# Απειλές κυβερνοασφάλειας έναντι ανθρώπινης ζωής

## Η ανθρώπινη ασφάλεια στην ψηφιακή εποχή

Δημόπουλος Μιχαήλ Κωνσταντίνος
Νετκίδης Ευθύμιος

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

# Εισαγωγή

Καθώς οι ψηφιακές τεχνολογίες συνεχίζουν να προοδεύουν, η ενσωμάτωση των μέτρων κυβερνοασφάλειας στα συστήματα δημόσιας ασφάλειας είναι πρωταρχικής σημασίας.

Αυτή η παρουσίαση στοχεύει να διερευνήσει τον ζωτικό ρόλο που διαδραματίζει η κυβερνοασφάλεια στη διαφύλαξη των κοινοτήτων μας,

# Κυβερνοασφάλεια

- **Εμπιστευτικότητα** - Διασφάλιση ότι οι ευαίσθητες πληροφορίες είναι προσβάσιμες μόνο σε εξουσιοδοτημένα άτομα και συστήματα
- **Ακεραιότητα** - Προστασία δεδομένων από κακόβουλη αλλοίωση ή παραποίηση από τρίτους
- **Διαθεσιμότητα** - Διασφάλιση ότι οι πληροφορίες και τα συστήματα είναι προσβάσιμα όταν χρειάζονται.
- **Αυθεντικοποίηση** - Επαλήθευση της ταυτότητας των χρηστών και των συσκευών πριν από την παραχώρηση πρόσβασης.
- **Μη-αποκήρυξη** - Εξασφάλιση πως οι ενέργειες ή οι συναλλαγές δεν μπορούν να αποκυρηχθούν post factum.

# Τομείς ενδιαφέροντος

**Διαδίκτυο των Πραγμάτων**

- Παγκόσμιο δίκτυο έξυπνων συσκευών, που συλλέγουν και ανταλάζουν πληροφορίες
- Περιλαμβάνουν αισθητήρες και ενεργοποιητές, που επιτρέπουν διευκόλυνση και αυτοματισμούς, αλλά ευρύνουν το φάσμα επιθέσεων
- Υπολογιστικά περιορισμένες συσκευές, που δυσκολεύουν την υλοποίηση μέτρων ασφαλείας

# Τομείς ενδιαφέροντος

**Συστήματα υγείας**

- Πληροφοριακά μηχανήματα των οποίων η διαθεσιμότητα είναι ύψιστης σημασίας, καθώς κρατάνε ανθρώπους σε ζωή
- Προσωπικά δεδομένα υγείας ασθενών που μπορεί να διερρεύσουν και να κλαπούν

**Συστήματα μεταφοράς**

- Έλεγχος της κυκλοφορίας και των δικτύων δημόσιας συγκοινωνίας
- Ευαίσθητα σε κυβερνοεπιθέσεις που μπορούν να διαταράξουν τις υπηρεσίες, να προκαλέσουν ατυχήματα και να οδηγήσουν σε σημαντικούς κινδύνους επιβατών και πεζών

# Τομείς ενδιαφέροντος

**Κρίσιμες υποδομές**

- Εργοστάσια παραγωγής ενέργειας στην οποία βασίζονται κοινότητες και οικισμοί
- Συστήματα μεταφοράς πόσιμου νερού, φράγματα, κινητές γέφυρες κλπ.

**Υπηρεσίες πληροφοριών**

- Οι υπηρεσίες πληροφοριών αποτελούν πρωταρχικούς στόχους για κυβερνοεπιθέσεις με στόχο την κλοπή απόρρητων πληροφοριών, που διακυνδυνεύουν την εθνική ασφάλεια.

# Γνωστά περιστατικά

**Ukraine power grid hack (2015)**

- Επίθεση που στόχεψε εταιρείες διανομής ηλεκτρικής ενέργειας στην Ουκρανία
- Αφήσε εκατοντάδες χιλιάδες χωρίς ρεύμα κατά τη διάρκεια του χειμώνα

**Stuxnet Worm (2010)**

- Malware που σχεδιάστηκε για να σαμποτάρει το πυρηνικό πρόγραμμα του Ιράν, στοχεύοντας συγκεκριμένα τις φυγόκεντρες που χρησιμοποιούνται για τον εμπλουτισμό ουρανίου.
- θα μπορούσε να είχε καταρρακτώδεις επιπτώσεις στη δημόσια υγεία και ασφάλεια

# Γνωστά περιστατικά

- **WannaCry Ransomware (2017):** Στόχεψε νοσοκομεία και εγκαταστάσεις υγειονομικής περίθαλψης σε όλο τον κόσμο, διακόπτοντας τη φροντίδα των ασθενών

- **Colonial Pipeline Attack (2021):** Επίθεση σε μεγάλο αγωγό καυσίμων στις ΗΠΑ που οδήγησε σε ελλείψεις καυσίμων και σημαντικές διακοπές στις αλυσίδες εφοδιασμού καυσίμων

- **SolarWinds Supply Chain Attack (2020):** Στοχεύτηκε σε κρατικούς και ιδιωτικούς οργανισμούς πληροφοριών, με στόχο τη κατασκοπεία και τη κλοπή δεδομένων

# Μέτρα ασφαλείας

- **Εμπιστευτικότητα –** χρήση ισχυρών αλγορίθμων κρυπτογράφησης (όπως AES)
- **Ακεραιότητα** – χρήση αλγορίθμων hash, ψηφιακές υπογραφές, πλεονασμός/backups
- **Αυθεντικοποίηση** – εφαρμογή κανόνων ελάχιστων δικαιωμάτων, βιομετρικά στοιχεία, MFA
- **Μη-αποκύρηξη** – logs, ψηφιακές υπογραφές, ασύμετρη κρυπτογράφηση
- **Διαθεσιμότητα** – αποκεντρωμένα, self-healing δίκτυα και διακομιστές

# Μέτρα ασφαλείας

**Φυσικές ασφάλειες**

- Σε περίπτωση που το λογισμικό έχει καταληφθεί, είναι καλό να υπάρχουν υλικά μέτρα ασφαλείας

  π.χ Therac-25

# Συμπεράσματα

Η κυβερνοασφάλεια διαδραματίζει κρίσιμο ρόλο στη διαφύλαξη της ανθρώπινης ζωής και της ευημερίας σε έναν όλο και πιο ψηφιακό κόσμο.

Δίνοντας προτεραιότητα σε ισχυρά μέτρα κυβερνοασφάλειας, μπορούμε να μετριάσουμε τους κινδύνους των απειλών στον κυβερνοχώρο σε βασικά συστήματα και υποδομές, διασφαλίζοντας την ασφάλεια και την ασφάλεια ατόμων και κοινοτήτων.

# Πηγές και βιβλιογραφεία

C. Johnson, R. Harkness, and M. Evangelopoulou, “Forensic Attacks Analysis and the Cyber Security of Safety-Critical Industrial Control Systems,” Journal of System Safety, vol. 53, no. 1, pp. 29–34, Apr. 2017, doi: https://doi.org/10.56094/jss.v53i1.102.

N. A. A. Bakar, W. M. W. Ramli, and N. H. Hassan, “The internet of things in healthcare: an overview, challenges and model plan for security risks management process,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 15, no. 1, p. 414, Jul. 2019.

P. Mueller and B. Yadegari, “The Stuxnet Worm,” 2012. Available: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic9-final/report.pdf

“Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” 2016. Available: http://www.sherpain.net/SW_upload_file/SW_qna/a615bde86d160330091226.pdf

# Τέλος

Ευχαριστούμε για τον χρόνο σας!

Μη διστάσετε να κάνετε ερωτήσεις.