda tas-Servizzi Distribwita (DDoS)** u attakkki ta’ **Ċaħda tas-Servizzi (DoS)**. Għandek tikkuntattja minnufih lit-timijiet tas-sigurtà u tal-IT tiegħek jekk tinduna jew tesperjenza kwalunkwe wieħed mill-indikaturi li ġejjin ta’ attakki potenzjali kontinwi ta’ DDoS u ta’ DoS għas-servizzi jew għas-sistemi tiegħek:

- *Żieda fit-talbiet li jikkonsmaw il-kapaċità tan-network (meqjusa bħala servizzi u tweġibiet bil-mod) li tirriżulta f’fallimenti tas-servizz jew tas-sistema minħabba tagħbija eċċessiva*

- *Żieda fid-domanda għall-użu tar-riżorsi tal-memorja mingħajr raġuni ovvja*

- ***Imġiba mhux mistennija ta’ servizzi u sistemi**, ikkraxxjar frekwenti u messaġġi ta’ errur strambi minħabba konsum malizzjuż ta’ riżorsi komputazzjonali jew konnessjonijiet tan-network*

- ***Prestazzjoni degradata** tal-apparati, ħin twil biex jitwettqu kompiti trivjali u attivitajiet notevoli (eż. fann storbjuż waqt li l-apparati jkunu qed jaħdmu bil-mod)*

- ***Konnessjonijiet jew telf ta’ konnessjonijiet mal-internet mhux mistennija** għas-servizzi u sistemi*

- *Bidliet sottili fl-imġiba tal-kontrolli jew tat-teknoloġiji tal-operat li jirriżultaw f’danni fiżiċi*

- *Ċaħdiet ta’ aċċessi għal kontijiet privileġġati jew amministrattivi sabiex il-proċeduri ta’ rispons għal aċċidenti jiġu mblokkati mill-irkupru.*

Prattiki tajbin kontra l-Aċċess mhux Awtorizzat u s-Serq

Sabiex jiġu evitati attakki li jinvolvu aċċess mhux awtorizzat u serq, huwa meħtieġ li jiġu segwiti prinċipji bħal *"ħtieġa ta' tagħrif"* u *"sigurtà u privatezza prestabbilita"*, li jenfasizzaw li l-assi sensittivi u kunfidenzjali (inkluż *data* personali u sensittiva, sistemi tat-trasport, eċċ.) għandhom ikunu aċċessibbli biss għal min ikollu d-dritt li jaċċessahom sabiex iwettaq id-dmirijiet tiegħu. Tista' tgħin fil-protezzjoni tal-organizzazzjoni tiegħek billi ssegwi prattiki tajbin għall-identifikazzjoni u għall-prevenzjoni ta' aċċess mhux awtorizzat u serq, bħal:

- *Segwi l-politiki organizzazzjonali tas-sigurtà*
- *Evita li taqsam u tippubblika kredenzjali u data personali online, inkluż stampi li jista' jkun fihom tali informazzjoni*
- *Evita l-użu jew it-trażmissjoni ta' kredenzjali u ta' data personali (u data sensittiva oħra) fuq networks, apparat jew servizzi tal-web mhux fdati u mhux siguri (eż. siti web li jużaw protokolli jew indirizzi mhux siguri http:// u mhux siguri https://)*
- ***Qatt tiżvela l-kredenzjali tiegħek** (eż. login u password) anke permezz tal-posta elettronika jew bit-telefown*
- *Ipproteġi d-data sensittiva ittajpjata fuq it-tastiera jew murija fuq l-iskrins (inkluż fuq apparat mobbli) minn individwi mhux awtorizzati, installa skrins tal-privatezza, u evita li taħdem minn postijiet pubbliċi b'apparat privat, u evita li tħalli kwalunkwe apparat mhux illokkjat u mingħajr superviżjoni*
- ***Uża passwords kumplessi** (eż. password twila biżżejjed li tgħaqqad karattri alfanumeriċi u speċjali) li jikkonformaw mal-politiki ta' sigurtà organizzazzjonali rilevanti sabiex jiġi evitat aċċess mhux awtorizzat*
- ***Biddel il-passwords prestabbiliti** tas-sistemi u tal-apparati konnessi (eż. stampaturi, routers, kameras, serraturi intelliġenti, eċċ.)*
- *Evita li tuża l-istess kredenzjali (eż. login u password) għal numru ta' servizzi u sistemi, u evita l-użu tal-istess kredenzjali għal servizzi u sistemi li jeħtieġu kontijiet privileġġati*
- *Ibgħat passwords u "keys" għal fajls protetti ttrasferiti (eż. arkivji ZIP) biss permezz ta' mezz 'il barra mill-kanal fiss ta' komunikazzjon (eż. SMS permezz tal-GSM u telefonata) u qatt permezz tal-posta elettronika*
- ***Attiva l-Awtentikazzjoni b'Żewġ Fatturi (2FA)** jew l-Awtentikazzjoni b'Multi Fattur (MFA), jekk possibbli.*

Prattiki tajbin kontra l-Manipulazzjoni tas-Software

Tista’ tgħin fil-protezzjoni tal-organizzazzjoni tiegħek billi ssegwi prattiki tajbin għall-identifikazzjoni u l-prevenzjoni tal-manipulazzjoni tas-software, bħal:

- *Evita li tinstalla software mhux affidabbli fuq sistemi u apparati (inkluż kompjuters personali, servers, periferali, apparat tan-network, smartphones, eċċ.)*
- *Dejjem installa software u aġġornamenti minn sorsi u minn siti web uffiċjali (eż. produtturi, repożitorji korporattivi, eċċ.)*
- *Evita li tniżżel software u applikazzjonijiet (u kwalunkwe fajl) minn sorsi illegali*
- *Neħħi software li ma huwiex meħtieġ jew li ma ntużax reċentement, u ddiżattiva konnessjonijiet bla bżonn (eż. protokolli u servizzi tan-network) inkluż l-aċċess għal servizzi remoti (eż. servizzi ta’ ħżin fuq il-cloud)*
- *Skennja kwalunkwe software jew apparat tal-ħżin b’antivirus affidabbli u aġġornat*
- *Niżżel software industrijali sikur (eż. aġġornamenti, patches, prodotti ġodda, eċċ.) minn forniturifdati bl-użu tal-prinċipju “white station”*
- *Aġġorna s-software installat kollu f’konformità mal-politiki u l-prattiki organizzazzjonali.*

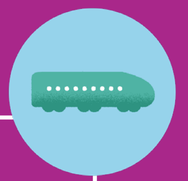
Il-Kummissjoni Ewropea

Profil II: Dawk li jieħdu d-deċiżjonijiet fuq affarijiet relatati maċ-ċibersigurtà tat-trasport

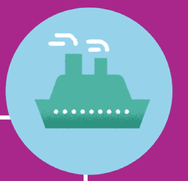
Din il-parti għandha fil-mira tagħha lill-persunal li għandu r-responsabbiltajiet ta’ teħid ta’ deċiżjonijiet għas-sigurtà jew għaċ-ċibersigurtà fl-organizzazzjonijiet tat-trasport. Din il-mogħdija tenfasizza prattiki tajbin imfassla għall-modi differenti tat-trasport. Partikolarment, din tipprovdi prattiki tajbin għall-identifikazzjoni, għall-protezzjoni, għad-detezzjoni u għar-risposta għat-theddid ċibernetiku emerġenti.

Il-Kummissjoni Ewropea

Prattiki tajbin ta’ sigurtà ċibernetika mfassla għat-trasport bl-Ajru



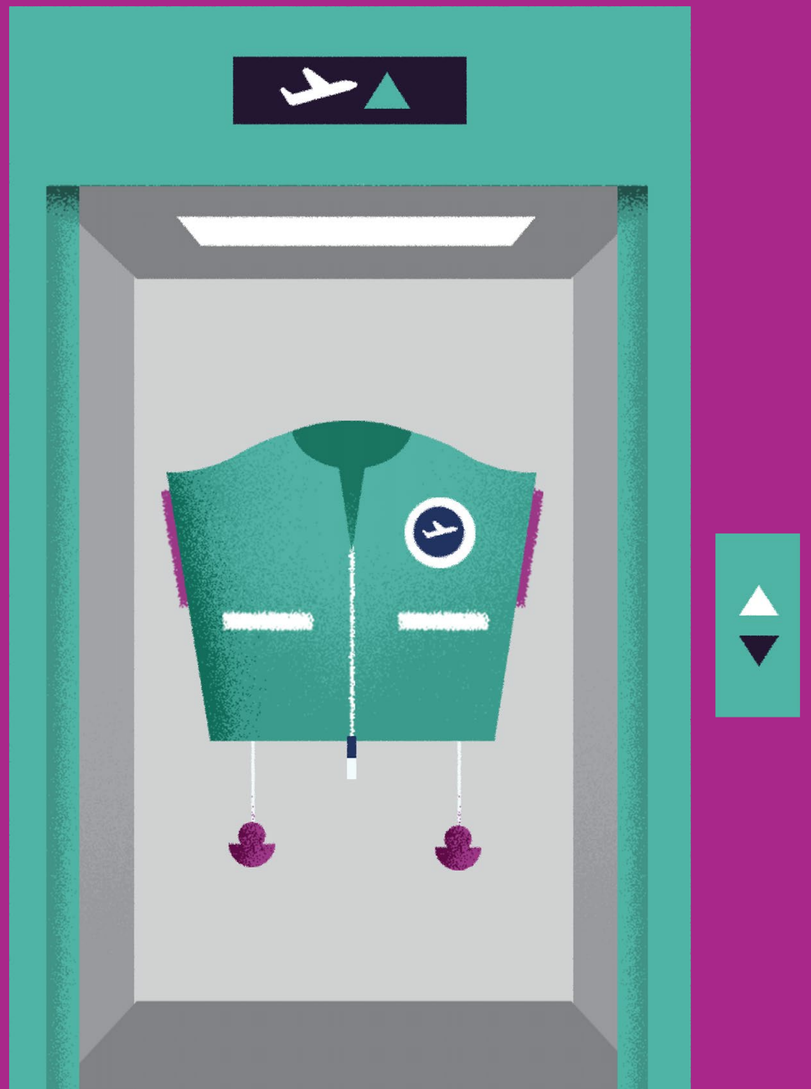
Prattiki tajbin ta’ ċibersigurtà mfassla għat-trasport fuq l-Art



Prattiki tajbin ta’ sigurtà ċibernetika relatati mat-trasport Marittimu

Il-Kummissjoni Ewropea

Prattiki Tajbin u Miżuri ta’ Sigurtà mfassla għat-Trasport bl-Ajru



Governanza

L-organizzazzjonijiet tal-avjazzjoni jeħtieġu fehim ċar dwar it-theddid emerġenti sabiex jiddefinixxu l-politiki u l-proċessi ta’ ġestjoni biex jirregolaw l-approċċi tagħhom sabiex itejbu ċ-ċibersigurtà tas-servizzi u tas-sistemi fl-operazzjonijiet, inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT).

Il-prattiki tajbin għall-organizzazzjonijiet ta’ kwalunkwe daqs jinvolvu:

- L-iżgurar li l-livelli ta’ maniġment superjuri jirrapportaw tħassib dwar iċ-ċibersigurtà lill-eżekuttivi u lill-bordijiet, li jistgħu jieħdu deċiżjonijiet infurmati dwar l-allokazzjonijiet tar-riżorsi

- Il-ħatra ta’ rwol superjuri, responsabbli għaċ-ċibersigurtà kif ukoll għas-sigurtà fiżika, b’responsabbiltajiet amministrattivi kumplessivi għas-sigurtà tat-Teknoloġija tal-Informazzjoni (IT) u tat-Teknoloġija Operazzjonali (OT), iżda mingħajr involviment fl-operazzjonijiet sabiex jiġu evitati kunflitti ta’ interess

- Id-definizzjoni ċara tar-rwoli, tar-responsabbiltajiet, tal-kompetenzi, u tal-approvazzjonijiet relatati maċ-ċibersigurtà u l-komunikazzjoni u l-qbil dwarhom mal-persunal rilevanti, partikolarment, għall-membri tal-Iskwadra ta’ Rispons f’Emerġenza relatata mal-Kompjuters (CERTs)

- L-iżgurar tal-governanza taċ-ċibersigurtà tul il-katina kollha tas-servizzi tal-provvista tas-sigurtà, inkluż interfaċċi kemm fiżiċi kif ukoll diġitali, mill-manifatturi tat-teknoloġija u mill-installaturi sal-fornituri tas-sigurtà

- Il-qbil fuq l-attivitajiet u l-kontrolli, inkluż ir-responsabbiltajiet kondiviżi, għall-ġestjoni tar-riskji taċ-ċibersigurtà, u l-iżgurar li dawn ir-responsabbiltajiet jiġu sostnuti matul il-ħajja kollha (eż. permezz ta’ ftehimiet ta’ servizz) tas-soluzzjonijiet u s-servizzi ta’ sigurtà

- Id-definizzjoni ta’ mekkaniżmi ta’ governanza (eż. politiki) sabiex ikun hemm konformità mal-obbligi meħuda mir-regolamenti u mid-direttivi rilevanti bħal, pereżempju, ir-Regolament 2018/1139 dwar regoli komuni fil-qasam tal-avjazzjoni ċivili u r-Regolament ta’ Implimentazzjoni tal-Kummissjoni 2017/373 li jistabbilixxi r-rekwiżiti komuni għall-fornituri ta’ servizzi fil-ġestjoni tat-traffiku tal-ajru/tas-servizzi tan-navigazzjoni bl-ajru u funzjonijiet oħrajn tan-network tal-ġestjoni tat-traffiku tal-ajru u s-sorveljanza tagħhom kif ukoll id-Direttiva NIS (id-Direttiva tal-UE 2016/1148 dwar miżuri għal livell għoli komuni ta’ sigurtà tan-networks u tas-sistemi tal-informazzjoni madwar l-Unjoni).

Eżempji ta’ servizzi u sistemi fit-trasport bl-ajru: Eżempji ta’ IT huma dawk aċċessibbli għall-impjegati (eż. kompjuters personali, mowbajls, periferali tal-uffiċċji, eċċ.) kif ukoll għall-passiġġieri (eż. routers pubbliċi tal-Wi-Fi u konnessjonijiet, eċċ.). Eżempji ta’ OT huma s-sistemi ta’ Kontrolli ta’ Sorveljanza u tal-Akkwist tad-*Data* (SCADA), is-sistemi ta’ tisħin, ventilazzjoni u arja kondizzjonata (HVAC), il-punti ta’ kontroll tas-sigurtà għall-bagalji tal-kabina, is-sistemi tal-immaniġġar tal-bagalji (BHS), il-kontroll tal-aċċess, il-monitoraġġ, is-sorveljanza, ir-rispons f’każ ta’ allarm, it-teknoloġija tal-iskrinjar, is-sistemi ta’ kontroll tad-dawl fl-ajrudrom, is-sistemi u s-sensuri tar-radar, is-Sistemi ta’ Pożizzjonament Globali (GPS), is-sistemi tal-Ġestjoni tat-Traffiku tal-Ajru (ATM), is-sistemi ta’ Komunikazzjoni, Navigazzjoni u Sorveljanza (CNS), is-Sistemi ta’ Informazzjoni Ajrunawtika, is-Sistemi Meteoroloġiċi, is-Sistemi taċ-Ċentru tal-Operazzjonijiet tas-Sigurtà, is-sistemi ta’ abbord il-linja tal-ajru, u oħrajn.

Identifikazzjoni tat-Theddid Ċibernetiku

Ġestjoni tar-Riskju: L-organizzazzjonijiet tal-avjazzjoni jridu jieħdu passi xierqa biex jidentifikaw, jivvalutaw u jifhmu r-riskji taċ-ċibersigurtà għan-network u għas-sistemi ta' informazzjoni li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali.

Dan jeħtieġ approċċ organizzazzjonali ġenerali tal-ġestjoni tar-riskju, li jinvolvi:

- *L-iżgurar ta' ħarsa ġenerali ċara lejn id-diversi sistemi tal-hardware u tas-software użati għall-kunsinna ta' servizzi differenti. Fil-kuntest tal-avjazzjoni, tali sistemi jinvolvu t-Teknoloġija tal-Informazzjoni (IT) kif ukoll it-Teknoloġiji Operazzjonali (OT)*

- *It-twettiq **ta' valutazzjonijiet tar-riskju taċ-ċibersigurtà**, li jqisu t-theddid emerġenti, il-vulnerabbiltajiet magħrufa, u d-data operazzjonali fir-rigward tas-sistemi fil-kamp ta' applikazzjoni. Organizzazzjonijiet bħall-Iskwadra ta' Rispons f'Emerġenza relatata mal-Kompjuters tal-Ġestjoni tat-Traffiku tal-Ajru Ewropew (EATM-CERT) u ċ-Ċentru tal-Kondiviżjoni u l-Analiżi tal-Informazzjoni dwar l-Avjazzjoni (A-ISAC) jistgħu jipprovdu għarfien dwar it-theddid li għandu fil-mira t-trasport bl-ajru*

- *L-iżgurar li l-valutazzjonijiet tar-riskju jkopru wkoll ir-riskji relatati mal-attivitajiet ta' kuljum tal-persunal (eż. l-użu tal-midja soċjali, l-użu tal-apparat personali, l-ipproċessar tad-data, il-kondiviżjoni tal-informazzjoni, eċċ.)*

- *L-identifikazzjoni u l-implimentazzjoni ta' miżuri u pjanijiet għat-trattament tar-riskju biex jittaffew ir-riskji taċ-ċibersigurtà*

- *L-implimentazzjoni ta' **Sistema għall-Ġestjoni tas-Sigurtà tal-Informazzjoni** (ISMS) komprensiva u ta' **Sistema għall-Ġestjoni tal-Informazzjoni dwar il-Privatezza** (PIMS) allinjata ma' sistemi ta' ġestjoni oħrajn. Sistemi ta' ġestjoni bħal dawn (jiġifieri l-ISMS u l-PIMS) jinvolvu l-implimentazzjoni ta' kontrolli tas-sigurtà (kif ukoll tal-protezzjoni tad-data u tal-privatezza) sabiex jiġi mmitigat u evitat theddid emerġenti li jaffettwa s-sigurtà tas-servizzi u tas-sistemi tal-avjazzjoni (inkluża d-data tagħhom)*

- *Filwaqt li titqies kwalunkwe restrizzjoni kkonċernata **mal-ġestjoni tal-assi u mal-ippjanar tar-riżorsi** (jiġifieri, restrizzjonijiet li jistgħu jaffettwaw il-konsenja, il-manutenzjoni u l-appoġġ ta' sistemi kritiċi għall-operazzjonijiet ta' funzjonijiet essenzjali fit-trasport bl-ajru).*

Eżempji ta’ oqfsa ta’ ġestjoni tar-riskju: Oqfsa differenti (eż. standards fil-familja tal-ISO/IEC 27000, il-qafas taċ-ċibersigurtà NIST, il-qafas MITRE ATT&CK, BSI-IT-Grundschutz, eċċ.) jistgħu jinfurmaw u jsostnu approċċ imfassal apposta għall-ġestjoni tar-riskju għat-trasport bl-ajru. Organizzazzjonijiet internazzjonali bħall-IATA u l-ICAO jipprovdu gwida għall-valutazzjonijiet tar-riskju taċ-ċibersigurtà. L-ENISA, l-EASA, il-EUROCONTROL, u l-Kunsill Internazzjonali tal-Ajruporti (ACI) fost l-oħrajn jenfasizzaw prattiki tajbin għas-sigurtà tal-ajruporti, tal-forniturі tal-ġestjoni tat-traffiku tal-ajru, u ta’ organizzazzjonijiet oħrajn tal-avjazzjoni. L-Impriża Konġunta SESAR tikkoordina u tikkonċentra l-attivitajiet kollha ta’ riċerka u żvilupp (R&D) tal-UE fil-Ġestjoni tat-Traffiku tal-Ajru li jkopru wkoll aspetti tas-sikurezza kif ukoll is-sigurtà.

Protezzjoni kontra Theddid Ċibernetiku

L-organizzazzjonijiet fit-trasport bl-ajru jenħtieġ li jimplimentaw miżuri ta' sigurtà adegwati u proporzjonati sabiex jipproteġu n-networks u s-sistemi tal-informazzjoni tagħhom – inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT) minn attakki ċibernetiċi. Miżuri ta' Sigurtà jinkludu:

- ***Politiki u Proċessi tas-Sigurtà:*** *id-definizzjoni, l-implimentazzjoni, il-komunikazzjoni u l-infurzar ta' politiki u proċessi xierqa, li jiddefinixxu approċċ ġenerali għall-iżgurar tas-sistemi u tad-data li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fl-avjazzjoni. Tali politiki u proċeduri ta' sigurtà (eż. politiki dwar il-passwords u dwar il-ħżin) għandhom ikopru wkoll il-ġestjoni tal-patches u tal-vulnerabbiltà tal-hardware u tas-sistemi tas-software (inkluż IT u OT), il-Ġestjoni tal-Inċidenti, il-protezzjoni tas-Sistema u tan-Network.*

- ***Ġestjoni tal-Identitajiet u tal-Aċċess:*** *il-fehim, id-dokumentazzjoni u l-ġestjoni tal-aċċess għan-networks u għas-sistemi tal-informazzjoni (inkluż l-IT u l-OT) li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fit-trasport bl-ajru. L-utenti (jew il-funzjonijiet awtomatizzati) li jistgħu jaċċessaw id-data jew is-sistemi jiġu vverifikati, awtentikati u awtorizzati kif xieraq. Dan għandu jqis ukoll ir-rwoli u r-responsabbiltajiet differenti għal kontijiet regolari u privileġġati.*

- ***Sigurtà tad-Data u tas-Sistema:*** *il-protezzjoni tad-data (maħżuna u trażmessa elettronikament), tan-networks kritiċi u tas-sistemi tal-informazzjoni (inklużi l-IT u l-OT) minn attakki ċibernetiċi. Filwaqt li jitqies approċċ xprunat mir-riskju, l-organizzazzjonijiet jenħtieġ li jimplimentaw miżuri ta' sigurtà biex jillimitaw effettivament l-opportunitajiet għal dawk li jwettqu l-attakki biex jikkompromettu d-data, in-networks u s-sistemi. Dawn il-miżuri ta' sigurtà għandhom jinkludu wkoll l-adozzjoni ta' protokolli ta' kriptaġġ u ta' komunikazzjoni sigura sabiex tiġi protetta d-data mistrieħa u fi tranżitu mit-theddid ċibernetiku li jirriżulta f'attakki kkawżati mill-bniedem. Barra minn hekk, huwa meħtieġ li tali miżuri jiġu kkombinati ma' miżuri ta' sigurtà fiżika sabiex jiġi protett l-aċċess għas-sistemi (eż. is-sistemi għandhom ikunu jinsabu fi kmamar konfinati b'aċċess ristrett).*

- ***Reżiljenza tan-Networks u tas-Sistemi:*** *il-bini tar-reżiljenza tan-networks u tas-sistemi (inklużi tal-IT u tal-OT) billi jitfasslu u jiġu implimentati (u l-proċeduri operazzjonali tagħhom) sabiex jirreżistu u jtaffu l-impatt tal-attakki ċibernetiċi. Eżempji ta' soluzzjonijiet ta' disinn u implimentazzjoni li jsaħħu r-reżiljenza huma: funzjonijiet kritiċi vverifikati formalment, ir-ridondanza tas-sistemi u n-networks, is-segregazzjoni tan-networks (partikolarment, is-segregazzjoni tal-IT u tal-OT), il-miżuri ta' sigurtà f'diversi livelli, u ħafna oħrajn. Innota li minn perspettiva tas-sigurtà tal-informazzjoni, l-oqsma tas-sigurtà li jimplimentaw is-segregazzjonijiet tan-networks u tas-sistema jistgħu jipprovdu soluzzjonijiet ta' sigurtà xierqa. Madankollu, il-ħtiġijiet operazzjonali (eż. l-attivitajiet ta' manutenzjoni, it-trasferimenti tad-data, eċċ.) tas-sistemi jistgħu jeħtieġu l-evitar jew il-konnessjoni ta' oqsma differenti ta' sigurtà (eż. sistemi u networks segregati), inkluż il-konnessjoni tal-IT u tal-OT.*

Identifikazzjoni tat-Theddid Ċibernetiku

Jenħtieġ li l-organizzazzjonijiet jiżguraw li l-miżuri ta' sigurtà jibqgħu effettivi, u jidentifikaw kwalunkwe avveniment taċ-ċibersigurtà li jaffettwa jew li għandu l-potenzjal li jaffettwa l-kontrolli tas-sigurtà kif ukoll is-servizzi u s-sistemi essenzjali. Sabiex jiġu identifikati t-theddidiet ċibernetiċi, il-miżuri rilevanti ta' sigurtà huma:

- ***Monitoraġġ tas-Sigurtà:*** *il-monitoraġġ tal-istatus tas-sigurtà tan-networks u tas-sistemi tal-informazzjoni – inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT) – li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fis-servizzi tat-trasport bl-ajru. Sabiex jiġi appoġġat il-monitoraġġ tas-sigurtà, id-data li titqies hija, pereżempju:*

  - *reġistri tas-sigurtà*
  - *reġistri tad-detezzjoni tal-virusijiet*
  - *reġistri tad-detezzjoni tal-intrużjoni*
  - *reġistri tal-identifikazzjoni, tal-awtentikazzjoni u tal-awtorizzazzjoni*
  - *reġistri tas-sistemi u tas-servizzi*
  - *reġistri tat-traffiku tan-network*
  - *reġistri tal-ipproċessar tad-data*

- ***Sejbien ta' Eventi ta' Sigurtà:*** *l-identifikazzjoni ta' attivitajiet malizzjużi (jiġifieri avvenimenti ta' sigurtà) li jaffettwaw jew li għandhom il-potenzjal li jaffettwaw is-sigurtà tan-networks u tas-sistemi tal-informazzjoni (inkluż l-IT u l-OT) li jappoġġaw operazzjonijiet ta' funzjonijiet essenzjali fis-servizzi tat-trasport bl-ajru.*

Dawn il-miżuri jistgħu jeħtieġu l-adozzjoni ta' teknoloġiji speċifiċi (eż. il-Ġestjoni tal-Informazzjoni u tal-Eventi ta' Sigurtà, Sistema ta' Detezzjoni tal-Intrużjoni, Sistema ta' Prevenzjoni tal-Intrużjoni, eċċ.) u l-istabbiliment ta' SOC (Ċentru tal-Operazzjonijiet ta' Sigurtà) jew ekwivalenti. Jiġifieri, l-iżvilupp ta' mezzi għall-identifikazzjoni, analiżi, rispons u rkupru minn attakki ċibernetiċi lokalment.

L-Iskwadra ta' Rispons għal Inċidenti relatati mas-Sigurtà tal-Kompjuters (CSIRTs), is-CERTs settorjali (eż. it-Tim Ewropew ta' Rispons għal Emerġenza tas-Sistema Ewropea għall-Ġestjoni tat-Traffiku tal-Ajru EATM-CERT) tal-EUROCONTROL), is-CERTs kummerċjali tal-linji tal-ajru, u ċ-Ċentru tal-Kondiviżjoni u tal-Analiżi tal-Informazzjoni dwar l-Avjazzjoni (A-ISAC) jistgħu jipprovdu Intelliġenza kontra l-Attakki Ċibernetiċi (CTI) li tinforma dwar il-monitoraġġ u l-iskoperta tas-sigurtà.

Pjanar tar-rispons u tal-irkupru

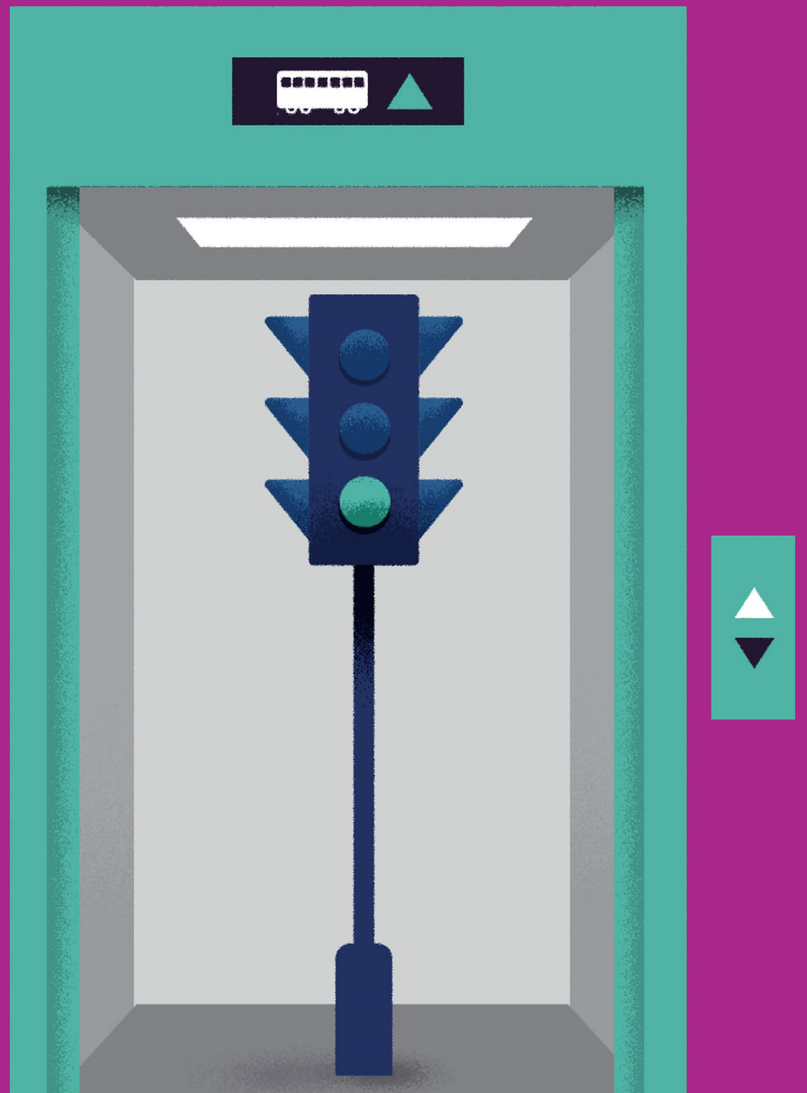
L-organizzazzjonijiet għandhom jiddefinixxu, jimplimentaw u jittestjaw il-proċeduri ta' ġestjoni tal-inċidenti, li jkollhom l-intenzjoni li jiżguraw il-kontinwità tan-negozju tas-servizzi u tas-sistemi fl-eventwalità ta' inċidenti taċ-ċibersigurtà. Il-miżuri ta' mitigazzjoni għandhom l-għan li jrażżnu jew li jillimitaw l-impatt tal-inċidenti taċ-ċibersigurtà.

L-ippjanar tar-rispons u tal-irkupru għandu jqis il-miżuri ta' sigurtà, filwaqt li jtaffi l-impatt ta' attakki speċifiċi taċ-ċibersigurtà, bħal:

- *Il-koordinazzjoni u l-kollaborazzjoni mas-CSIRTs Nazzjonali, mas-CERTs (pubbliċi u kummerċjali) u mal-ISACs matul inċidenti taċ-ċibersigurtà, il-koordinazzjoni tal-inċidenti, u l-kriżijiet fil-livell Pan-Ewropew*
- *Il-kondiviżjoni ta' informazzjoni ma' organizzazzjonijiet oħrajn, inklużi fornituri fil-katina tal-provvista tas-servizzi tal-avjazzjoni*
- *It-twettiq ta' **eżerċizzji perjodiċi ta' attakk ċibernetiku** (koordinazzjoni "table top" kif ukoll teknika) għall-valutazzjoni tal-miżuri u tal-proċeduri ta' sigurtà kif ukoll ir-reżiljenza tal-organizzazzjoni biex jiġu ttrattati l-inċidenti ċibernetiċi*
- *Aċċess għal postijiet ta' ħżin arkivjati jew ta' riżerva f'każ ta' kompromess fl-integrità u d-disponibbiltà tal-ħażniet tad-data*
- ***Il-playbooks tas-sigurtà** għandhom proċeduri dettaljati għall-ġestjoni tal-inċidenti ċibernetiċi u biex is-servizzi u s-sistemi jinġiebu lura f'kundizzjonijiet operazzjonali normali*
- *Ridirezzjonijiet tat-traffiku tan-network għal servizzi żejda matul l-attakki taċ-ċaħda tas-servizzi*
- *Proċeduri manwali għat-tħaddim b'servizzi u b'sistemi f'modalitajiet operazzjonali degradati*
- *Id-definizzjoni ta' proċeduri sabiex jiġi indirizzat il-ksur tad-data, inklużi proċeduri biex jiġi ttrattat il-ksur tad-data li jaffettwa d-data personali f'konformità mar-Regolament Ġenerali dwar il-Protezzjoni tad-Data (GDPR) u kwalunkwe regolament jew Direttiva settorjali rilevanti oħra*
- *L-akkwist ta' **assigurazzjoni ċibernetika** sabiex ir-riskju assoċjat ma' inċidenti ċibernetiċi severi jibda parzjalment*
- *Id-dħul f'kuntratt għal rispons għall-inċidenti ma' ditta/i speċjalizzata/i waħda jew aktar għal kapaċità u għarfien espert addizzjonali*
- *Id-definizzjoni ta' proċeduri **għall-kondiviżjoni tal-informazzjoni dwar inċidenti** taċ-ċibersigurtà mal-partijiet ikkonċernati rilevanti, inkluż proċeduri għan-notifika ta' inċidenti f'konformità mad-Direttiva NIS (id-Direttiva tal-UE 2016/1148 dwar miżuri għal livell għoli komuni ta' sigurtà tan-networks u tas-sistemi tal-informazzjoni madwar l-Unjoni).*

Il-Kummissjoni Ewropea

Prattiki Tajbin u Miżuri ta’ Sigurtà mfassla għat-Trasport fuq l-Art



Governanza

L-organizzazzjonijiet tat-trasport fuq l-art (bil-ferrovija u bit-triq) jeħtieġu fehim ċar dwar it-theddid emerġenti sabiex jiddefinixxu l-politiki u l-proċessi ta’ ġestjoni biex jirregolaw l-approċċi tagħhom sabiex itejbu ċ-ċibersigurtà tas-servizzi u tas-sistemi fl-operazzjonijiet, inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT).

Il-prattiki tajbin għall-organizzazzjonijiet ta’ kwalunkwe daqs jinvolvu:

- *L-iżgurar li l-livelli ta’ maniġment superjuri jirrapportaw tħassib dwar iċ-ċibersigurtà lill-eżekuttivi u lill-bordijiet, li jistgħu jieħdu deċiżjonijiet infurmati dwar l-allokazzjonijiet tar-riżorsi*

- *Il-ħatra ta’ rwol superjuri, responsabbli għaċ-ċibersigurtà kif ukoll għas-sigurtà fiżika, b’responsabbiltajiet amministrattivi kumplessivi għas-sigurtà tat-Teknoloġija tal-Informazzjoni (IT) u tat-Teknoloġija Operazzjonali (OT), iżda mingħajr involviment fl-operazzjonijiet sabiex jiġu evitati kunflitti ta’ interess*

- *Id-definizzjoni ċara tar-rwoli, tar-responsabbiltajiet, tal-kompetenzi, u tal-approvazzjonijiet relatati maċ-ċibersigurtà u l-komunikazzjoni u l-qbil fuqhom mal-persunal rilevanti. Dan huwa meħtieġ, partikolarment, għall-membri tal-Iskwadri ta’ Rispons għal Inċidenti relatati mas-Sigurtà tal-Kompjuters (CERTs)*

- *L-iżgurar tal-governanza taċ-ċibersigurtà tul il-katina kollha tas-servizzi tal-provvista tas-sigurtà, inkluż interfaċċi kemm fiżiċi kif ukoll diġitali, mill-manifatturi tat-teknoloġija u mill-installaturi sal-fornituri tas-sigurtà*

- *Il-qbil fuq l-attivitajiet u l-kontrolli, inkluż ir-responsabbiltajiet kondiviżi, għall-ġestjoni tar-riskji taċ-ċibersigurtà, u l-iżgurar li dawn ir-responsabbiltajiet jiġu sostnuti matul il-ħajja kollha (eż. permezz ta’ ftehimiet ta’ servizz) tas-soluzzjonijiet u s-servizzi ta’ sigurtà*

- *Id-definizzjoni ta’ mekkaniżmi ta’ governanza (eż. politiki) sabiex ikun hemm konformità mal-obbligi meħuda mir-regolamenti u d-direttivi rilevanti. Dan jinkludi sett wiesgħa ta’ politiki li jkopru l-modi speċifiċi tat-trasport kif ukoll tipi differenti ta’ partijiet ikkonċernati (eż. inkluż il-manifatturi tal-vetturi u tas-sistemi ferrovjarji) kif ukoll id-Direttiva tal-NIS (id-Direttiva tal-UE 2016/1148 dwar miżuri għal livell għoli komuni ta’ sigurtà tan-networks u tas-sistemi tal-informazzjoni).*

Eżempji ta’ servizzi u sistemi tat-trasport fuq l-art:
Eżempji ta’ IT huma dawk aċċessibbli għall-impjegati (eż. kompjuters personali, mowbajls, periferali tal-uffiċċji, eċċ.) kif ukoll għall-passiġġieri (eż. routers pubbliċi tal-Wi-Fi u konnessjonijiet, eċċ.). Eżempji ta’ OT huma s-sistemi ta’ Kontrolli Superviżorji u ta’ Ksib ta’ *Data* (SCADA), is-sistemi tat-tisħin, tal-ventilazzjoni, u tal-arja kundizzjonata (HVAC), is-Sistemi ta’ Pożizzjonament Globali (GPS), il-kontroll tal-aċċess, il-monitoraġġ, is-sorveljanza, ir-rispons għall-allarm u t-teknoloġija tal-iskrinjar. Is-sistemi speċifiċi għat-trasport bil-ferrovija huma, pereżempju: operazzjonali (sistema ta’ kontroll-kmand) inklużi sistemi ta’ sinjalar, is-Sistema Ewropea tal-Ġestjoni tat-Traffiku Ferrovjarju (ERTMS), sistemi fuq il-ferrovija, sistemi ta’ manutenzjoni, u oħrajn.

Identifikazzjoni tat-Theddid Ċibernetiku

Ġestjoni tar-Riskju: L-organizzazzjonijiet tat-trasport fuq l-art jeħtieġ li jieħdu passi xierqa biex jidentifikaw, jivvalutaw u jifhmu r-riskji taċ-ċibersigurtà għan-network u għas-sistemi ta' informazzjoni li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali. Dan jeħtieġ approċċ organizzazzjonali ġenerali tal-ġestjoni tar-riskju, li jinvolvi:

- *L-iżgurar ta' ħarsa ġenerali ċara lejn id-diversi sistemi tal-hardware u tas-software użati għall-kunsinna ta' servizzi differenti. Fil-kuntest tat-trasport fuq l-art, tali sistemi jinvolvu t-Teknoloġija tal-Informazzjoni (IT) kif ukoll it-Teknoloġiji Operazzjonali (OT)*

- *It-twettiq ta' **valutazzjonijiet tar-riskju taċ-ċibersigurtà**, li jenħtieġ li jqisu t-theddid emerġenti, il-vulnerabbiltajiet magħrufa, u d-data operazzjonali fir-rigward tas-sistemi fil-kamp ta' applikazzjoni. Eżempji ta' sistemi fil-modalitajiet tat-trasport fuq l-art huma: sistemi ta' pagament, sistemi ta' network u ta' komunikazzjoni (eż. internet, komunikazzjoni bir-radju, WiFi, eċċ.), tagħmir abbord, ċentri ta' kontroll operazzjonali, sistemi ta' ġestjoni tal-identità, sistemi ta' sikurezza, u oħrajn. Għall-infrastrutturi ferrovjarji, eżempji ta' sistemi huma: rolling stock, is-subsistemi tal-operat u tal-ġestjoni tat-traffiku, il-kontroll-kmand, u s-subsistemi tas-sinjalar abbord u mal-ġenb tal-linji tal-ferroviji, u oħrajn*

- *L-iżgurar li l-valutazzjonijiet tar-riskju jkopru wkoll ir-riskji relatati mal-attivitajiet ta' kuljum tal-persunal (eż. l-użu tal-midja soċjali, l-użu tal-apparat personali, l-ipproċessar tad-data, il-kondiviżjoni tal-informazzjoni, eċċ.)*

- *L-identifikazzjoni u l-implimentazzjoni ta' miżuri u pjanijiet għall-mitigazzjoni tar-riskji taċ-ċibersigurtà. Bħall-implimentazzjoni ta' **Sistema għall-Ġestjoni tas-Sigurtà tal-Informazzjoni** (ISMS) komprensiva u **Sistema għall-Ġestjoni tal-Informazzjoni dwar il-Privatezza** (PIMS), allinjati ma' sistemi oħra ta' ġestjoni. Sistemi ta' ġestjoni bħal dawn (jiġifieri l-ISMS u l-PIMS) jinvolvu l-implimentazzjoni ta' kontrolli tas-sigurtà (kif ukoll tal-protezzjoni tad-data u tal-privatezza) sabiex jiġi mmitigat u evitat theddid emerġenti li jaffettwa s-sigurtà tas-servizzi u tas-sistemi tat-trasport fuq l-art (inkluża d-data tagħhom)*

- *Bit-teħid inkunsiderazzjoni ta' kwalunkwe restrizzjoni kkonċernata **bil-ġestjoni tal-assi u l-ippjanar tar-riżorsi** (jiġifieri, restrizzjonijiet li jistgħu jaffettwaw il-konsenja, il-manutenzjoni, u l-appoġġ ta' sistemi kritiċi għall-operazzjonijiet ta' funzjonijiet essenzjali fit-trasport fuq l-art).*

Eżempji ta’ oqfsa ta’ ġestjoni tar-riskju: Oqfsa differenti (eż. standards fil-familja ISO/IEC 27000, il-qafas taċ-ċibersigurtà NIST, il-Qafas MITRE ATT&CK, BSI IT-Grundschutz, eċċ.) jistgħu jinfurmaw u jsostnu approċċ imfassal apposta għall-ġestjoni tar-riskju għat-trasport bit-triq u bil-ferrovija. Organizzazzjonijiet bħall-ENISA jiddefinixxu prattiki tajbin għaċ-ċibersigurtà tal-karozzi intelliġenti u tat-trasport pubbliku intelliġenti, li jinfurmaw lill-manifatturi u lill-assoċjazzjonijiet tal-industrija (eż. l-Assoċjazzjoni Ewropea tal-Manifatturi tal-Vetturi – ACEA). Fit-trasport bil-ferrovija, l-Aġenzija tal-Unjoni Ewropea għall-Ferroviji (ERA) tiddefinixxi l-Ispeċifikazzjonijiet Tekniċi ta’ Interoperabbiltà (TSIs), li jridu jiġu ssodisfati minn kull subsistema jew parti mis-subsistema sabiex jiġu ssodisfati r-rekwiżiti essenzjali u sabiex tiġi żgurata l-interoperabbiltà tas-sistema ferrovjarja tal-Unjoni Ewropea. L-Impriża Konġunta Shift2Rail qed tmexxi wkoll l-inizjattivi u l-proġetti tal-innovazzjoni (inkluża ċ-ċibersigurtà) għat-trasport bil-ferrovija.

Protezzjoni kontra Theddid Ċibernetiku

L-organizzazzjonijiet tat-trasport fuq l-art jenħtieġ li jimplimentaw miżuri ta' sigurtà adegwati u proporzjonati sabiex jipproteġu lin-networks u lis-sistemi tal-informazzjoni tagħhom – inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT) minn attakki ċibernetiċi. Miżuri ta' sigurtà jinkludu:

- ***Politiki u Proċessi tas-Sigurtà:*** *id-definizzjoni, l-implimentazzjoni, il-komunikazzjoni u l-infurzar ta' politiki u proċessi xierqa, li jiddefinixxu approċċ ġenerali għall-iżgurar tas-sistemi u tad-data li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fil-modi tat-trasport fuq l-art. Tali politiki u proċeduri ta' sigurtà (eż. politiki dwar il-passwords u dwar il-ħżin) għandhom ikopru wkoll il-ġestjoni tal-patches u tal-vulnerabbiltà tal-hardware u tas-sistemi tas-software (inkluż IT u OT), il-Ġestjoni tal-Inċidenti, il-protezzjoni tas-Sistema u tan-Network.*

- ***Ġestjoni tal-Identitajiet u tal-Aċċess:*** *il-fehim, id-dokumentazzjoni u l-ġestjoni tal-aċċess għan-networks u għas-sistemi tal-informazzjoni (inkluż l-IT u l-OT) li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fil-modi tat-trasport fuq l-art. L-utenti (jew il-funzjonijiet awtomatizzati) li jistgħu jaċċessaw id-data jew is-sistemi jiġu vverifikati, awtentikati u awtorizzati kif xieraq. Dan għandu jqis ukoll ir-rwoli u r-responsabbiltajiet differenti għal kontijiet regolari u privileġġati.*

- ***Sigurtà tad-Data u tas-Sistema:*** *il-protezzjoni tad-data (maħżuna u trażmessa elettronikament), tan-networks kritiċi u tas-sistemi tal-informazzjoni (inklużi l-IT u l-OT) minn attakki ċibernetiċi. Filwaqt li jitqies approċċ xprunat mir-riskju, l-organizzazzjonijiet jenħtieġ li jimplimentaw miżuri ta' sigurtà biex jillimitaw effettivament l-opportunitajiet għal dawk li jwettqu l-attakki biex jikkompromettu d-data, in-networks u s-sistemi. Dawn il-miżuri ta' sigurtà għandhom jinkludu wkoll l-adozzjoni ta' protokolli ta' kriptaġġ u ta' komunikazzjoni sigura sabiex tiġi protetta d-data mistrieħa u fi tranżitu mit-theddid ċibernetiku li jirriżulta f'attakki kkawżati mill-bniedem. Barra minn hekk, huwa meħtieġ li tali miżuri jiġu kkombinati ma' miżuri ta' sigurtà fiżika sabiex jiġi protett l-aċċess għas-sistemi (eż. is-sistemi għandhom ikunu jinsabu fi kmamar konfinati b'aċċess ristrett). Dan huwa importanti ħafna għal dawk is-sistemi li jista' jkollhom impatt fuq is-sikurezza tal-ħajja.*

- ***Reżiljenza tan-Networks u tas-Sistemi:*** *il-bini tar-reżiljenza tan-networks u tas-sistemi (inklużi tal-IT u tal-OT) billi jitfasslu u jiġu implimentati (u l-proċeduri operazzjonali tagħhom) sabiex jirreżistu u jtaffu l-impatt tal-attakki ċibernetiċi. Eżempji ta' soluzzjonijiet ta' disinn u implimentazzjoni li jsaħħu r-reżiljenza huma: funzjonijiet kritiċi vverifikati formalment, in-nuqqas ta' użu ta' sistemi u networks, is-segregazzjoni tan-networks (partikolarment, is-segregazzjoni tal-IT u tal-OT), il-miżuri ta' sigurtà f'diversi livelli u ħafna oħrajn. Innota li minn perspettiva tas-sigurtà tal-informazzjoni, l-oqsma tas-sigurtà li jimplimentaw is-segregazzjonijiet tan-networks u tas-sistema jistgħu jipprovdu soluzzjonijiet ta' sigurtà xierqa. Madankollu, il-ħtiġijiet operazzjonali (eż. l-attivitajiet ta' manutenzjoni, it-trasferimenti tad-data, eċċ.) tas-sistemi jistgħu jeħtieġu l-evitar jew il-konnessjoni ta' oqsma differenti ta' sigurtà (eż. sistemi u networks segregati), inkluż il-konnessjoni tal-IT u tal-OT.*

Identifikazzjoni tat-Theddid Ċibernetiku

Jenħtieġ li l-organizzazzjonijiet jiżguraw li l-miżuri ta’ sigurtà jibqgħu effettivi, u jidentifikaw kwalunkwe avveniment taċ-ċibersigurtà li jaffettwa jew li għandu l-potenzjal li jaffettwa l-kontrolli tas-sigurtà kif ukoll is-servizzi u s-sistemi essenzjali. Sabiex jiġu identifikati t-theddidiet ċibernetiċi, il-miżuri rilevanti ta’ sigurtà huma:

- ***Monitoraġġ tas-Sigurtà:*** *il-monitoraġġ tal-istatus tas-sigurtà tan-networks u tas-sistemi tal-informazzjoni – inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT) – li jappoġġaw l-operazzjonijiet ta’ funzjonijiet essenzjali fil-modi tat-trasport fuq l-art. Dan huwa meħtieġ sabiex jiġu identifikati theddidiet potenzjali għas-sigurtà u sabiex tiġi segwita l-effettività kontinwa tal-miżuri protettivi ta’ sigurtà. Sabiex jiġi appoġġat il-monitoraġġ tas-sigurtà, id-data li titqies hija, pereżempju:*

  - *reġistri tas-sigurtà*
  - *reġistri tad-detezzjoni tal-virusijiet*
  - *reġistri tad-detezzjoni tal-intrużjoni*
  - *reġistri tal-identifikazzjoni, tal-awtentikazzjoni u tal-awtorizzazzjoni*
  - *reġistri tas-sistemi u tas-servizzi*
  - *reġistri tat-traffiku tan-network*
  - *reġistri tal-ipproċessar tad-data*

- ***Sejbien ta’ Event ta’ Sigurtà:*** *l-identifikazzjoni ta’ attivitajiet malizzjużi (jiġifieri avvenimenti ta’ sigurtà) li jaffettwaw jew li għandhom il-potenzjal li jaffettwaw is-sigurtà tan-networks u tas-sistemi tal-informazzjoni (inkluż l-IT u l-OT) li jappoġġaw operazzjonijiet ta’ funzjonijiet essenzjali.*

Dawn il-miżuri jistgħu jeħtieġu l-adozzjoni ta’ teknoloġiji speċifiċi (eż. il-Ġestjoni tal-Informazzjoni u tal-Eventi ta’ Sigurtà, Sistema ta’ Detezzjoni tal-Intrużjoni, Sistema ta’ Prevenzjoni tal-Intrużjoni, eċċ.) u l-istabbiliment ta’ SOC (Ċentru tal-Operazzjonijiet ta’ Sigurtà) jew ekwivalenti. Jiġifieri, l-iżvilupp ta’ mezzi għall-identifikazzjoni, analiżi, rispons u rkupru minn attakki ċibernetiċi lokalment. Skwadri Nazzjonali ta’ Rispons għal Inċidenti relatati mas-Sigurtà tal-Kompjuters (CSIRTs), CERTs settorjali u kummerċjali jew operaturi tat-toroq u tal-ferroviji, u ċ-Ċentru Ewropew tal-Kondiviżjoni u tal-Analiżi tal-Informazzjoni (ER-ISAC) jistgħu jipprovdu Intelliġenza dwar it-Theddid Ċibernetiku (CTI) li tinforma l-monitoraġġ u l-iskoperta tas-sigurtà.

Pjanar tar-rispons u tal-irkupru

L-organizzazzjonijiet għandhom jiddefinixxu, jimplimentaw u jittestjaw il-proċeduri ta' ġestjoni tal-inċidenti, li jkollhom l-intenzjoni li jiżguraw il-kontinwità tan-negozju tas-servizzi u tas-sistemi fl-eventwalità ta' inċidenti taċ-ċibersigurtà.

L-ippjanar tar-rispons u tal-irkupru għandu jqis il-miżuri ta' sigurtà, filwaqt li jtaffi l-impatt ta' attakki speċifiċi taċ-ċibersigurtà, bħal:

- *Il-koordinazzjoni u l-kollaborazzjoni mas-CSIRTs Nazzjonali, mas-CERTs (pubbliċi u kummerċjali) u mal-ISACs matul inċidenti taċ-ċibersigurtà, il-koordinazzjoni tal-inċidenti u kriżijiet fil-livell Pan-Ewropew*

- *Il-kondiviżjoni ta' informazzjoni ma' organizzazzjonijiet oħrajn, inklużi fornituri fil-katina tal-provvista ta' servizzi tat-trasport fuq l-art*

- *It-twettiq ta' eżerċizzji perjodiċi **ta' attakki ċibernetiċi** (simulazzjoni tal-koordinazzjoni kif ukoll teknika) għall-valutazzjoni ta' miżuri u proċeduri ta' sigurtà kif ukoll ir-reżiljenza tal-organizzazzjonijiet biex jittrattaw inċidenti ċibernetiċi*

- *Aċċess għal postijiet ta' ħżin arkivjati jew ta' riżerva f'każ ta' kompromess fl-integrità u d-disponibbiltà tal-ħażniet tad-data*

- ***Il-playbooks tas-sigurtà għandhom** proċeduri dettaljati għall-ġestjoni tal-inċidenti taċ-ċibersigurtà, u biex is-servizzi u s-sistemi jinġiebu lura f'kundizzjonijiet operazzjonali normali*

- *Ridirezzjonijiet tat-traffiku tan-network għal servizzi żejda matul l-attakki taċ-ċaħda tas-servizzi*

- *Proċeduri manwali għat-tħaddim b'servizzi u b'sistemi f'modalitajiet operazzjonali degradati*

- *Id-definizzjoni ta' proċeduri sabiex jiġi indirizzat il-ksur tad-data, inklużi proċeduri biex jiġi ttrattat il-ksur tad-data li jaffettwa d-data personali f'konformità mar-Regolament Ġenerali dwar il-Protezzjoni tad-Data (GDPR) u kwalunkwe regolament jew Direttiva settorjali rilevanti oħra*

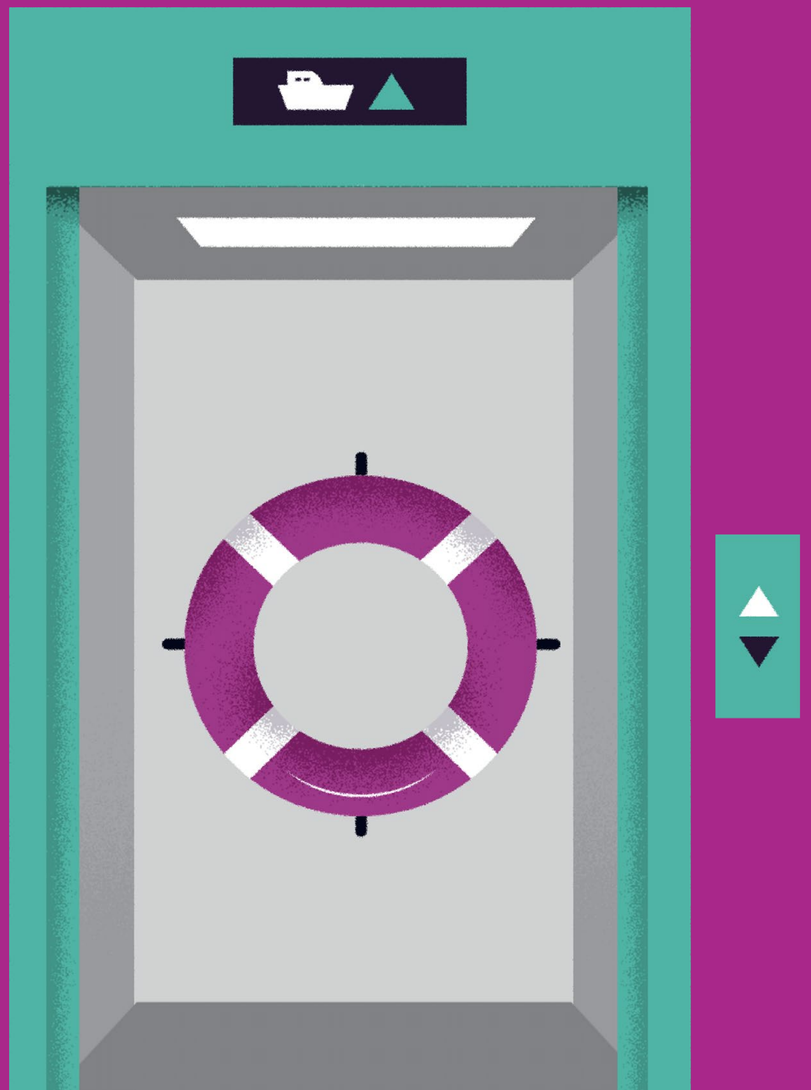
- *L-akkwist ta' **assigurazzjoni ċibernetika** sabiex ir-riskju assoċjat ma' inċidenti ċibernetiċi severi jibda parzjalment*

- *Id-dħul f'kuntratt għal rispons għall-inċidenti ma' ditta/i speċjalizzata/i waħda jew aktar għal kapaċità u għarfien espert addizzjonali*

- *Id-definizzjoni ta' proċeduri għall-kondiviżjoni tal-informazzjoni dwar inċidenti taċ-ċibersigurtà mal-partijiet ikkonċernati rilevanti, inkluż proċeduri għan-notifika ta' inċidenti f'konformità mad-Direttiva NIS (id-Direttiva tal-UE 2016/1148 dwar miżuri għal livell għoli komuni ta' sigurtà tan-networks u tas-sistemi tal-informazzjoni madwar l-Unjoni).*

Il-Kummissjoni Ewropea

Prattiki Tajbin u Miżuri ta’ Sigurtà mfassla għat-Trasport Marittimu



Governanza

L-organizzazzjonijiet fit-trasport marittimu jeħtieġu fehim ċar dwar it-theddid emerġenti sabiex jiddefinixxu l-politiki u l-proċessi ta' ġestjoni biex jirregolaw l-approċċi tagħhom sabiex itejbu ċ-ċibersigurtà tas-servizzi u tas-sistemi fl-operazzjonijiet, inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT).

Prattiki tajbin għall-organizzazzjonijiet ta' kwalunkwe daqs jinvolvu:

- *L-iżgurar li l-livelli ta' maniġment superjuri jirrapportaw ħassib dwar iċ-ċibersigurtà lill-eżekuttivi u lill-bordijiet, li jistgħu jieħdu deċiżjonijiet infurmati dwar l-allokazzjonijiet tar-riżorsi*

- *Il-ħatra ta' rwol superjuri b'responsabbiltajiet ġenerali ta' ġestjoni għas-sigurtà tat-Teknoloġija tal-Informazzjoni (IT) u tat-Teknoloġija Operattiva (OT). Dan ir-rwol għandu jkun responsabbli għaċ-ċibersigurtà kif ukoll għas-sigurtà fiżika*

- *Id-definizzjoni ċara tar-rwoli, tar-responsabbiltajiet, tal-kompetenzi, u tal-awtorizzazzjonijiet relatati maċ-ċibersigurtà, id-definizzjoni tal-livelli tal-awtorità u l-linji ta' komunikazzjoni bejn, u fost, il-persunal tax-xatt u ta' abbord il-bastimenti, u l-qbil fuqhom mal-persunal rilevanti. Dan huwa meħtieġ, partikolarment, għall-membri tal-Iskwadri ta' Rispons f'Emerġenza relatata mal-Kompjuters (CERTs). Il-persunal bi rwoli relatati mal-leġiżlazzjonijiet tal-UE dwar is-sigurtà u s-sikurezza marittima, bħall-Uffiċjali tas-Sigurtà tal-Faċilità tal-Port, l-Uffiċjali tas-Sigurtà tal-Portijiet jew l-Uffiċjali tas-Sigurtà tal-Kumpaniji jew il-Persuna Nnominata fuq l-Art (DPA) u l-Master abbord, jenħtieġ li tal-anqas ikunu familjari mal-miżuri taċ-ċibersigurtà tal-organizzazzjoni*

- *L-iżgurar tal-governanza taċ-ċibersigurtà tul il-katina kollha tas-servizzi tal-provvista tas-sigurtà, inkluż interfaċċi kemm fiżiċi kif ukoll diġitali, mill-manifatturi tat-teknoloġija u mill-installaturi sal-fornituri tas-sigurtà*

- *Il-qbil fuq l-attivitajiet u l-kontrolli, inkluż ir-responsabbiltajiet kondiviżi, għall-ġestjoni tar-riskji taċ-ċibersigurtà, u l-iżgurar li dawn ir-responsabbiltajiet jiġu sostnuti matul il-ħajja kollha (eż. permezz ta' ftehimiet ta' servizz) tas-soluzzjonijiet u s-servizzi ta' sigurtà*

- *Id-definizzjoni ta' mekkaniżmi ta' governanza (eż. politiki) sabiex ikun hemm konformità mal-obbligi meħuda mir-regolamenti u d-direttivi rilevanti, pereżempju, ir-Regolament 2019/1239 li jistabbilixxi sistema ta' Single Window Marittima Ewropea (EMSWe), ir-Regolament 725/2004 dwar it-titjib tas-sigurtà tal-bastimenti u tal-faċilitajiet tal-portijiet, id-Direttiva 2005/65/KE dwar it-titjib fis-sigurtà fuq il-bastimenti u fil-portijiet u r-Regolament (KE) Nru 336/2006 dwar l-implimentazzjoni tal-Kodiċi Internazzjonali dwar l-Amministrazzjoni tas-Sigurtà fi ħdan il-Komunità (ISM), u r-Riżoluzzjoni A.741(18) li tadotta l-Kodiċi ta' Amministrazzjoni Internazzjonali għal Ħidma Sigura ta' Vapuri u għall-Prevenzjoni tat-Tniġġis. F'dan il-kuntest, huwa rilevanti wkoll li jissemma' l-Ambjent Komuni għall-Qsim tal-Informazzjoni (CISE), inizjattiva tal-UE li għandha l-għan li tagħmel is-sistemi ta' sorveljanza Ewropej u tal-Istati Membri interoperabbli biex l-awtoritajiet ikkonċernati kollha jingħataw aċċess għall-informazzjoni klassifikata u mhux klassifikata li jkollhom bżonn biex iwettqu missjonijiet fuq il-baħar.*

Eżempji ta’ servizzi u sistemi fit-trasport marittimu: Eżempji ta’ IT huma dawk aċċessibbli għall-impjegati (eż. kompjuters personali, mowbajls, periferali tal-uffiċċji, eċċ.) kif ukoll għall-passiġġieri (eż. routers pubbliċi tal-Wi-Fi u konnessjonijiet, eċċ.). Eżempji ta’ OT huma s-Sistemi ta’ Kontrolli Superviżorji u tal-Ksib tad-*Data* (SCADA), is-sistemi tat-tisħin, tal-ventilazzjoni, u tal-arja kundizzjonata (HVAC), is-Sistemi ta’ Pożizzjonament Globali (GPS), il-kontroll tal-aċċess, il-monitoraġġ, is-sorveljanza, ir-rispons għall-allarm, it-teknoloġija tal-iskrinjar, is-sistemi tan-navigazzjoni abbord, SafeSeaNet, is-sistemi tal-pont, is-sistemi tal-maniġġ u tal-ġestjoni ta’ merkanzija, il-ġestjoni tal-propulsjoni u tal-makkinarju u s-sistemi ta’ kontroll tal-enerġija, is-sistemi ta’ kontroll tal-aċċess, is-sistemi ta’ manutenzjoni u ta’ ġestjoni tal-passiġġieri, in-networks pubbliċi tal-passiġġieri, is-sistemi amministrattivi u tal-benesseri tal-ekwipaġġ, is-sistemi ta’ komunikazzjoni, u oħrajn.

Identifikazzjoni tat-Theddid Ċibernetiku

Ġestjoni tar-Riskju: L-organizzazzjonijiet marittimi jridu jieħdu passi xierqa biex jidentifikaw, janalizzaw, jivvalutaw, u jikkomunikaw ir-riskji taċ-ċibersigurtà, u jaċċettawhom, jevitawhom, jittrasferixxuhom, jew jimmitigawhom għal livell aċċettabbli. Dan jeħtieġ approċċ organizzazzjonali ġenerali tal-ġestjoni tar-riskju, li jinvolvi:

- *L-iżgurar ta' ħarsa ġenerali ċara lejn id-diversi sistemi tal-hardware u tas-software użati għall-kunsinna ta' servizzi differenti. Fil-kuntest tat-trasport marittimu, tali sistemi jinvolvu t-Teknoloġija tal-Informazzjoni (IT) kif ukoll it-Teknoloġiji Operazzjonali (OT), u kif dawn is-sistemi jikkollegaw u jintegraw man-naħa tal-kosta, inklużi l-awtoritajiet pubbliċi, it-terminals tal-baħar u l-burdnara*

- *L-identifikazzjoni u l-evalwazzjoni ta' operazzjonijiet ewlenin abbord il-bastimenti, li huma vulnerabbli għal attakki ċibernetiċi, u t-twettiq ta' valutazzjonijiet tar-riskju taċ-ċibersigurtà (inkluż il-valutazzjoni tal-impatti operazzjonali potenzjali u l-probabbiltà ta' okkorrenza), li jenħtieġ li jqisu t-theddid emerġenti, il-vulnerabbiltajiet magħrufa, u d-data operazzjonali fir-rigward tas-sistemi fil-kamp ta' applikazzjoni. Fejn xieraq, issir ir-rabta mal-valutazzjonijiet tas-sigurtà mwettqa għall-bastimenti (SSAs), il-faċilitajiet portwarji (PFSAs), u l-portijiet (PSAs) kif stabbilit mil-leġiżlazzjoni tal-UE dwar is-sigurtà marittima. Dawn jidentifikaw theddid tas-sigurtà possibbli għall-infrastruttura tal-port u d-dgħufijiet tas-sigurtà. Barra minn hekk, l-organizzazzjonijiet marittimi bħall-Organizzazzjoni Marittima Internazzjonali (IMO) u l-ISACs marittimi jistgħu jipprovdu għarfien dwar it-theddid li għandu fil-mira t-trasport marittimu.*

- *L-iżgurar li l-valutazzjonijiet tar-riskju jkopru wkoll ir-riskji relatati mal-attivitajiet ta' kuljum tal-persunal (eż. l-użu tal-midja soċjali, l-użu tal-apparat personali, l-ipproċessar tad-data, il-kondiviżjoni tal-informazzjoni, eċċ.)*

- *L-identifikazzjoni u l-implimentazzjoni ta' miżuri u pjanijiet għat-trattament tar-riskji taċ-ċibersigurtà. Pereżempju, l-implimentazzjoni ta' Sistema għall-Ġestjoni tas-Sigurtà tal-Informazzjoni (ISMS) komprensiva u Sistema għall-Ġestjoni tal-Informazzjoni dwar il-Privatezza (PIMS), allinjati ma' sistemi oħrajn ta' ġestjoni bħas-Sistemi ta' Ġestjoni tas-Sikurezza (SMS) f'konformità mal-Kodiċi Internazzjonali tal-Ġestjoni tas-Sikurezza (ISM). Sistemi ta' ġestjoni bħal dawn (jiġifieri l-ISMS u l-PIMS) jinvolvu l-implimentazzjoni ta' kontrolli tas-sigurtà (kif ukoll tal-protezzjoni tad-data u tal-privatezza) sabiex jiġi mmitigat u evitat theddid emerġenti li jaffettwa s-sigurtà tas-servizzi u tas-sistemi marittimi (inkluża d-data tagħhom)*

- *Filwaqt li titqies kwalunkwe restrizzjoni kkonċernata bil-**ġestjoni tal-assi u bl-ippjanar tar-riżorsi** (jiġifieri, restrizzjonijiet li jistgħu jaffettwaw it-twassil, il-manutenzjoni u l-appoġġ ta' sistemi kritiċi għall-operazzjonijiet ta' funzjonijiet essenzjali fit-trasport marittimu). Fir-rigward tal-valutazzjonijiet, għandha ssir kontroreferenza fejn xieraq għar-rekwiżiti tal-kodiċi tal-ISM, tas-Sistemi ta' ġestjoni tas-Sikurezza (SMS) u tal-pjanijiet ta' sigurtà mwettqa skont il-leġiżlazzjoni tal-UE dwar is-sikurezza u s-sigurtà marittima.*

Eżempji ta’ oqfsa ta’ ġestjoni tar-riskju: Oqfsa differenti (eż. il-Kodiċi tal-ISM jew l-istandards fil-familja tal-ISO/IEC 27000, il-qafas taċ-ċibersigurtà NIST, il-Qafas MITRE ATT&CK, BSI IT-Grundschutz, eċċ.) jistgħu jinfurmaw u jsostnu approċċ imfassal apposta għall-ġestjoni tar-riskju għat-trasport marittimu. Il-qafas taċ-ċibersigurtà NIST tfassal apposta wkoll biex jindirizza ċ-ċibersigurtà tat-Trasferiment ta’ Likwidi Marittimi bl-Ingrossa (MBLT), Operazzjonijiet lil hinn mill-Kosta, u Operazzjonijiet ta’ Bastimenti tal-Passiġġieri. Bl-istess mod, il-Kunsill Marittimu tal-Baltiku u Internazzjonali (BIMCO) ħareġ *“il-Linji Gwida dwar iċ-Ċibersigurtà Abbord il-Bastimenti”* u l-Organizzazzjoni Marittima Internazzjonali (OMI) ħarġet linji gwida speċifiċi *“dwar il-ġestjoni tar-riskju ċibernetiku marittimu”* (MSC-FAL.1/Circ.3). L-ENISA wettqet diversi studji kkonċernati bi prattiki tajbin għaċ-ċibersigurtà marittima, partikolarment, iċ-ċibersigurtà fil-portijiet. L-EMSA tipprovdi servizzi lill-komunità marittima, inkluż taħriġ ta’ sensibilizzazzjoni dwar iċ-ċibersigurtà. Standards (eż. IEC 61162-460:2018 dwar is-sikurezza u s-sigurtà tat-tagħmir u s-sistemi ta’ komunikazzjoni bir-radju u n-navigazzjoni marittima, ISO 16425:2013 dwar il-bastimenti u t-teknoloġija tal-baħar, IEC 62443-4-1:2018 dwar is-sigurtà għas-sistemi ta’ awtomatizzazzjoni u kontroll industrijali, eċċ.) jiddefinixxu wkoll rekwiżiti speċifiċi ta’ sigurtà u sikurezza għas-sistemi u n-networks fit-trasport marittimu.

Protezzjoni kontra Theddid Ċibernetiku

L-organizzazzjonijiet fit-trasport marittimu jenħtieġ li jimplimentaw miżuri ta' sigurtà adegwati u proporzjonati sabiex jipproteġu n-networks u s-sistemi tal-informazzjoni tagħhom – inkluż it-Teknoloġija tal-Informazzjoni (IT) u l-miżuri ta' Sigurtà Operazzjonali jinkludu:

- ***Politiki u Proċessi tas-Sigurtà:*** *id-definizzjoni, l-implimentazzjoni, il-komunikazzjoni u l-infurzar ta' politiki u proċessi xierqa, li jiddefinixxu approċċ ġenerali għall-iżgurar tas-sistemi u tad-data li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fit-trasport marittimu. Il-miżuri ta' sigurtà (inklużi l-miżuri ta' sigurtà ċibernetika u fiżika) jenħtieġ li jiġu inklużi fi pjanijiet rilevanti bħas-Sistema ta' Ġestjoni tas-Sikurezza (SMS) u fil-Pjan ta' Sigurtà tal-Bastimenti (SSP). Tali politiki u proċeduri ta' sigurtà (eż. politiki dwar il-passwords u dwar il-ħżin) għandhom ikopru wkoll il-ġestjoni tal-patches u tal-vulnerabbiltà tal-hardware u tas-sistemi tas-software (inkluż IT u OT), il-Ġestjoni tal-Inċidenti, il-protezzjoni tas-Sistema u tan-Network.*

- ***Ġestjoni tal-Identitajiet u tal-Aċċess:*** *il-fehim, id-dokumentazzjoni u l-ġestjoni tal-aċċess għan-networks u għas-sistemi tal-informazzjoni (inkluż l-IT u l-OT) li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fit-trasport marittimu. L-utenti (jew il-funzjonijiet awtomatizzati) li jistgħu jaċċessaw id-data jew is-sistemi jiġu vverifikati, awtentikati u awtorizzati kif xieraq. Dan għandu jqis ukoll ir-rwoli u r-responsabbiltajiet differenti għal kontijiet normali u privileġġati.*

- ***Sigurtà tad-Data u tas-Sistema:*** *il-protezzjoni tad-data (maħżuna u trażmessa elettronikament), tan-networks kritiċi u tas-sistemi tal-informazzjoni (inklużi l-IT u l-OT) minn attakki ċibernetiċi. Filwaqt li jitqies approċċ xprunat mir-riskju, l-organizzazzjonijiet għandhom jimplimentaw miżuri ta' sigurtà biex jillimitaw effettivament l-opportunitajiet għal dawk li jwettqu l-attakki biex jikkompromettu d-data, in-networks u s-sistemi. Dawn il-miżuri ta' sigurtà għandhom jinkludu wkoll l-adozzjoni ta' protokolli ta' kriptaġġ u ta' komunikazzjoni sigura sabiex tiġi protetta d-data mistrieħa u fi tranżitu mit-theddid ċibernetiku li jirriżulta f'attakki kkawżati mill-bniedem. Barra minn hekk, huwa meħtieġ li tali miżuri jiġu kkombinati ma' miżuri ta' sigurtà fiżika sabiex jiġi protett l-aċċess għas-sistemi (eż. is-sistemi għandhom ikunu jinsabu fi kmamar konfinati b'aċċess ristrett). Dan huwa importanti ħafna għal dawk is-sistemi li jista' jkollhom impatt fuq is-sikurezza tal-ħajja (eż. sistemi ta' navigazzjoni u komunikazzjoni bir-radju tal-kategoriji II u III).*

- ***Reżiljenza tan-Networks u tas-Sistemi:*** *il-bini tar-reżiljenza tan-networks u tas-sistemi (inklużi tal-IT u tal-OT) billi jitfasslu u jiġu implimentati (u l-proċeduri operazzjonali tagħhom) sabiex jirreżistu u jtaffu l-impatt tal-attakki ċibernetiċi. Eżempji ta' soluzzjonijiet ta' disinn u implimentazzjoni li jsaħħu r-reżiljenza huma: funzjonijiet kritiċi vverifikati formalment, in-nuqqas ta' użu ta' sistemi u networks, is-segregazzjoni tan-networks (partikolarment, is-segregazzjoni tal-IT u tal-OT), il-miżuri ta' sigurtà f'diversi livelli u ħafna oħrajn. Innota li minn perspettiva tas-sigurtà tal-informazzjoni, l-oqsma tas-sigurtà li jimplimentaw is-segregazzjonijiet tan-networks u tas-sistema jistgħu jipprovdu soluzzjonijiet ta' sigurtà xierqa. Madankollu, il-ħtiġijiet (eż. l-attivitajiet ta' manutenzjoni, it-trasferimenti tad-data, eċċ.) tas-sistemi (eż. Vapuri Marittimi Awtonomi li Jibqgħu fil-Wiċċ) jistgħu jeħtieġu l-evitar jew il-konnessjoni ta' oqsma differenti ta' sigurtà (eż. sistemi u networks segregati), inkluż il-konnessjoni tagħhom l-IT u l-OT.*

Identifikazzjoni tat-Theddid Ċibernetiku

Jenħtieġ li l-organizzazzjonijiet jiżguraw li l-miżuri ta' sigurtà jibqgħu effettivi, u jidentifikaw kwalunkwe avveniment taċ-ċibersigurtà li jaffettwa jew li għandu l-potenzjal li jaffettwa l-kontrolli tas-sigurtà kif ukoll is-servizzi u s-sistemi essenzjali. Sabiex jiġu identifikati t-theddidiet ċibernetiċi, il-miżuri rilevanti ta' sigurtà huma:

■ ***Monitoraġġ tas-Sigurtà:*** *il-monitoraġġ tal-istatus tas-sigurtà tan-networks u tas-sistemi tal-informazzjoni – inkluż it-Teknoloġija tal-Informazzjoni (IT) u t-Teknoloġija Operattiva (OT) –li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fis-servizzi tat-trasport marittimu. Dan huwa meħtieġ sabiex jiġu identifikati theddidiet potenzjali għas-sigurtà u sabiex tiġi segwita l-effettività kontinwa tal-miżuri protettivi ta' sigurtà. Sabiex jiġi appoġġat il-monitoraġġ tas-sigurtà, id-data li titqies hija, pereżempju:*

- *reġistri tas-sigurtà*
- *reġistri tad-detezzjoni tal-virusijiet*
- *reġistri tad-detezzjoni tal-intrużjoni*
- *reġistri tal-identifikazzjoni, tal-awtentikazzjoni u tal-awtorizzazzjoni*
- *reġistri tas-sistemi u tas-servizzi*
- *reġistri tat-traffiku tan-network*
- *reġistri tal-ipproċessar tad-data*

■ ***Sejbien ta' Event ta' Sigurtà:*** *l-identifikazzjoni ta' attivitajiet malizzjużi (jiġifieri avvenimenti ta' sigurtà) li jaffettwaw jew li għandhom il-potenzjal li jaffettwaw is-sigurtà tan-networks u tas-sistemi tal-informazzjoni (inkluż l-IT u l-OT) li jappoġġaw l-operazzjonijiet ta' funzjonijiet essenzjali fis-servizzi tat-trasport bil-baħar.*

Dawn il-miżuri jistgħu jeħtieġu l-adozzjoni ta' teknoloġiji speċifiċi (eż. il-Ġestjoni tal-Informazzjoni u tal-Eventi ta' Sigurtà, Sistema ta' Detezzjoni tal-Intrużjoni, Sistema ta' Prevenzjoni tal-Intrużjoni, eċċ.) u l-istabbiliment ta' SOC (Ċentru tal-Operazzjonijiet ta' Sigurtà) jew ekwivalenti.

Jiġifieri, l-iżvilupp ta' mezzi għad-detezzjoni, analiżi, rispons u rkupru minn attakki ċibernetiċi lokalment.

Skwadri Nazzjonali ta' Rispons għal Inċidenti relatati mas-Sigurtà tal-Kompjuters (CSIRTs), CERTs settorjali u CERTs kummerċjali tal-operaturi marittimi, l-ISCs marittimi jistgħu jipprovdu Intelliġenza dwar Theddid Ċibernetiku (CTI) li jinformaw il-monitoraġġ u l-iskoperta tas-sigurtà.

Pjanar tar-rispons u tal-irkupru

L-organizzazzjonijiet għandhom jiddefinixxu, jimplimentaw u jittestjaw il-proċeduri ta' ġestjoni tal-inċidenti, li jkollhom l-intenzjoni li jiżguraw il-kontinwità tan-negozju tas-servizzi u tas-sistemi fl-eventwalità ta' inċidenti taċ-ċibersigurtà. L-ippjanar tar-rispons u tal-irkupru għandu jqis il-miżuri ta' sigurtà, filwaqt li jtaffi l-impatt ta' attakki speċifiċi taċ-ċibersigurtà, bħal:

- *Ridirezzjonijiet tat-traffiku tan-network għal servizzi żejda matul l-attakki taċ-ċaħda tas-servizzi*
- *Proċeduri manwali għat-tħaddim b'servizzi u b'sistemi f'modalitajiet operazzjonali degradati*
- *L-istabbiliment ta' programmi għal drills u eżerċizzji (eż. koordinazzjoni "table top", eżerċizzji tekniċi u ta' rispons) bħala rispons għal attakki ċibernetiċi u sitwazzjonijiet ta' emerġenza kif ukoll biex jiġu vvalutati l-miżuri ta' sigurtà, il-proċeduri u r-reżiljenza organizzazzjonali biex jiġu indirizzati l-inċidenti ċibernetiċi*
- *Aċċess għal postijiet ta' ħżin arkivjati jew ta' riżerva f'każ ta' kompromess fl-integrità u d-disponibbiltà tal-ħażniet tad-data*
- *Il-koordinazzjoni u l-kollaborazzjoni mas-CSIRTs Nazzjonali, mas-CERTs (pubbliċi u kummerċjali) u mal-ISACs matul inċidenti taċ-ċibersigurtà, il-koordinazzjoni tal-inċidenti u kriżijiet fil-livell Pan-Ewropew*
- *Il-kondiviżjoni ta' informazzjoni ma' organizzazzjonijiet oħrajn, inklużi fornituri fil-katina tal-provvista ta' servizzi fit-trasport marittimu*
- *Il-playbooks tas-sigurtà għandhom proċeduri dettaljati għall-ġestjoni tal-inċidenti taċ-ċibersigurtà, u biex is-servizzi u s-sistemi jinġiebu lura f'kundizzjonijiet operazzjonali normali*
- *Id-definizzjoni ta' proċeduri sabiex jiġi indirizzat il-ksur tad-data, inklużi proċeduri biex jiġi ttrattat il-ksur tad-data li jaffettwa d-data personali f'konformità mar-Regolament Ġenerali dwar il-Protezzjoni tad-Data (GDPR) u kwalunkwe regolament jew Direttiva settorjali rilevanti oħra*
- *L-akkwist ta' assigurazzjoni ċibernetika sabiex ir-riskju assoċjat ma' inċidenti ċibernetiċi severi jibda parzjalment*
- *Id-dħul f'kuntratt għal rispons għall-inċidenti ma' ditta/i speċjalizzata/i waħda jew aktar għal kapaċità u għarfien espert addizzjonali*
- *Id-definizzjoni ta' proċeduri għall-kondiviżjoni tal-informazzjoni dwar inċidenti taċ-ċibersigurtà (inkluż nuqqasijiet ta' konformità, aċċidenti u sitwazzjonijiet perikoluż) mal-partijiet ikkonċernati rilevanti, inkluż proċeduri għan-notifika ta' inċidenti f'konformità mad-Direttiva NIS (id-Direttiva tal-UE 2016/1148 dwar miżuri għal livell għoli komuni ta' sigurtà tan-networks u tas-sistemi tal-informazzjoni madwar l-Unjoni).*

Il-Lussemburgu: L-Uffiċċju tal-Pubblikazzjonijiet tal-Unjoni Ewropea, 2021

Print ISBN 978-92-76-40477-4 doi:10.2832/059371 MI-05-21-230-MT-C
PDF ISBN 978-92-76-40485-9 doi:10.2832/043129 MI-05-21-230-MT-N

L-Uffiċċju tal-Pubblikazzjonijiet
tal-Unjoni Ewropea