【欧州】【Common】

Common - Latest trends in digital transformation: Cyber security incidents in the transport sector and its sub-sectors

Andrea Antolini Former Researcher JTTRI

【概要：Summary】

In the EU, the increasing level of digitalisation in all sectors has also increased the threat and the number of cyber-attacks in the past years. In the transport sector, the emergence of semi-autonomous vehicles, the increasingly used information and communications technology (ICT) and the use of AI techniques, potentially increase the risks of cyberattacks. and cybersecurity challenges in general.

To improve cybersecurity at European level, the EU Agency for Cybersecurity (ENISA), and an EU cybersecurity certification framework for information and communication technology (ICT) products, services, and processes has been established. ENISA aims to improve the resilience of the EU's information networks against cyber threats and attacks and coordinates responses to large-scale cross-border cyber incidents. To improve cybersecurity in the transport sector, the EU has introduced legal instruments for protecting electronic communications networks and a Transport Cybersecurity Toolkit.

ENISA's 2023 Report on the Transport Threat Landscape analyses the situation of cyber incidents in the transport sector from January 2021 to October 2022. It is the first ENISA report on the cyber threat landscape of the transport sector in the EU and aims to analyse the reality of the cyber threats in transport and its sub-sectors. The ENISA 2023 report analyses the prime threats, actors, and trends of cyberattacks targeting aviation, maritime, railway and road transport in a period of almost two years. The report identifies distinct threats including data-related issues and ransomware, which is becoming a major concern. Cybercriminals and hacktivists are the primary cyber threat actors in the transport sector.

Thereby, the ENISA threat transport landscape report intends to help decision-makers, policymakers, and security specialists to define strategies for better defending citizens, organisations, and cyberspace.

The ENISA report concludes that the transport sector is a lucrative target for cybercriminals, with customer data being a commodity and with highly valuable proprietary information in the transport supply chain.

However, the report also finds that attacks are underreported by organisations, for not risking a negative image. To change this, the transport sector must adapt to evolving cyber threats and improve its cybersecurity measures. The NIS 2 Directive aims to improve incident reporting and oversight with additional notification provisions towards an increased level of cyber security also in the transport sector and its sub-sectors.

【記事：Article】

1. Cyber Security related legislation and measures in the EU

As the digitalisation of the transport sector increases, also companies in the transport sector are increasingly exposed to cyber-threats and cyber-attacks. In the past years, the EU has implemented some legislative acts and initiatives to strengthen cybersecurity capacities to make Europe more cyberthreat-resilient. In 2016, the EU adopted the first legislative act regarding cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). Under the NIS Directive, measures, and obligations for operators of essential services are implemented to protect their digital services against cyber threats and attacks across all sectors, including the transport sector. They must adopt risk management practices and report significant incidents to the national authorities. Furthermore, in September 2017, the European Commission presented a proposal on the European Union Agency for Cybersecurity (ENISA), the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM (2017) 477 final). This resulted in Regulation (EU) 2019/881 on ENISA (the Cybersecurity Act), which introduces, for the first time, EU wide rules for the cybersecurity certification of products, processes, and services (Regulation (EU) 2019/881). In addition, Regulation (EU) 2019/881 defines a new permanent mandate for the EU Agency for Cybersecurity (ENISA). The Cybersecurity Act upgrades ENISA into a permanent EU agency for cybersecurity and strengthens ENISA's ability to help EU Member States to address cybersecurity threats, while acting as a centre of expertise dedicated to enhancing network and information security in the EU. Since 2019, the ENISA Agency has the main aim to improve the resilience of Europe's information infrastructure and networks against cyber threats and attacks.

ENISA contributes to the EU's cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes. The Agency cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges.

Regarding the vulnerabilities of the transport sector and its cyber security, the EU works on measures to make the system more resilient to cyber threats. On 16 December 2020, the European Commission adopted a new Strategy on Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final) with the aim to strengthening the EU's resilience and collective response to cyberthreats (JOIN(2020) 18 final). The strategy aims at improving the resilience against cyberattacks in transport, energy and health, telecommunications, and other sectors, because these are sectors, reliant on interconnected network and information systems (JOIN(2020) 18 final).

The Commission also proposed to reform the rules on the security of network and information systems, under the revision of the NIS Directive. This "NIS 2 Directive" is intended to increase the level of cyber resilience of critical public and private sectors, including critical infrastructure and services to modernise the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape. It is also intended to increase the level of cyber resilience of critical public and private sectors, including energy grids, railways, but also data centres, public administrations, as well as other critical infrastructure and services (COM(2020) 823 final). The EU cybersecurity rules in NIS2 Directive (Directive (EU) 2022/2555), which came into force on 16 January 2023, expands the scope

of the cybersecurity rules to new sectors and entities. It ensures that Member States cooperate, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States. It also further improves the resilience and incident response capacities of public and private entities, competent authorities, and the whole EU (Directive (EU) 2022/2555, European Commission 2023a).

The NIS 2 Directive also includes a deadline for the EU Member States to adopt and publish the measures necessary to comply with the NIS 2 Directive by 17 October 2024, while the former NIS Directive (Directive (EU) 2016/1148) is repealed with effect from 18 October 2024 (Directive (EU) 2022/2555). By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services, that will have to be updated on a regular basis and at least every two years thereafter. By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of the NIS 2 Directive, and report to the European Parliament and to the Council (Directive (EU) 2022/2555).

Furthermore, on 18 April 2023, the European Commission presented a proposal on a regulation amending the EU Cybersecurity Act (Regulation (EU) 2019/881) to enable the adoption of European certification schemes for 'managed security services' (COM(2023) 208 final).

2. Strengthening cyber security in the transport sector

With the emergence of semi-autonomous and autonomous cars, which make use of advanced machine learning and artificial intelligence techniques, the potential risks and cybersecurity will increase. With the increased connectivity that will be driven by the emergence of 5G broadband technology standard, it is expected that new cybersecurity risks and threats will arise, which need to be managed.

Furthermore, the introduction of autonomous vehicles with level 4 or 5 of autonomy by 2030 including AI functions will require the automotive industry to improve its level of preparedness and incident response capabilities to handle emerging cybersecurity issues connected to AI. Cyberattacks targeting smart cars including connected and automated vehicles could lead to a vehicle's immobilisation, road accidents and endanger also other road users' safety, among others.

Therefore, since the challenges of cyber security of the Internet of things (IoT) and the digitally connected devices including autonomous vehicles are increasing, measures need to be introduced to improve the resilience against cyberattacks also in the transport sector.

ENISA addresses the autonomous vehicles' cybersecurity issues as it intends to provide generic security measures to enhance cybersecurity across EU. It also addresses and responds to network and information security problems and provides legal measures to boost the overall level of cybersecurity in the EU.

On 25 November 2019, ENISA published its study entitled "ENISA Good Practices for Security of Smart Cars" regarding cybersecurity and resilience of smart cars (ENISA 2019a). The ENISA study defines good practices for security of smart cars, including connected and (semi-) autonomous vehicles and identifies the smart cars' sensitive assets, as well as the potential and main cyber threats, risks, and attack scenarios for smart cars (ENISA 2019a). According to a 2021 study of ENISA and JRC, the automotive industry should introduce a "security by design" approach for the development and deployment of AI functionalities, where cybersecurity becomes the central element of the entire supply chain for autonomous vehicles (Dede et.al. 2021).

In the maritime and offshore industry, Internet of Things (IoT) sees rising interest and is considered as one of the key digital trends, along with the development of autonomous and unmanned vessels, block chain, and artificial intelligence (ENISA 2019b). The digitalization of the maritime transport sector makes the about 50,000 operating ships a potential target to cyber threats and cyberattacks. In addition, ships can be attacked through data connections with the land-based services. Therefore, based on the linkage between on-board and terrestrial systems, the cyber security of the ship is also dependent on the cyber security of the land-based infrastructure. However, the global shipping industry is considered being a decade behind other sectors regarding the improvement of cyber security, although the shipping industry, the port authorities and operators have realised the need to take measures for improving their cyber security (ENISA 2019b).

In the aviation and maritime transport sector, current EU legislation already obliges authorities and stakeholders to perform risk assessments that identify critical data and put in place suitable measures addressing any risks. These measures need to be further developed to improve cyber awareness, cyber resilience, training, and information sharing.

ENISA has already issued guidance on managing cybersecurity risks in the rail sector and in ports, while EASA is working on legislation to ensure safety in civil aviation (COM (2022) 211 final). Furthermore, the European Commission has published a “Transport Cybersecurity Toolkit” on 16 December 2020 to address transport organisations with a collection of recommendations and good practices to enhance cybersecurity and cyber-resilience (European Commission 2021). The toolkit considers basic information on four threats, namely malware diffusion, denial of service, unauthorised access and theft, and software manipulation. For each transport mode, the toolkit provides guidance on identifying, protecting, detecting, and responding to cyber-threats (European Commission 2021).

Considering those threats affecting transport organisations, the toolkit lists mitigating practices and also provides more advanced information for security and cybersecurity professionals regarding the transport modes air, maritime and land regarding cyber-awareness and cybersecurity (European Commission 2021).

3. ENISA’s 2023 Report on the Transport Cyber threat landscape

Regarding the strengthening of cybersecurity in the transport sector, in 2023, ENISA published a report on the cyberthreat situation in the transport sector, entitled “Threat Landscape: Transport Sector”. This report is the first analysis conducted by ENISA on the cyber threat landscape of the transport sector in the EU and analyses the situation of cyber incidents in the transport sector from January 2021 to October 2022 (ENISA 2023a). The report aims to bring new insights into the transport sector’s reality of the cyber incidents by identifying prime threats, actors and trends based on the analysis of cyberattacks in aviation, maritime transport, railway, and road transport (ENISA 2023a). The report includes the analysis of the general threat landscape, the types of incidents, an assessment of threat actors and their motivations, the affected assets, the threat targets, and the major trends for each sub-sector (ENISA 2023a).

According to the analyses in this first ever ENISA report on the cyber threat landscape in the transport sector, the transport sector is considered being a lucrative business for cybercriminals, with customer data information being considered a highly valuable commodity (ENISA 2023b). The ENISA report shows six main threats affecting the transport sector,

including ransomware attacks; data related threats; malware; denial-of-service (DoS), distributed denial-of-service (DDoS) and ransom denial-of-service (RDoS) attacks; phishing/spear phishing; and supply-chain attacks (ENISA 2023a).

According to the report, ransomware attacks have become the most significant threat against the transport sector during 2022, surpassing data-related threats, which were the most significant threat in 2021 (ENISA 2023b). The ENISA report shows that the main threat identified is ransomware attacks (38%), followed by data related threats (30%), malware (17%), denial-of-service (DoS), distributed denial-of-service (DDoS) and ransom denial-of-service (RDoS) attacks (16%), phishing / spear phishing (10%), and supply-chain attacks (10%) (ENISA 2023b).

Furthermore, the ENISA report distinguishes four different categories of cybersecurity threat actors including state-sponsored actors, cybercriminals, hackers-for-hire, and hacktivists. State-sponsored actors are usually affiliated with a nation state and target organisations to compromise, steal, change, or destroy information (ENISA 2023b). The cybercriminals' primary motive is financial gain, often stealing data or demanding ransom, while hackers-for-hire sell their services to people who do not have the skills or capabilities to do so (ENISA 2023b). Finally, hacktivists are politically, socially, or ideologically motivated and target victims for publicity or to effect change (ENISA 2023b).

According to the ENISA report, the threat actors with the biggest impact on the transport sector were state-sponsored actors, cybercriminals, and hacktivists during the report period. In 2022, cybercriminals were responsible for most attacks on the transport sector, targeting all transport subsectors. 55% of the incidents observed in the reporting period were linked to cybercriminals, but the transport sector is not the only targeted sector as their motive for the attacks is financial gain (ENISA 2023a).

One fourth of the attacks are linked to hacktivist groups (23%), with the motivation of their attacks usually being linked to the geopolitical environment and aiming at operational disruption (20%) or they have an ideological motivation (6%) (ENISA 2023b). The report shows that hacktivist groups' share is on the rise, and they are increasingly targeting the transport sector. These actors mostly conduct distributed denial-of-service (DDoS) attacks, mainly targeting European airports, railways, and transport authorities (ENISA 2023a, 2023b). There was no reliable information in how far a cyberattack affected the safety of transport (ENISA 2023b). However, these DDoS attacks targeting the transport sector are expected to continue to increase.

The report shows that state-sponsored cybersecurity threat actors are mostly targeting the maritime sector and transport related government authorities, including also national or international transport organisations of all sub-sectors as well as ministries of transport (ENISA 2023a).

Considering the main threats per transport sub-sector, the aviation sector reported multiple threats in the reporting period with mostly data-related threats with customer data of airlines and proprietary information of original equipment manufacturers (OEM), being the prime targeted assets, combined with ransomware, and malware (ENISA 2023a). In 2022, there has been a rise in the number of ransomware attacks affecting airports (ENISA 2023b).

The ENISA report also shows that the maritime sector experiences ransomware, malware, and phishing attacks and these attacks mostly target port authorities, port operators, and manufacturers. State-sponsored attackers often conduct politically motivated attacks, causing operational disruptions at ports and on vessels (ENISA 2023a, 2023b).

Regarding the railway sector, the threats range from ransomware to data-related threats primarily targeting IT systems including passenger services, ticketing systems, and mobile applications, causing service disruptions (ENISA 2023a). Hacktivist groups have been conducting DDoS attacks against railway companies with an increasing rate, due to Russia's invasion of Ukraine (ENISA 2023b).

In road transport, the cyber threats are predominantly ransomware attacks, followed by data-related threats and malware (ENISA 2023a). In the automotive industry, especially Original Equipment Manufacturers (OEM) and suppliers have been targeted by ransomware leading to production disruptions (ENISA 2023b). Data-related cyber threats have targeted IT systems to acquire customer and employee data as well as proprietary information (ENISA 2023a).

Despite the EU Member States having legal requirements for the mandatory reporting of cyber incidents, it is often the attackers disclosing the cyberattacks first, but they do not disclose too many details. Instead, the attacked organisations tend to keep the information on threats to themselves to avoid a negative impact on their image.

Therefore, although ENISA gathered data from a variety of sources for its analysis, it is the main weakness of this report that ENISA's information on incidents remains limited. There are also concerns that the number and quality of non-disclosed incidents is high and outweigh by far those incidents made public (ENISA 2023a).

Therefore, the NIS 2 Directive and its additional notification provisions for security incidents aim to support a better overview on relevant incidents, which could also help to improve ENISA's future reports on the cyber threats in the transport sector (ENISA 2023a).

4. Conclusion

The increasing digitalization of the transport sector, including IoT and autonomous vehicles, has also led to more cybersecurity challenges and a new risk level for cyber threats. Accordingly, the EU has introduced legal tools like the NIS Directive, the NIS 2 Directive, and the Cybersecurity Act to establish EU-wide rules for increasing cybersecurity and cyber resilience in various sectors, including the transport sector.

In 2020, the European Commission also presented the "Transport Cybersecurity Toolkit", addressing threats like malware, denial of service, unauthorized access, and software manipulation, and offering guidance and recommendations to all staff and cybersecurity professionals in air, maritime, and land transport organisations to enhance cybersecurity and cyber-resilience.

In March 2023, ENISA presented its report on the transport sector's cyber threat landscape, identifying six main kinds of cyber threats, which include ransomware, data-related threats, malware, DoS/DDoS/RDoS attacks, phishing/spear phishing, and supply-chain attacks. Threat actors will increasingly conduct ransomware attacks with not only monetary motivations. As ransomware groups are taking sides also in political crisis and conflicts like Russia's was against Ukraine, pro-Russian/anti-NATO hacktivists are likely to continue to conduct retaliatory attacks against critical infrastructure. The increasing volume of DDoS attacks against the European transport sector was primarily observed in Q2 and Q3 2022, mainly targeting European airports, railways, and transport authorities. Consequently, the ENISA report concludes that the significant increase in hacktivist activity, which followed Russia's unprovoked invasion of Ukraine, and the increasing rate of DDoS attacks are very likely to continue.

However, the ENISA report also concludes that most organisations that have been victims of

cyberattacks prefer to deal with the problem internally to avoid bad publicity. In general, they rarely report on cyberattacks, especially those with non-significant impact or near misses. Therefore, in most cases a security attack is first disclosed by the attacker.

Against this background, the revised NIS 2 directive and the enhanced notification provisions for security incidents can be expected to increase the reporting of cyber incidents and thereby support a better understanding and oversight of relevant cyber threats and attacks in the transport sector.

References

COM (2017) 477 final: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''). COM/2017/0477 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0477, accessed 4 October 2023

COM(2022) 211 final: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A contingency plan for transport. COM (2022) 211 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A211%3AFIN, 23.5.2022, accessed 4 October 2023

COM/2023/208 final: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services. COM/2023/208 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208, accessed 4 October 2023

Dede, G., Hamon, R., Junklewitz, H., Naydenov, R., Malatras, A. and Sanchez, I.(2021): Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving, EUR 30568 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-28646-2, doi:10.2760/551271, JRC122440. In: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving, accessed 4 October 2023

Directive (EU) 2016/1148: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. In: OJ L 194, 19.7.2016, p. 1-30, https://eur-lex.europa.eu/eli/dir/2016/1148/oj, accessed 4 October 2023

Directive (EU) 2022/2555: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) PE/32/2022/REV/2. OJ L 333, 27.12.2022, p. 80-152. In: https://eur-lex.europa.eu/eli/dir/2022/2555, 27.12.2022, accessed 4 October 2023

ENISA (n.d.): Supporting the implementation of Union policy and law regarding cybersecurity. Cybersecurity Policy. In: https://www.enisa.europa.eu/topics/cybersecurity-policy, no date, accessed 6 October 2023

ENISA (2019a): ENISA puts Cybersecurity in the driver's seat. In: https://www.enisa.europa.eu/news/enisa-news/enisa-puts-cybersecurity-in-the-drivers-seat, November 25, 2019, accessed 4 October 2023

ENISA (2019b): Port Cyber security - Good practices for cyber security in the maritime sector. In: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-

in-the-maritime-sector, November 26, 2019, accessed 4 October 2023

ENISA (European Union Agency for Cybersecurity, ENISA) (2023a): Understanding Cyber Threats in Transport. In: https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport, March 21, 2023, accessed 4 October 2023

ENISA (European Union Agency for Cybersecurity, ENISA) (2023b): THREAT LANDSCAPE: TRANSPORT SECTOR. (January 2021 to October 2022). In: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape, 21 MARCH 2023, accessed 4 October 2023

European Commission (2021): European Commission publishes 'Cybersecurity Toolkit' to raise awareness on cyber-risks and build preparedness in the transport sector. In: https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en, 20 July 2021, accessed 6 October 2023

ENISA (European Union Agency for Cybersecurity, ENISA) (2023): Understanding Cyber Threats in Transport. In: https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport, March 21, 2023, accessed 4 October 2023

European Commission (2023a): Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). In: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, last update 14 September 2023, accessed 6 October 2023

European Commission (2023b): Cybersecurity. In: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity, 16 June 2023, accessed 6 October 2023

JOIN(2020) 18 final: JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. JOIN/2020/18 final. In: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018, 16/12/2020, accessed 4 October 2023

Regulation (EU) 2019/881: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). In: PE/86/2018/REV/1. In: OJ L 151, 7.6.2019, p. 15-69, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881, 17 April 2019, accessed 4 October 2023