2022-01

þÿ Á ¿ ² » ® ¼ ± Ä ± ‘ ¾ ¹ ¿ À ¹ Ã Ä ¯ ± Â ” ¹ º Ä

þÿ º ± ¹ Á ¿ Ã Ä ± Ã ¯ ± » · Á ¿ Æ ¿ Á ¹ Î ½

þÿ § ± Á ± » ¬ ¼ À ¿ Å Â , “ ¹ ± ½ ½ ¬ º · Â

þÿ œ µ Ä ± À Ä Å Ç ¹ º Ì À Á Ì ³ Á ± ¼ ¼ ± Ã Ä ± » · Á ¿ Æ ¿ Á ¹ ± º ¬ £ Å Ã Ä ® ¼ ± Ä ± º ± ¹ Ä · ½ ¨ · Æ ¹ ± º
þÿ £ Ç ¿ » ® ” ¹ ¿ ¯ º · Ã · Â º ± ¹ • À ¹ Ã Ä ® ¼ · Â ¥ À ¿ » ¿ ³ ¹ Ã Ä Î ½ , ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â

Τμήμα: **Πληροφοριακά Συστήματα**
και **Ψηφιακή Καινοτομία.**

«Προβλήματα Αξιοπιστίας Δικτύων και Προστασία Πληροφοριών»

ΧΑΡΑΛΑΜΠΟΥΣ ΓΙΑΝΝΑΚΗΣ

ΙΑΝΟΥΑΡΙΟΣ 2022

Τμήμα: Πληροφοριακά Συστήματα και Ψηφιακή Καινοτομία.

«Προβλήματα Αξιοπιστίας Δικτύων και Προστασία Πληροφοριών»

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά Συστήματα και την Ψηφιακή Καινοτομία στο Πανεπιστήμιο Νεάπολις

ΧΑΡΑΛΑΜΠΟΥΣ ΓΙΑΝΝΑΚΗΣ

ΙΑΝΟΥΑΡΙΟΣ 2022

Πνευματικά δικαιώματα

Δηλώνω υπευθύνως ότι όλα τα στοιχεία σε αυτήν την εργασία τα απέκτησα, τα επεξεργάσθηκα και τα παρουσιάζω σύμφωνα με τους κανόνες και τις αρχές της ακαδημαϊκής δεοντολογίας, καθώς και τους νόμους που διέπουν την έρευνα και την πνευματική ιδιοκτησία. Δηλώνω επίσης υπευθύνως ότι, όπως απαιτείται από αυτούς τους κανόνες, αναφέρομαι και παραπέμπω στις πηγές όλων των στοιχείων που χρησιμοποιώ και τα οποία δεν συνιστούν πρωτότυπη δημιουργία μου.

Η έγκριση της διατριβής από το Πανεπιστημίου Νεάπολις δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Πανεπιστημίου.

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: ΓΙΑΝΝΑΚΗΣ ΧΑΡΑΛΑΜΠΟΥΣ

Τίτλος Μεταπτυχιακής Διατριβής: Προβλήματα Αξιοπιστίας Δικτύων και Προστασία Πληροφοριών

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις ……01/02/2022…… [ημερομηνία έγκρισης] από τα μέλη της Εξεταστικής Επιτροπής.

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)…Ζαχαριουδάκης Ελευθέριος Λέκτορας…… [ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: Κακουλλή Έλενα

Λέκτορας……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: Χριστοδούλου Παναγιώτης

Λέκτορας……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

2 Πίνακας Περιεχομένων

Πίνακας Εικόνων

Γλωσσάρι

H/Y	Ηλεκτρονικός / Υπολογιστής
ARPA	Advanced Research Projects Agency
DoD	Department of Defense
ACM	Association for Computing Machinery
IMP	Interface Message Processor
UCLA	University of California at Los Angeles
UCSB	University of California at Santa Barbara
SRI	Stanford Research Institute
NCP	Network Control Protocol
TCP	Transmission Control Protocol
IP	Internetworking Protocol
VoIP	Voice over Internet Protocol
PSTN	Public Switched Telephone Network
P2P	Peer to Peer
LAN	Local Area Network
WAN	Wide Area Network
MAN	Metropolitan Area Network
SAN	Storage Area Network
PAN	Personal Area Network
WLAN	Wireless Local Area Network
CAN	Campus Area Network
VPN	Virtual Private Network
PON	Passive Optical Network
IT	Information Technology
OT	Operational Technology
ΤΠΕ	Τμήμα Πληροφοριών – Επικοινωνίας
WPA	Wi-Fi Protect Access
RACI	Responsible- Accountable-Consulted-Informed

SLA	Service Level Agreement
HIDS	Host Intrusion Detection System
WAF	Web Application Firewall
AV	Application Visibility
ETDR	Endpoint Threat Detection Response

Περίληψη

Στις μέρες μας είναι αρκετά ορατό όχι μόνο στους επαγγελματίες της Πληροφορικής και ειδικά στους υπεύθυνους ασφάλειας αλλά και σε τρίτους ότι κρίσιμες κρατικές, αμυντικές υποδομές στις προηγμένες δυτικές κοινωνίες δεν μπορούν να λειτουργήσουν χωρίς τις τεχνολογίες των πληροφοριών και των δικτύων. Οι ασφάλειες αυτών των υποδομών επηρεάζουν τη λειτουργία επιχειρήσεων κοινής ωφέλειας, την οικονομική ζωή του τόπου, τη δημόσια διοίκηση, τον αμυντικό τομέα ή ακόμα και την παραμικρή λεπτομέρεια της καθημερινότητας.

Συνεπώς τα δίκτυα τους και η ασφάλεια αυτών έχουν ζωτική σημασία. Ο λόγος είναι πολύ απλός: αν αυτά τα συστήματα δεν λειτουργούν, τότε δεν λειτουργεί ούτε η κοινωνία. Η σημασία της ασφάλειας του κυβερνοχώρου τους δεν μπορεί να αμφισβητηθεί. Αντίστοιχα, οι προκλήσεις και οι απειλές για τον κυβερνοχώρο πρέπει να αντιμετωπιστούν σε στρατηγικό επίπεδο ξεκινώντας από τη θωράκιση της πολιτικής της ασφάλειας των δικτύων των παραπάνω οργανισμών.

Σκοπός της παρούσας διπλωματικής είναι να προτείνει το πλαίσιο σχεδιασμού και υλοποίησης μία πολιτικής δικτυακής ασφάλειας που περνάει από την τεκμηρίωση, στο σχεδιασμό και την εκτέλεση, καθώς και το συνεχή έλεγχο για τη βελτιστοποίηση της. Θεωρεί ότι ο οργανισμός χρησιμοποιεί πολλαπλούς τομείς δικτύων (IT, Cloud, IoT) και προτείνει μία μεθοδολογία προσέγγισης του προβλήματος.

Η παρούσα πτυχιακή μελετά αρχικά ευπάθειες και αδυναμίες και αντλεί μαθήματα από προβλήματα που προκάλεσαν κυβερνοεπιθέσεις στο παρελθόν όσον αφορά την αξιοπιστία, ακεραιότητα, πρόσβαση, ταυτοποίηση σε υπολογιστικά συστήματα. Με βάση αυτά τα μαθήματα η εργασία καθοδηγεί ένα πλαίσιο δημιουργίας κανόνων ασφάλειας ανεξαρτήτως των τεχνολογιών και πεδίων εφαρμογής που θα αποτρέπουν την μελλοντική εμφάνιση τέτοιων συμβάντων. Αυτό θα βοηθήσει στην εύρεση κατάλληλης διαδικασίας με την οποία θα μοντελοποιήσουμε μια πολιτική η οποία θα μπορεί να εφαρμοστεί σε δίκτυα Υψηλής ασφάλειας λόγο της φύσεως των οργανισμών (κρατικές υπηρεσίες, οργανισμοί ασφάλειας ,χρηματοοικονομικοί οργανισμοί κ.α).

Abstract

Nowadays it is quite visible not only to IT professionals and especially to security officials but also to third parties that critical state, defense infrastructure in advanced western societies cannot function without the presence of information and network technologies. The security of these infrastructures affects the operation of utilities, the economic life of the place, the public administration, the defense sector or even the smallest detail of everyday life.

Therefore their networks and their security are vital. The reason is very simple: if these systems do not work, then neither does society. The importance of their cyber security cannot be questioned. Accordingly, the challenges and threats to cyberspace must be addressed at a strategic level starting from the shielding of the security policy of the networks of the above organizations.

The purpose of this dissertation is to propose the framework for the design and implementation of a cybersecurity policy that goes through documentation, design and execution, as well as continuous monitoring to optimize it. Considers that the organization uses multiple network domains (IT, Cloud, IoT) and proposes a methodology to approach the problem.

This dissertation initially studies vulnerabilities and threats and draws lessons from problems that have caused cyber-attacks in the past in terms of reliability, integrity, accessibility, authentication in network systems. Based on these lessons, this work guides a framework for creating policy rules regardless of the technologies and areas of application that will prevent such incidents from occurring in the future. This will help to find a suitable process by which we will model a policy that can be implemented in networks of strict security measures due to the nature of such organizations (government agencies, security agencies, financial institutions, etc.).