PREDRAG ŠKUNDRIĆ
Yunycom d.o.o,
Bulevar Oslobođenja 185
Belgrade, Serbia,
E-mail: predrag@skundric.com

VANJA KORAĆ
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,

ZORAN DAVIDOVAC
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,

Received: June 7th 2022
Accepted: November 15th 2022
Original research article
UDC: 007:004.056.5(4-672EU)
https://doi.org/10.18485/arhe_apn.2022.18.18

EU CYBER INITIATIVES AND INTERNATIONAL CYBERSECURITY STANDARDS – AN OVERVIEW

ABSTRACT

The paper presents the legal directives, decisions, instruments, and policies as the holder of the strategic development of the EU digital transition. EU initiatives and international cybersecurity standards are covered through the EU Strategic initiatives and international cybersecurity standards. Cross-sectoral standards of cybersecurity and cross-sectoral good cybersecurity practices are particularly emphasised. The recommendations of the security standards in the energy, transport, financial and banking sector, health sector, water supply and drinking water distribution sector, and digital service providers sector have been provided. This also represents the ultimate goal of the NIS directive, which implies ensuring the network and information security of the systems in the mentioned sectors.

KEYWORDS: INFORMATION SECURITY, CYBER INITIATIVES, INTERNATIONAL SECURITY STANDARDS.

INTRODUCTION

EU cyber initiatives

The European Union sees digital transformation as one of the basic features of the future. This transformation is of key importance for realising the transition towards climate-neutral, circular, and resilient economies. In the wider context, it brings to the Union prosperity, security and competitiveness, as well as the well-being of European societies.(1)

The strategic direction of the Union's digital transition development is a long-term process that includes a broad spectrum of legal directives, decisions, instruments and policies:

- Data Governance Act(2),
- Digital Services Act(3),
- Digital Markets Act(4),
- Cybersecurity Strategy for the Digital Decade (5)
- The Union Budgetary Instruments: Cohesion programmes, Technical Support Instrument, Digital Europe Programme6, Horizon Europe7 and InvestEU (8).
- Security Union Strategy (9),
- Skills Agenda of the EU,
- Digital Education Action Plan (10)
- 2021 Strategic Foresight Report (11)
- Green deal package (12).

EU digital decade

The European Commission adopted the decision named "2030 Digital Compass: The European way for the Digital Decade" ("Digital Compass Communication") (13) on 9 March 2021, which presents the vision, goals, and methods for the successful digital transformation of the European Union by 2030.

The "Path to the Digital Decade" programme aims to ensure that the European Union accomplishes its goals in the direction of the digital transformation of society and economy in accordance with EU values, reinforcing digital management, and promoting the digital policy that strengthens citizens and companies. The digital targets for 2030 are based on four fundamental points: digital skills, digital infrastructure, digitalisation of companies, and public services.

Solving the massive staff shortage in cybersecurity is vital for protecting the EU from internet threats. In accordance with the Social Rights Action Plan, the plan of the EU is the training of 20 million employed specialists in information and communication technology.

Governments have the role of initiators of the new platforms for building safe public services.(14)

EU INICIATIVES AND INTERNATIONAL CYBERSECURITY STANDARDS

EU strategic initiatives

The central place in the new EU Cybersecurity Strategy (adopted on 16/12/2020) are three initiatives whose integral parts are:

Critical infrastructure protection,

Small and medium-sized enterprises protection, and

Cyber diplomacy.

Extreme exposure to cyber threats (15-17) initiated the launch of a whole set of initiatives to find solutions for the strategic weaknesses of internet technologies, with a particular focus on DNS service vulnerabilities (18-21).

The establishment of the so-called EU Cyber Diplomacy Network is intended to "promote the EU vision of cyberspace, exchange of information and coordination of development." In addition, it has been announced that the EU will develop the "EU External Cyber Capacity Building Agenda" that will be in line with the "External Cyber Capacity Building Guidelines" (22) and the 2030 Agenda for Sustainable Development. (23)

The EU will continue to work in the UN on introducing consensus on cyberspace and responsibility in cyberspace. (24-25) The so-called "Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA)" (26) is under preparation in the UN. The PoA provides a legal platform for cooperation and the exchange of information.

International cybersecurity standards

According to Directive (EU), 2016/1148 published by the European Parliament and Council of Europe, the directive regarding the security of *Network and Information Systems* ("NIS") (27) refers to the security framework that provides necessary services to the European market.

The ultimate goal of the NIS directive is to ensure network and information system security in all sectors (energy, transport, water and food, banking, financial market infrastructure, healthcare, and digital infrastructure) that are of vital social and economic importance and which depend on ICT [*Information* and *communication technologies]* (Article 5, 2-6, NISD). Operators identified by the Member States as OES (Operators of Essential Services) should undertake appropriate and proportional technical and organisational measures for risk management intended for network and information systems security (Article 14, 51, NISD).

With the adoption of the directive on the security of Network and Information Systems (NIS) in 2016, a basic security level of network and information systems should be achieved at the EU level. This will support the wider vision of the Digital Single Market of the EU (28), protecting European society's interests and providing essential services to European citizens.

Cross-Sector Cybersecurity Standards:

ANSI/ISA, Series "ISA-62443: Security for Industrial Automation and Control System"

ISO 27001 Information Technology Security Techniques Information Security Management Systems Requirements

NIST Framework for Improving Critical Infrastructure Cybersecurity

ISO/IEC 27002:2013: Code of practice for information security controls

ISO 27003 - Information technology -- Security techniques -- Information security management system implementation guidance

ISO/IEC 27004:2016 Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation

ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements

ISO/IEC 27010:2015 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications

ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)

ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework

ISO/IEC 27013:2015 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security

ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity

ISO/IEC 27033-1:2015 Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts

ISO/IEC 27034-1:2011 Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts

ISO/IEC TR 19791:2010 Information technology -- Security techniques -- Security assessment of operational systems

European Telecommunications Standards Institute (ETSI) Cybersecurity Standards

TR 103 303 - TR 103 309 CYBER series

TR 103 331

TR 103 369

TS 103 487

IT Infrastructure Library (ITIL) v3

NIST SP 800-53

Information Assurance for SMEs (IASME)

ISF Standard of Good Practice for Information Security

ITU X series: Information security management framework

Cross-Sector Cybersecurity good practices:

The CIS Critical Security Controls

Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002,

Generally Accepted Information Security Principles (GAISP) – ISSA

The Open Group Open Information Security Management Maturity Model (O-ISM3)

ISACA BMIS

IT Baseline Protection Manual Standard Security Measures – BSI

UK Cyber Essentials (CREST)

Cyber Defence Capability Assessment Tool (CDCAT®) – CESG

HMG Security Policy Framework (SPF) – CESG

NIST/NSA/DISA/DoD Security Technical Implementation Guides (STIGs)

Carnegie Melon Capability Maturity Model (CMM)

The list of standards for assessing and managing cybersecurity risks is in Annex 1.

Energy sector

The NIS directive divides the energy sector into 3 subsectors:

Electricity subsector

Oil and gas subsector

Energy subsector

For the electricity subsector, the following security standards are recommended:

NIST SP 800-82 Rev. 2 (Guide to Industrial Control Systems (ICS) Security (29) provides guidelines on how to secure Industrial Control Systems (ICS). EU operators usually use this as a good practice;

ISO 27019 is a guideline for information management (30) based on ISO/IEC 27002 for process control systems specific to the energy utility industry;

NERC CIP (North American standard, focus on electric reliability and critical infrastructure

protection) (31) The standard is followed by EU operators who expand their business activity in the United States.

For the oil and gas subsector, the following security standards are recommended:

The most well-known security framework associated with the oil and gas sector is the Chemical Facility Anti-Terrorism Standards (CFATS) programme, the standard for chemical capacity security with the highest risk in the United States. However, CFATS does not consider cybersecurity but physical and operative security.

The most applicable cybersecurity standards in the energy industry are: ISO 27001, NIST Cyber Security Framework and ISA/IEC 62443.

Traffic (transport) sector

The transport (traffic) sector is divided into the following subsectors: air, rail, river and sea traffic, and road traffic.

a) Air traffic subsector:

Due to the increased spectre of threats, the cybersecurity and physical security of the transport sector can no longer be treated separately (32). The "Roadmap to Secure Control Systems in the Transportation Sector" stands out among the good practices for the transport sector. (33)

The most applicable cybersecurity standards are: ISO 27001, NIST Cyber Security Framework и ISA/IEC 62443. Other standards (that do not include cybersecurity): *ARINC 811* Commercial Aircraft Information Security Concepts of Operations and Process Framework

ICAO Aviation Security Manual - Document 8973 (Restricted Access) (34)

EUROCAE ED-201 – 204 Aeronautical Information System Security (AISS) Framework

RTCA DO-326 Airworthiness Security Process Specifications

Good practices that include cybersecurity:

AIAA (The American Institute of Aeronautics and Astronautics) The Connectivity Challenge: Protecting Critical Assets in a Networked World35

Information Security Certification and Accreditation (C&A) Handbook – FAA

FAA Issue Paper, Aircraft Electronic Systems Security Protection from Unauthorised External Access

FAA Aircraft systems information security protection overview

b) Rail traffic subsector:

Most of the security standards in the domain of rail transport refer mainly to the broader security aspects, not the cybersecurity challenges, that could ultimately influence the security of modern signalisation systems and train control. The applicable cybersecurity standards are ISO 27001 and ISA/IEC 62443.

The UK Rail Cyber Security Guidance to Industry should be emphasised as cybersecurity good practices in this subsector.

c) River and Sea traffic subsector:

The ICT systems supporting river and sea traffic, from port management to ship-to-ship/ship-to-shore communication, are generally very complex and use various ICT technologies. In this sector, there is no particular holistic consideration of cybersecurity. The applicable cybersecurity standards are ISO 27001 and ISA/IEC 62443.

Standards pertaining to security:

International Safety Management (ISM) Code (36)

IMO interim guidelines on maritime cyber risk management

International Ship and Port Facility Security (ISPS) Code

IEC 62351:2017 SER - Power systems management and associated information exchange - Data and communications security

IEC 61162 - Digital interfaces for navigational equipment within a ship

ISO 13613:2011 - Ships and marine technology -- Maintenance and testing to reduce losses in critical "systems for propulsion

Good practices that include cybersecurity:

BIMCO Guidelines on Cyber Security Onboard Ships - The Guidelines on Cyber security Onboard ships

DNVGL-RP-0496 (DNV-GL, 2016) Cyber security resilience management for ships and mobile offshore units in operation

Cyber-enabled ships: ShipRight procedure – autonomous ships

Cyber-enabled ships: Deploying information and communications technology in shipping – Lloyd's Register's approach to assurance

United States coast guard – Cyber Strategy Draft Guidelines on maritime cyber risk management

d) Road transport:

Several initiatives (37) led to defining the guidelines and regulations for implementing security in the automotive industry (38), and other initiatives sought cooperation in the automotive industry security topics (39). Even though some of them are ahead in *development*, such as ISO/AWI 21434 (40), the broadest security initiative is currently led by the TC22/SC3/WG16 committee within the development of ISO 262626 (41).

Road Transport Security Standards:

SAE J3061 Cybersecurity Guidebook for Cyber- Physical Vehicle Systems

SAE J3101 Requirements for Hardware- Protected Security for Ground Vehicle Applications (WiP)

ISO 15031 Road Vehicles - Communication between vehicle and external equipment for emissions-related diagnostics. Part 7: Data link security

ISO 15764 Road Vehicles - Extended data link security

ISO/AWI 21434 - Road Vehicles -- Automotive Security Engineering

ISO 26262-1:2011 - Road vehicles -- Functional safety

TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management

TS 103 096-1 to TS 103 096-3: Intelligent Transport Systems (ITS);

TR 103 061-6 Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 6: Validation report

Best practices:

ENISA Cyber Security and Resilience of smart cars – ENISA

Auto ISAC, Automotive Information Sharing and Analysis Center, Best Practices

Five Star Automotive Cyber Safety Framework

Guideline on cybersecurity and data protection of connected vehicles and vehicles with ADT – UNECE

Finance and banking sector

Finance and Banking Sector Security Standards:

ISO/TR 13569:2005

Gramm–Leach–Bliley Act

Sarbanes–Oxley Act

Payment services (PSD 2) - Directive (EU) 2015/2366

EBA on the security of internet payments (42)

ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services

American National Standards Institute *(ANSI) X9 series*

Cybersecurity good practices:

Payment Card Industry Data Security Standard (PCI DSS)

Basel II

Draft Guidelines on the security measures for operational and security risks of payment services under PSD2 43

CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure (44)

SEC OCIE Cybersecurity (45)

ISO/TR 13569:2005 Financial services — Instructions for information security (46) provide guidelines for developing the information security programme in the financial services industry. Implementation of the security controls is processed, as well as the elements necessary for managing the information security risk within the framework of the modern financial services institution.

Gramm–Leach–Bliley Act (GLB Modernization Act or GLBA) (47), also known as the Financial Modernization Act of 1999, is the federal law passed in the United States to control how financial institutions deal with the private information of individuals. It is required of the financial institutions, companies offering consumers financial products or services such as credits and financial or investment counselling, to be obliged to explain their company practices or information exchange to their clients and to protect sensitive data.

Sarbanes–Oxley Act from 2002 (SOX) (48) is the act adopted by the American Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations. The SOX Act ordered strict reforms to improve corporate financial disclosures and prevent accounting fraud.

Basel II, or International Convergence of Capital Measurement and Capital Standards, is a series of recommendations issued by the Basel Committee on Banking Supervision Basel II. The Basel Committee believes that risk assessments of banks' internal systems, as investments in capital budgets, are critical. (49)

Payment Services (PSD 2)- Directive (EU) 2015/2366 (50) tends to improve existing EU regulations for electronic payment. It takes into account emerging and innovative payment services, such as internet and mobile payments. It sets rules related to strict security conditions for electronic payment and the protection of consumer financial data, guaranteeing secure identity confirmation and reducing the risk of fraud; transparency of conditions and information requirements for payment services; rights and obligations of users and payment service providers

The Payment Card Industry Data Security Standard (PCI DSS) (51) represents the security standard of information for organisations handling branded credit cards. The PCI DSS standard is provided by card brands and managed by the Payment Card Industry Security Standards Council. The standard is created to increase data controls about the card owner to reduce credit card fraud.

Healthcare sector

ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002

Health Insurance Portability and Accountability Act (HIPPA)

ISO 13485:2003 Medical devices -- Quality management systems – Requirements for regulatory purposes

ISO 80001-1:2010 Application of risk management for IT networks incorporating medical devices

ETSI eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth (52)

Digital Imaging and Communications in Medicine (DICOM)

EC Medical Devices Regulation (text agreed by EP and Council – in adoption process)

NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Guide

Healthcare Cybersecurity Best Practices:

Royal Australian College of General Practitioners (RACGP) Computer Information Security Standards (CISS)

ISO 7799:2016 (53) provides guidelines for standards of organisation security information and practices for information management, including selection, implementation, and control management. It defines the guidelines for the support of interpretation and implementation of the healthcare information code of practice ISO/IEC 27002.

Health Insurance Portability and Accountability Act from 1996 (HIPAA) (54). The United States Department of Health and Human Services (HHS) developed regulations to protect the privacy and security of certain health information. With the rule called "*Security Standards for the Protection of Electronic Protected Health Information*", abbreviated to "Security Rule") (55), the national package of the security standards for the protection of certain health information that is saved or transferred in the electronic form was established. The security standard includes technical and non-technical protection measures that health organisations must implement to secure the "electronic protected health information" of individuals. (e-PHI) (56).

Water supply sector and drinking water distribution

Regarding drinking water operators, the most applicable cybersecurity standards for this sector are ISO- 27001 and ISA/IEC 62443

However, it is worth mentioning the standard ANSI/AWWA G430-09 "Security practice and waste management", published by the American Association for Water Supply, which aims to define minimal conditions for the water protection programme that will improve security protection of the employed, public health, public security, and public trust.

Digital service providers sector

According to the directive on security of Network and Information Systems (NIS) (57) (EU)2016/1148, Member States should adopt the common security requirements package for Operators of Essential Services (OES)58 and Digital Service Providers (DSP) (59).

- The EU strategic directives regarding the Digital Service Providers:
- NIS Working Group, security measures for OES60;
- ENISA report on the security measures for DSP[61]; and

- European Commission Act on implementation of measures for DSP (62).

The list of the Digital Service Providers security standards:

ISO/IEC 27011:2008 Information technology -- Security techniques -- Information security management guidelines for telecommunications organisations based on ISO/IEC 27002

List of good practices:

- *Technical guidance on the security measures for Telcos in Article 13a*, ENISA

*ISO/IEC 27011:2008 (***63)** refers to the security information management guidelines for telecommunication organisations, and is based on ISO/IEC 27001:2013.

CONCLUSIONS

The aim of all of the aforementioned standards is to ensure that the European Union (with the "Path to Digital Decade" programme) accomplishes its goals in the direction of the digital transformation of society and the economy in accordance with EU values, reinforcing digital management, and promoting the digital policy that strengthens citizens and companies. The ultimate goal of the NIS directive is to ensure network and information system security in all sectors (energy, transport, water and food, banking, financial market infrastructure, healthcare, and digital infrastructure) that are of vital social importance and the economies that depend on ICT. This paper provides insight into the standards aiming to increase protection against Internet threats in different sectors.

BIBLIOGRAPHY

1) Conclusions of the Council of Europe dated 25/3/2021

2) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final.

3) Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.

4) Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

5) Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final.

6) Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, OJ L 166, 11.5.2021, p. 1.

7) Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013, OJ L 170, 12.5.2021, p. 1.

8) Regulation (EU) 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programme and amending Regulation (EU) 2015/1017, OJ L 107, 26.3.2021, p. 30.

9) Communication on the EU Security Union Strategy. COM(2020) 605 final.

10) Communication on Digital Education Action Plan 2021-2027. COM/2020/624 final.

11) COM(2021) 750 final of 8.9.2021 – "2021 Strategic Foresight Report - The EU's capacity and freedom to act".

12) https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.

13) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade, COM/2021/118 final/2, 9. 3. 2021.

14) Berlin Declaration on Digital Society and Value-Based Digital Government.

15) https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP- EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

16) Ransomware was used for the attack on the healthcare sector, for example, in Romania (June 2020), Düsseldorf (September 2020), and Vastaamo (October 2020).

17) PwC, The Global State of Information Security 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.

18) Internet Society, The Global Internet Report: Consolidation in the Internet Economy; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global- internet-report-consolidation-in-the-internet-economy-explores-this-question/

19) https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

20) 2020 Digital Economy and Society Index; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020;
https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

21) Eurostat Press release, 'ICT security measures taken by vast majority of enterprises in the EU', 6/2020 - 13 January 2020. 'Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation'; WEF, The Global Risks Report 2020.

22) https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

23) https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm

24) https://www.un.org/en/sections/un-charter/un-charter-full-text/

25) As reflected in the relevant reports of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGEs), endorsed by the UNGA, notably the 2015, 2013 and 2010 reports.

26) https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the- future-of-cyber-discussions-at-the-un-10302020.pdf

27) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

28) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&-from=EN

29) https://csrc.nist.gov/csrc/media/publications/sp/800-82/rev-2/final/documents/sp800_82_r2_second_draft.pdf

30) https://www.iso.org/standard/43759.html

31) http://www.nerc.com/pa/Stand/Pages/CIP-Standards.aspx

32) https://www.enisa.europa.eu/publications/good-practices-recommendations

33) https://ics-cert.us-cert.gov/sites/default/files/documents/TransportationRoadmap20120831.pdf

34) http://www.icao.int/Security/SFP/Pages/SecurityManual.aspx

35) https://www.hklaw.com/publications/Coast-Guard-DHS-Mandate-Cybersecurity-Reporting-Move-to-Require-Maritime- Cybersecurity-Programs-07-20-2017/

36) http://www.imo.org/en/Publications/PublishingImages/PagesfromEB117E.pdf & http://www.imo.org/en/OurWork/humanelement/safetymanagement/pages/ismcode.aspx

37) https://www.automotiveisac.com/best-practices/

38)https://wiki.unece.org/download/attachments/40009763/%28ITS_AD-10-11- Rev1%29%20Revised%20draft%20of%20guideline%20on%20cybersecurity%20and%20data%20protection.pdf?api=v2

39) https://www.iamthecavalry.org/domains/automotive/5star/

40) https://www.iso.org/standard/70918.html

41) https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:en

42) http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

43) http://www.eba.europa.eu/documents/10180/1836621/Consultation+Paper+on+the+security+measures+for+operational+and+security+risks+of+payment+services+under+PSD2+%28EBA-CP-2017-04%29.pdf

44) http://www.bis.org/cpmi/publ/d146.pdf

45) https://www.sec.gov/spotlight/cybersecurity

46) https://www.iso.org/standard/37245.html

47) https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
48) http://www.ey.com/Publication/vwLUAssets/ey-the-sarbanes-oxley-act-at-15/$File/ey-the-sarbanes-oxley-act-at-15.pdf

49) https://www.enisa.europa.eu/topics/threat-risk-management/riskmanagement/current-risk/laws-regulation/corporate-governance/basel-ii

50) https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
51)https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

52) http://www.etsi.org/technologies-clusters/technologies/ehealth

53) https://www.iso.org/standard/62777.html

54) https://www.hhs.gov/hipaa/for-professionals/security/index.html?language=es 40
55) https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es 41

56) https://www.awwa.org/store/productdetail.aspx?productid=20779

57) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

58) ANNEX II NISD. The operators of the essential services are public and private entities stated in Annex II of the Directive that meet the criteria from Article 5(2).

59) ANNEX III Directives

60) http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

61) https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

62) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG

63) ISO/IEC 27011:2008 - Information security management guidelines for telecommunications organisations based on ISO/IEC 27002; URL: https://www.iso.org/standard/43751.html

REZIME

SAJBER INICIJATIVE EU I MEĐUNARODNI STANDARDI IZ OBLASTI SAJBER BEZBEDNOSTI – PREGLED

KLJUČNE REČI: INFORMACIONA BEZBEDNOST, SAJBER INICIJATIVE, MEDJUNARODNI STANDARDI BEZBEDNOSTI.

U radu je dat prikaz zakonskih direktiva, odluka, instrumenata i polisa kao nosioca strateškog razvoja digitalne tranzicije EU. Inicijative EU i međunarodni standardi iz oblasti sajber bezbednosti obuhvaćeni su kroz strateške inicijative EU i međunarodne standarde iz oblasti sajber bezbednosti. Posebno su istaknuti međusektorski standardi sajber bezbednosti i međusektorske dobre

prakse iz oblasti sajber bezbednosti. Date su preporuke bezbednosnih standarda iz oblasti energetike, saobraćaja, finansijskog i bankarskog sektora, zdravstvenog sektora, sektor snabdevanja vodom i distrubucija pitke vode i sektora pružalaca digitalnih usluga. Ovo ujedno predstavlja i krajnji cilj NIS Direktive koja podrazumeva da se osigura mrežna i informaciona bezbednost sistema u pomenutim sektorima.

* * *