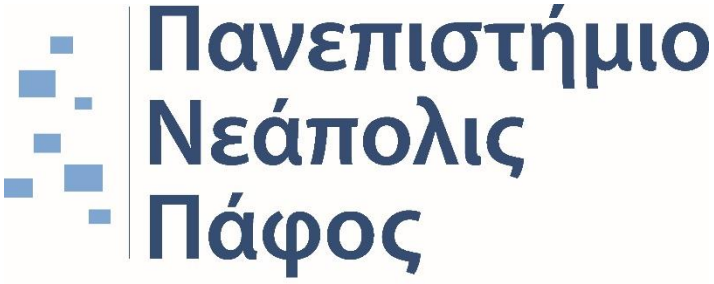
2024-05

þÿ ‘ Ã Æ ± » µ ¹ ¿ À ¿ ¯ · Ã · Ä ¿ Å º Å ² µ Á ½ ¿ þÿ Ã Ä ¿ À » ± ¯ Ã ¹ ¿ Ä · Â •• : µ Í Á ¿ Â þÿ À ¿ » ¹ Ä ¹ º Î ½ , ± À ¿ Ä µ » µ Ã ¼ ± Ä ¹ º Ì Ä þÿ ´ Å ½ ± Ä Ì Ä · Ä µ Â ² µ » Ä ¯ É Ã · Â

þÿ £ Ä ± Å Á ± º ¿ À ¿ Í » ¿ Å , ¦ É Ä µ ¹ ½ ®

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Á Ì ³ Á ± ¼ ¼ ± ” ¹ µ ¸ ½ Î ½ £ Ç - Ã µ É ½ , £ Ä Á ± Ä · ³ ¹ º ® Â º ± ¹ ‘ Ã Æ ¬ » µ ¹ ± Â
þÿ š ¿ ¹ ½ É ½ ¹ º Î ½ • À ¹ Ã Ä · ¼ Î ½ , ¤ µ Ç ½ Î ½ º ± ¹ ‘ ½ ¸ Á É À ¹ Ã Ä ¹ º Î ½ £ À ¿ Å ´ Î ½ , ± ½ µ À ¹ Ã Ä ®



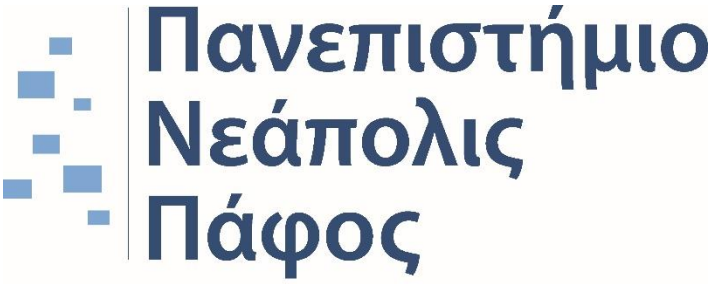
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ

ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της ΕΕ: εύρος πολιτικών, αποτελεσματικότητα, δυνατότητες βελτίωσης

ΦΩΤΕΙΝΗ ΣΤΑΥΡΑΚΟΠΟΥΛΟΥ

ΜΑΙΟΣ 2024



ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ

ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της ΕΕ: εύρος πολιτικών, αποτελεσματικότητα, δυνατότητες βελτίωσης

Διπλωματική Εργασία η οποία υποβλήθηκε προς απόκτηση Μεταπτυχιακού τίτλου σπουδών στις Διεθνείς Σχέσεις, Στρατηγική και Ασφάλεια στο Πανεπιστήμιο Νεάπολις Πάφος.

ΦΩΤΕΙΝΗ ΣΤΑΥΡΑΚΟΠΟΥΛΟΥ

ΜΑΙΟΣ 2024

Πνευματικά δικαιώματα

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: Φωτεινή Σταυρακοπούλου

Τίτλος Διπλωματικής Εργασίας: «Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της ΕΕ: εύρος πολιτικών, αποτελεσματικότητα, δυνατότητες βελτίωσης».

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολης και εγκρίθηκε στις 10 Ιουνίου 2024 από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος): Ιωάννης Γαλαριώτης

Μέλος Εξεταστικής Επιτροπής: Μάριος Ευθυμιόπουλος

Μέλος Εξεταστικής Επιτροπής: Μάριος Ευρυβιάδης

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Η Φωτεινή Σταυρακοπούλου, γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της ΕΕ: εύρος πολιτικών, αποτελεσματικότητα, δυνατότητες βελτίωσης», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Η Δηλούσα

Περιεχόμενα

Πίνακας Συντομογραφιών

CCPA	California Consumer Privacy Act
CER Directive	Critical Entities Resilience Directive
CERT	Computer Emergency Response Team
CIO	Chief information officer
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DoD	Department of Defense
DORA	Digital Operational Resilience Act
EDPS	European Data Protection Supervisor
ΕΕ	Ευρωπαϊκή Ένωση
ΕΚΤ	Ευρωπαϊκή Κεντρική Τράπεζα
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
IAEA	International Atomic Energy Agency
IAM	Identity and Access Management
IDS	Intrusion Detection System
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and. Communications Integration Center
NICP	National Institute of Crime Prevention
NIS Directive	Directive on security of network and information systems
OECD	Organisation for Economic Co-operation and Development
PSD2	Payment Services Directive 2
SOAR	Security Orchestration, Automation, and Response
UN	United Nations
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
IoT	Internet of Things
ΚΕΠΠΑ	Κοινή Εξωτερικής Πολιτική και Πολιτική Ασφάλειας
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών

ΠΕΡΙΛΗΨΗ

Η κυβερνοασφάλεια αποτελεί κρίσιμο παράγοντα στο σύγχρονο ψηφιακό περιβάλλον του κυβερνοχώρου, αφού αναφέρεται στην προστασία των δικτύων, των συστημάτων και των δεδομένων από κυβερνοαπειλές. Οι κυβερνοεπιθέσεις εξελίσσονται συνεχώς, και έτσι η κυβερνοασφάλεια απαιτεί σταθερή προσαρμογή και εξέλιξη. Στόχος της είναι η διασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εχεμύθειας των πληροφοριών, καθώς και η προστασία από επιπτώσεις όπως η διαρροή δεδομένων και οι διακοπές υπηρεσιών. Η κυβερνοασφάλεια αποτελεί προτεραιότητα, ειδικά σε τομείς όπως η υγεία και οι κρίσιμες υποδομές, όπου οι επιπτώσεις μπορούν να είναι σοβαρές. Η σχέση μεταξύ κυβερνοασφάλειας και ασφαλειοποίησης είναι στενή και συμπληρωματική, ενώ αφορά διαφορετικές πτυχές του κυβερνοχώρου. Η κυβερνοασφάλεια επικεντρώνεται στην προστασία των ψηφιακών συστημάτων, των δικτύων και των δεδομένων από κινδύνους όπως κυβερνοεπιθέσεις και κακόβουλο λογισμικό. Από την άλλη πλευρά, η ασφαλειοποίηση αφορά στην προστασία σε περίπτωση που συμβούν προβλήματα ασφάλειας ή κυβερνοεπιθέσεις και προσφέρει αντιμετώπιση των επιπτώσεων σε περίπτωση ανεπάρκειας των μέτρων ασφαλείας. Η Ευρωπαϊκή Ένωση έχει εφαρμόσει πολλές πρωτοβουλίες για την κυβερνοασφάλεια στο διαδίκτυο, λαμβάνοντας υπόψη την ανάγκη να προστατευθούν οι πολίτες, οι χώρες και οι επιχειρήσεις από κυβερνοεπιθέσεις και κυβερνοαπειλές. Ειδικότερα, η ΕΕ έχει εγκρίνει νομοθεσίες όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), που θέτει πρότυπα για την προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ. Επίσης έχει θέσει σε λειτουργία οργανισμούς όπως ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), που παρέχει εμπειρογνωμοσύνη και στήριξη στα κράτη μέλη για θέματα κυβερνοασφάλειας. Παράλληλα, η ΕΕ συνεργάζεται με διεθνείς εταίρους και οργανισμούς για την αντιμετώπιση κοινών κυβερνοασφαλειακών προκλήσεων. Αυτή η συνεργασία περιλαμβάνει την ανταλλαγή πληροφοριών και την κοινή ανάπτυξη καλύτερων πρακτικών. Η αντιμετώπιση των κυβερνοεπιθέσεων στα πλαίσια της ΕΕ διαμορφώνεται δυναμικά, καθώς η τεχνολογική εξέλιξη και οι απειλές στον κυβερνοχώρο συνεχώς εξελίσσονται. Η ΕΕ επιδιώκει να δημιουργήσει ένα ισχυρό κοινό πλαίσιο κυβερνοασφάλειας, να αναπτύξει νέες τεχνολογίες και μεθόδους , καθώς και να ενισχύσει τη συνεργασία μεταξύ των κρατών μελών, των δημόσιων αρχών και των ιδιωτικών εταιρειών για την αντιμετώπιση των διαφόρων προκλήσεων-απειλών και την επίτευξη της ασφαλειοποίησης του κυβερνοχώρου.

Λέξεις κλειδιά: κυβερνοχώρος, ασφαλειοποίηση, κυβερνοασφάλεια, ΕΕ

ABSTRACT

Cybersecurity is essential in today's digital landscape of cyberspace as it involves safeguarding networks, systems, and data from cyber threats. With the continuous evolution of cyberattacks, cybersecurity must also constantly adapt and evolve. Its primary goal is to ensure the integrity, availability, and confidentiality of information while preventing issues such as data breaches and service disruptions. Cybersecurity is particularly crucial in sectors like healthcare and critical infrastructure, where the consequences can be severe. The relationship between cybersecurity and securitization is close and complementary, while addressing different aspects of cyberspace. Cybersecurity focuses on protecting digital systems, networks and data from risks such as cyber-attacks and malware. On the other hand, securitization is about protection in case of security problems or cyber-attacks and offers to deal with the consequences in case of inadequacy of security measures. The European Union has launched numerous initiatives to enhance cybersecurity on the internet, recognizing the need to shield citizens, countries and businesses from cyber-attacks and threats. Notably, the EU has enacted legislation such as the General Data Protection Regulation (GDPR), which establishes standards for protecting the personal data of EU citizens. Additionally, the EU has created entities like the European Union Agency for Cybersecurity (ENISA), which offers expertise and support to member states on cybersecurity matters. At the same time, the EU works with international partners and organizations to address common cybersecurity challenges. This cooperation includes the sharing of information and the joint development of best practices. The EU's approach to responding to cyberattacks is continually evolving in response to ongoing technological advancements and emerging threats in cyberspace. The EU aims to create a strong common cybersecurity framework, develop new technologies and methods, as well as strengthen cooperation between member states, public authorities and private companies to address the various challenges-threats and achieve the securitization of cyberspace.

Keywords: cyberspace, securitization, cybersecurity, EU