

Τεχνητή Νοημοσύνη & Κυβερνοασφάλεια Απειλές και οφέλη για την Δημόσια Διοίκηση και τοπική Αυτοδιοίκηση”

Αθανάσιος ΚΟΣΜΟΠΟΥΛΟΣ LLB, LLM, PhDc
Cert. DPO ISO/IEC 17024 - Cert. IA ISO 27001:2022
Υπεύθυνος Προστασίας Δεδομένων
Υπουργείο Ψηφιακής Διακυβέρνησης



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης



Αξιοποίηση της ΤΝ στην Αυτοδιοίκηση

Αξιοποίηση νέων τεχνολογιών με έμφαση στην ΤΝ.
Να τις ενσωματώσουμε γρήγορα και αποτελεσματικά στις διαδικασίες των Δήμων μας:

- για τον πολίτη και πιο συγκεκριμένα την βελτίωση των υπηρεσιών
- για τους υπαλλήλους/υπηρεσίες για ένα πιο παραγωγικό αποτέλεσμα και διευκόλυνση της εργασίας τους



Που εφαρμόζεται η TN στην Αυτοδιοίκηση

- Εξυπηρέτηση πολιτών
- Διαχείριση υποδομών
- Ανάλυση δεδομένων
- Συμμετοχή πολιτών
- Αντιμετώπιση κρίσεων



Βελτίωση εξυπηρέτησης πολιτών

- Ψηφιακοί βοηθοί (chatbots)
- Αυτόματη έκδοση πιστοποιητικών
- Προσωποποιημένες ενημερώσεις
- Μείωση γραφειοκρατίας



Έξυπνες Πόλεις (Smart Cities)

- Έξυπνη στάθμευση & κυκλοφορία
- Αισθητήρες για καθαριότητα και φωτισμό
- Ενεργειακή διαχείριση κτιρίων
- Περιβάλλον



Διαφάνεια και συμμετοχή πολιτών

- Ανάλυση κοινωνικών αναγκών
- Ψηφιακές πλατφόρμες
διαβούλευσης
- Ενίσχυση εμπιστοσύνης στη
διοίκηση



Λήψη αποφάσεων βάσει δεδομένων

- Προγνωστικά μοντέλα για πυρκαγιές, πλημμύρες, κυκλοφοριακή συμφόρηση
- Χαρτογράφηση αναγκών & ευκαιριών



Ψηφιακός Μετασχηματισμός

Αποτελεσματικότητα και Διαφάνεια

- **Βελτίωση Δημόσιων Υπηρεσιών**
Αυτοματοποίηση και αποδοτικότητα
- **Υψηλή Προσβασιμότητα**
Διαφάνεια μέσω ηλεκτρονικών πλατφορμών



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης



Αυτοματοποίηση Διαδικασιών

Αποτελεσματικότητα και Ακρίβεια

Η αυτοματοποίηση διαδικασιών μέσω νέων τεχνολογιών εξοικονομεί χρόνο και πόρους, βελτιώνοντας την ακρίβεια και την αποδοτικότητα στη Δημόσια Διοίκηση.



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης



Διαφάνεια και Εμπιστοσύνη

Ενίσχυση της Διαφάνειας και Εμπιστοσύνης



Διαφάνεια στην Πληροφόρηση

Δημιουργία ανοικτών
πηγών πληροφοριών για
όλους.



Εμπιστοσύνη μέσω Ψηφιακής Αλληλεπίδρασης

Ενίσχυση της συμμετοχής
πολιτών με ψηφιακά μέσα.



Αυτονομία από Προμηθευτές

Ανάπτυξη εσωτερικών
λύσεων χωρίς εξωτερική
εξάρτηση.



Ασφάλεια Δεδομένων

Διασφάλιση της
προστασίας προσωπικών
και ευαίσθητων
πληροφοριών.



Κυβερνοασφάλεια Προκλήσεις

Ασφάλεια στον Δημόσιο Τομέα: Από τις Απειλές στην Εμπιστοσύνη



Το Πρόβλημα

Οι δημόσιες υπηρεσίες είναι ευάλωτες σε κυβερνοεπιθέσεις που απειλούν την ασφάλεια τους.



Η Λύση

Επενδύσεις σε τεχνολογίες ασφάλειας και εκπαίδευση προσωπικού ενισχύουν την κυβερνοασφάλεια.



Το Αποτέλεσμα

Ενισχυμένη προστασία και διατήρηση της εμπιστοσύνης των πολιτών μέσω αποτελεσματικών λύσεων.



Διαχείριση Ιδιωτικότητας

Προστασία Δεδομένων

Η διαχείριση ιδιωτικότητας είναι κρίσιμη για τη διασφάλιση της προστασίας των προσωπικών δεδομένων στην εποχή των νέων τεχνολογιών.



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης



Ψηφιακός Αποκλεισμός

Εκπαίδευση για την καταπολέμηση του ψηφιακού αποκλεισμού



Προγράμματα εκπαίδευσης

Εκπαίδευση πολιτών για
την ψηφιακή πρόσβαση.



Δημιουργία κοινών πόρων

Ανάπτυξη ψηφιακών
εργαλείων για όλους.



Αύξηση ευαισθητοποίησης

Ενημέρωση σχετικά με τις
τεχνολογικές ευκαιρίες.



Συνεργασία δημόσιου και ιδιωτικού τομέα

Στρατηγικές συνεργασίας
για την πρόσβαση σε
τεχνολογίες.



Ανασφάλεια Προσωπικού

Στήριξη και Επανακατάρτιση
Προσωπικού

- **Προγράμματα
Επανακατάρτισης**
Ενίσχυση δεξιοτήτων προσωπικού
- **Στήριξη Προσωπικού**
Προσαρμογή στις νέες τεχνολογίες



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης





Επίγειες Κρίσιμες Υποδομές: Επισκόπηση

Ενεργειακές Εγκαταστάσεις

Περιλαμβάνουν δίκτυα ηλεκτρικής ενέργειας, σταθμούς παραγωγής και συστήματα διανομής που είναι ζωτικής σημασίας για τη λειτουργία της κοινωνίας.

Δίκτυα Ύδρευσης

Συστήματα επεξεργασίας και διανομής νερού που εξυπηρετούν βασικές ανθρώπινες ανάγκες και βιομηχανικές διαδικασίες.

Τηλεπικοινωνίες

Υποδομές που υποστηρίζουν την επικοινωνία μεταξύ ατόμων, επιχειρήσεων και κυβερνήσεων, συμπεριλαμβανομένων των δικτύων κινητής τηλεφωνίας και διαδικτύου.

Μεταφορές

Αεροδρόμια, σιδηροδρομικά δίκτυα, αυτοκινητόδρομοι και συστήματα διαχείρισης κυκλοφορίας που διευκολύνουν τη μετακίνηση ανθρώπων και αγαθών.



Three core competing regulatory models



Μέθοδοι Κυβερνοεπιθέσεων: Malware και Ransomware



Κρυπτογράφηση Δεδομένων

Το ransomware κρυπτογραφεί κρίσιμα δεδομένα και απαιτεί λύτρα για την αποκατάσταση της πρόσβασης. Στις κρίσιμες υποδομές, αυτό μπορεί να παραλύσει ολόκληρα συστήματα και να διακόψει ζωτικές υπηρεσίες.



Κακόβουλο Λογισμικό

Εξειδικευμένο malware μπορεί να σχεδιαστεί για να στοχεύσει συγκεκριμένα βιομηχανικά συστήματα ελέγχου, όπως το Stuxnet που χρησιμοποιήθηκε εναντίον πυρηνικών εγκαταστάσεων του Ιράν.



Μακροχρόνια Παρουσία

Προηγμένο malware μπορεί να παραμείνει αδρανές για μεγάλα χρονικά διαστήματα, συλλέγοντας πληροφορίες και περιμένοντας την κατάλληλη στιγμή για να ενεργοποιηθεί και να προκαλέσει ζημιά.

Μέθοδοι Κυβερνοεπιθέσεων: DDoS Επιθέσεις



Οι επιθέσεις **Distributed Denial of Service (DDoS)** χρησιμοποιούν χιλιάδες μολυσμένους υπολογιστές (**botnet**) για να κατακλύσουν τους στοχευμένους διακομιστές με τεράστιο όγκο ψεύτικης κίνησης. Αυτό μπορεί να καταστήσει τις υπηρεσίες αδύνατο να προσπελαστούν από νόμιμους χρήστες.

Στην περίπτωση κρίσιμων υποδομών, μια επίθεση DDoS μπορεί να εμποδίσει την πρόσβαση σε συστήματα ελέγχου ή να αποτελέσει αντιπερισπασμό για πιο στοχευμένες επιθέσεις που συμβαίνουν ταυτόχρονα.



Μέθοδοι Κυβερνοεπιθέσεων: Phishing και Social Engineering

Στοχευμένα Μηνύματα

Οι επιτιθέμενοι δημιουργούν πειστικά μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνονται να προέρχονται από αξιόπιστες πηγές, όπως συναδέλφους ή προμηθευτές.

Ψεύτικοι Ιστότοποι

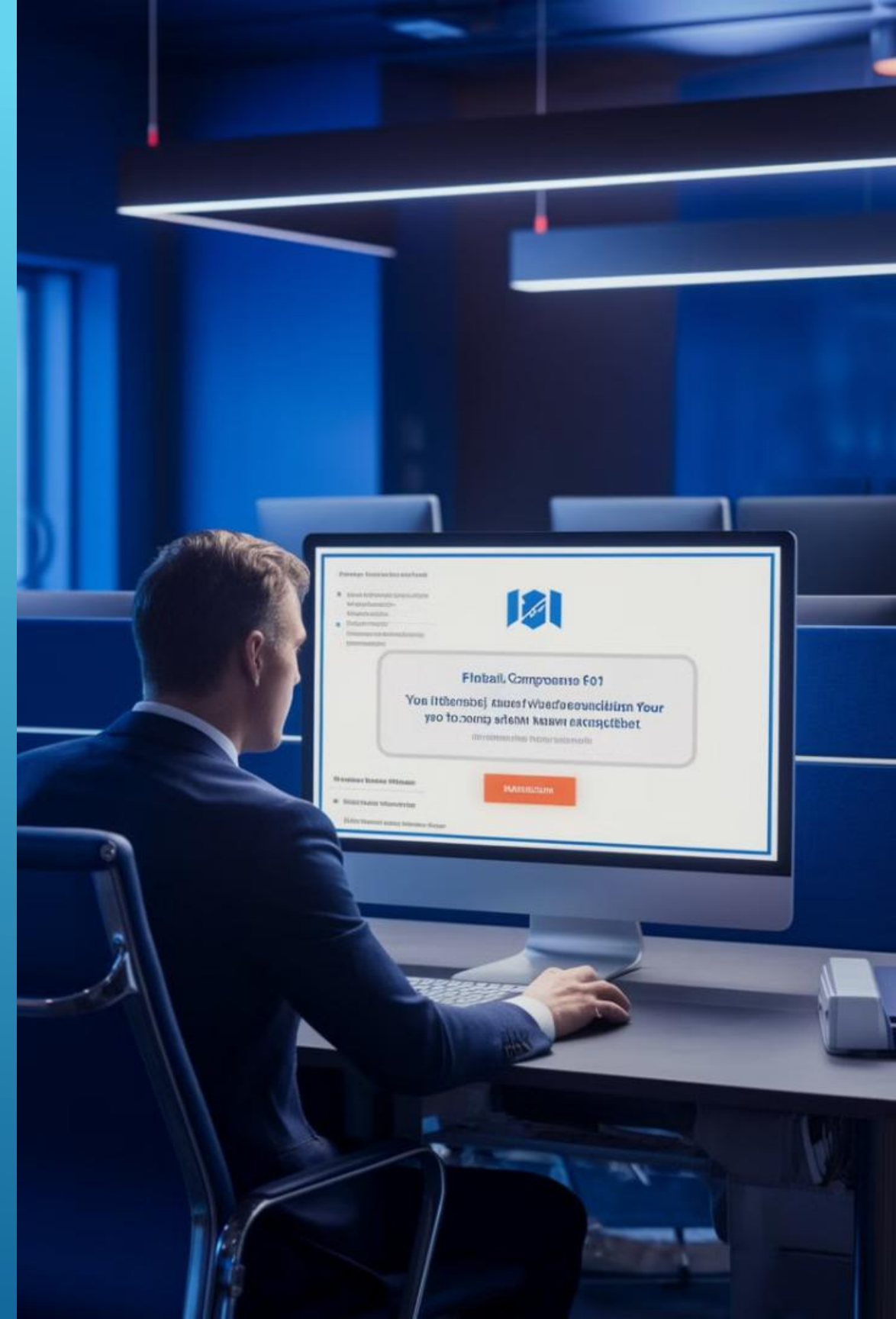
Τα θύματα οδηγούνται σε ψεύτικους ιστότοπους που μιμούνται νόμιμες πλατφόρμες, όπου τους ζητείται να εισάγουν τα διαπιστευτήριά τους.

Συλλογή Διαπιστευτηρίων

Μόλις αποκτηθούν τα διαπιστευτήρια, οι επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση σε κρίσιμα συστήματα και να εκτελέσουν κακόβουλες ενέργειες.

Εσωτερική Πρόσβαση

Με νόμιμη πρόσβαση, οι επιτιθέμενοι μπορούν να κινηθούν οριζόντια στο δίκτυο, στοχεύοντας ακόμα πιο κρίσιμα συστήματα και υποδομές.



Μέθοδοι Κυβερνοεπιθέσεων: Advanced Persistent Threats (APT)



Οι Advanced Persistent Threats είναι μακροχρόνιες και στοχευμένες επιθέσεις που συνήθως διεξάγονται από κράτη ή οργανωμένες ομάδες με σημαντικούς πόρους. Στοχεύουν κρίσιμες υποδομές για κατασκοπεία, σαμποτάζ ή προετοιμασία για μελλοντικές συγκρούσεις.

Μέτρα Προστασίας: Τεχνολογικές Λύσεις

Ισχυρή Κρυπτογράφηση

Η χρήση προηγμένων αλγορίθμων κρυπτογράφησης για την προστασία ευαίσθητων δεδομένων και επικοινωνιών είναι απαραίτητη για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Firewalls και IDS/IPS

Τα συστήματα τείχους προστασίας και τα συστήματα ανίχνευσης/πρόληψης εισβολών παρακολουθούν και φιλτράρουν την κίνηση δικτύου, εντοπίζοντας και αποκλείοντας ύποπτες δραστηριότητες.

Έλεγχος Πρόσβασης

Η εφαρμογή αυστηρών πολιτικών ελέγχου πρόσβασης με βάση την αρχή των ελάχιστων προνομιών περιορίζει τις πιθανές ζημιές από παραβιασμένους λογαριασμούς.

Τακτικές Ενημερώσεις

Η διατήρηση όλων των συστημάτων και λογισμικού ενημερωμένων με τις τελευταίες διορθώσεις ασφαλείας κλείνει γνωστά τρωτά σημεία που θα μπορούσαν να εκμεταλλευτούν οι επιτιθέμενοι.



Μέτρα Προστασίας: Ανθρώπινος Παράγοντας

1

Εκπαίδευση Προσωπικού

Η συνεχής εκπαίδευση των εργαζομένων σχετικά με τις απειλές κυβερνοασφάλειας, όπως το phishing και το social engineering, είναι κρίσιμη για την αποφυγή ανθρώπινων λαθών που μπορούν να οδηγήσουν σε παραβιάσεις.

2

Προσομοιώσεις Επιθέσεων

Οι τακτικές ασκήσεις προσομοίωσης επιθέσεων βοηθούν στον εντοπισμό αδυναμιών και στην προετοιμασία του προσωπικού για την αντιμετώπιση πραγματικών περιστατικών.

3

Διαδικασίες Αντιμετώπισης Περιστατικών

Η ανάπτυξη και δοκιμή σαφών πρωτοκόλλων αντιμετώπισης περιστατικών ασφαλείας διασφαλίζει γρήγορη και αποτελεσματική ανταπόκριση σε περίπτωση παραβίασης.

4

Κουλτούρα Ασφάλειας

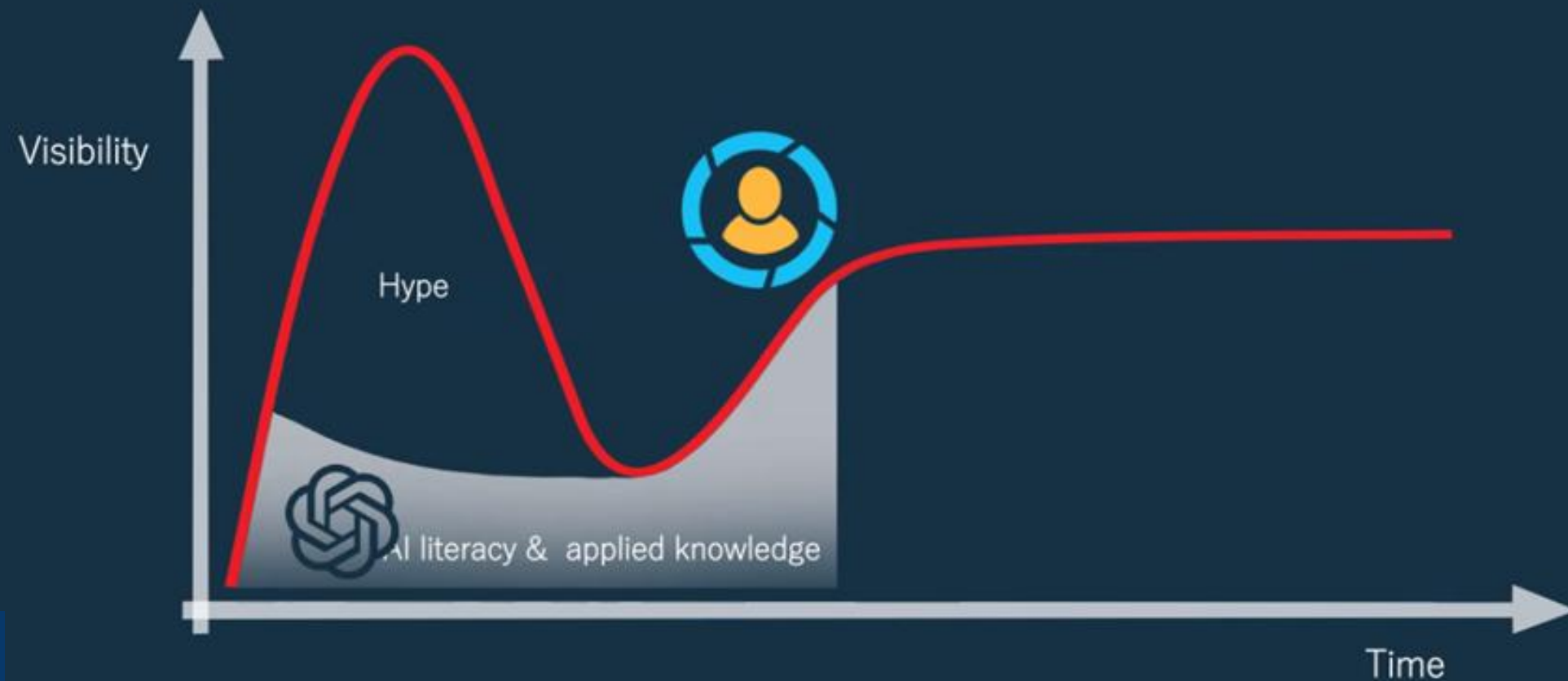
Η καλλιέργεια μιας κουλτούρας όπου η ασφάλεια αποτελεί προτεραιότητα για όλους τους εργαζόμενους ενισχύει την προστασία των κρίσιμων υποδομών σε όλα τα επίπεδα.



«Τείνουμε να υπερεκτιμούμε την επίδραση μιας τεχνολογίας στο βραχυπρόθεσμο και να την υποτιμούμε στο μακροπρόθεσμο.»

Amara's law

It takes a lot of time to apply knowledge in a productive way, beyond the initial hype















ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

- Όταν εμφανίζεται μια νέα ιδέα / τεχνολογία (π.χ. τεχνητή νοημοσύνη, blockchain, μετασύμπαν), όλοι ενθουσιάζονται, νομίζοντας ότι θα αλλάξει τον κόσμο άμεσα και ότι αποτελεί επιχειρηματική ευκαιρία.
- Στην πράξη, η πρόοδος είναι πιο αργή απ' όσο περιμέναμε στην αρχή, οπότε απογοητευόμαστε.
- Όμως, σε βάθος χρόνου, η τεχνολογία αυτή τελικά αλλάζει τον κόσμο — πολύ περισσότερο απ' όσο φανταζόμασταν στην αρχή.



- Όταν εμφανίστηκε το Ίντερνετ τη δεκαετία του '90, υπήρχε υπερβολικός ενθουσιασμός — κάποιοι πίστευαν πως θα αλλάξει τα πάντα σε λίγα χρόνια.
- Για ένα διάστημα, δεν φάνηκε να αλλάζει και τόσα πολλά, και ο κόσμος απογοητεύτηκε (dot-com φούσκα).
- Όμως 20-30 χρόνια μετά, βλέπουμε ότι το Ίντερνετ όντως άλλαξε τα πάντα — επικοινωνία, εμπόριο, πληροφορία.
-



Συμπεράσματα και Μελλοντικές Προκλήσεις



Συνεχής Εξέλιξη

Οι κυβερνοαπειλές εξελίσσονται διαρκώς, απαιτώντας συνεχή προσαρμογή των στρατηγικών Προστασίας και επένδυση σε νέες τεχνολογίες ασφαλείας.



Αυξανόμενη Διασύνδεση

Η αυξανόμενη διασύνδεση μεταξύ δομών της Δημόσιας Διοίκησης & Αυτοδιοίκησης δημιουργεί νέα τρωτά σημεία που απαιτούν ολιστικές προσεγγίσεις ασφάλειας.



Τεχνητή Νοημοσύνη

Η Τεχνητή Νοημοσύνη αποτελεί εργαλείο αλλά και Οπλικό Σύστημα που απαιτεί πρωτοφανή συνεργασία μεταξύ κυβερνήσεων, ιδιωτικού τομέα και Ακαδημαϊκής κοινότητας για την αντιμετώπιση των προκλήσεων και των απειλών.



Τεχνητή Νοημοσύνη & Κυβερνοασφάλεια Απειλές και οφέλη για την Δημόσια Διοίκηση και τοπική Αυτοδιοίκηση”

Ευχαριστώ για την Προσοχή σας

Αθανάσιος ΚΟΣΜΟΠΟΥΛΟΣ LLB, LLM, PhDc
Cert. DPO ISO/IEC 17024 - Cert. IA ISO 27001:2022
Υπεύθυνος Προστασίας Δεδομένων
Υπουργείο Ψηφιακής Διακυβέρνησης



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

