Ψηφιακός μετασχηματισμός & Κυβερνοασφάλεια στις Δ.Ε.Υ.Α.

ΕΛΕΥΘΕΡΙΟΣ ΣΦΥΡΗΣ, ΤΕΧΝΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ ΤΗΣ Ε.Δ.Ε.Υ.Α.

Ε.Δ.Ε.Υ.Α.
ΕΝΩΣΗ ΔΗΜΟΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΥΔΡΕΥΣΗΣ - ΑΠΟΧΕΤΕΥΣΗΣ

17ο OTS Forum

Τι είναι ο Ψηφιακός Μετασχηματισμός;

Από το 2020, λόγω COVID-19, έχουμε στραφεί σε μια λογική αξιοποίησης ψηφιακών τεχνολογιών και δεδομένων για τον ανασχεδιασμό διαδικασιών, προϊόντων και εμπειριών με στόχο την ευελιξία, την αποδοτικότητα και τον προσανατολισμό στον πελάτη.

Τι **δεν** είναι ο Ψηφιακός Μετασχηματισμός;

Δεν είναι μόνο τεχνολογία - είναι διαδικασίες, άνθρωποι, δεδομένα, διακυβέρνηση.

Δράσεις Ψηφιακού Μετασχηματισμού (1/2)

Λειτουργία δικτύων & εγκαταστάσεων: SCADA/τηλεμετρία, αισθητήρες, ανίχνευση διαρροών, διαχείριση πίεσης

Έξυπνη μέτρηση & τιμολόγηση: AMR/AMI, ακρίβεια μετρήσεων, αυτοματοποιημένες εκκαθαρίσεις/εισπράξεις

Διαχείριση παγίων & συντήρηση: mobile εργασίες πεδίου, GIS ολοκλήρωση

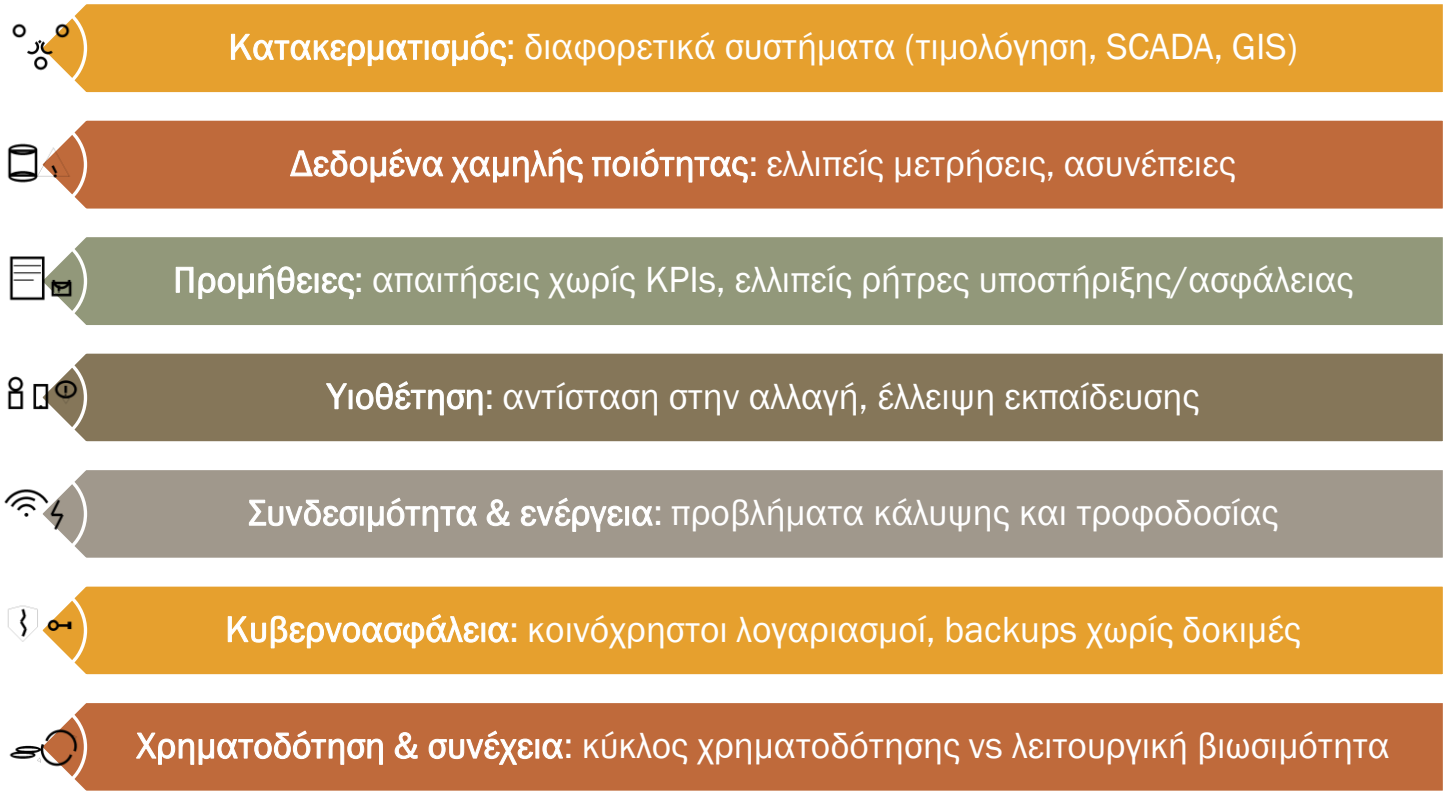
Ποιότητα νερού: online μετρήσεις, αναφορές συμμόρφωσης.

Εξυπηρέτηση πολίτη: e-αιτήματα/βλάβες, ραντεβού, e-πληρωμές, διαφάνεια

Δράσεις Ψηφιακού Μετασχηματισμού (2/2)

‘Σκαλοπάτια’ ψηφιακής ωρίμανσης

Προβλήματα και Δυσκολίες



Κυβερνοασφάλεια και Κρίσιμες Υποδομές

ΓΙΑΤΊ ΤΏΡΑ;

Τα τελευταία χρόνια παρατηρείται αύξηση επιθέσεων σε κρίσιμες υποδομές νερού, ενώ ταυτόχρονα αυξάνεται και η εξάρτηση των παρόχων από απομακρυσμένη πρόσβαση (γεωγραφική διασπορά εγκαταστάσεων, ανάγκη για 24/7 παρακολούθησης και παρέμβαση χωρίς μετακίνηση, περιορισμένοι ανθρώπινοι πόροι που συνεπάγεται remote-first).

Έτσι, με την Οδηγία (ΕΕ) 2022/2555 (NIS2) και με την Οδηγία (ΕΕ) 2022/2557 (CER) το **Πόσιμο νερό** και τα **Λύματα** ανήκουν στο ρυθμιστικό πεδίο της ΕΕ ως «βασικές οντότητες» (essential entities). Αυτό συνεπάγεται βασικά μέτρα ασφάλειας και υποχρεώσεις αναφοράς περιστατικών.

Νομοθετικό Πλαίσιο

ΕΝΩΣΙΑΚΟ ΔΙΚΑΙΟ

- **Κανονισμός (ΕΕ) 2019/881 (Cybersecurity Act):** ενισχυμένη ENISA & πλαίσιο ευρωπαϊκής πιστοποίησης
- **Οδηγία (ΕΕ) 2022/2555 (NIS2):** κοινό επίπεδο ασφάλειας για «βασικές/σημαντικές» οντότητες, μέτρα & αναφορά περιστατικών
- **Οδηγία (ΕΕ) 2022/2557 (CER):** ανθεκτικότητα κρίσιμων οντοτήτων (ύδρευση/λύματα κ.ά.)
- **Κανονισμός (ΕΕ) 2024/2847 (Cyber Resilience Act - CRA):** οριζόντιες απαιτήσεις ασφάλειας για προϊόντα με ψηφιακά στοιχεία
- **Κανονισμός (ΕΕ) 2025/38 (Cyber Solidarity Act):** «Ευρωπαϊκή Ασπίδα», δίκτυο SOCs & μηχανισμός έκτακτης ανάγκης

Τα παραπάνω συμπληρώνονται από μια πληθώρα Οδηγιών και Κανονισμών (DORA, eIDAS 2, EECC, GDPR, AI Act).

ΕΘΝΙΚΟ ΔΙΚΑΙΟ

- **Ν. 5086/2024 (ΦΕΚ Α' 23/14.02.2024):** Ίδρυση Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ) & αρμοδιότητες
- **Ν. 5160/2024 (ΦΕΚ Α' 195/27.11.2024):** Ενσωμάτωση NIS2 — μέτρα διαχείρισης κινδύνου, οντότητες, αναφορές (24h/72h/1 μήνα), EL-CSIRT (Computer Security Incident Response Team) υπό την ΕΑΚ για λειτουργική υποστήριξη, παρακολούθηση συμβάντων και αποστολή προειδοποιήσεων
- **Ν. 5236/2025 (ΦΕΚ Α' 175/10.10.2025):** Ενσωμάτωση CER — προσδιορισμός κρίσιμων οντοτήτων, αρμόδια αρχή: ΓΓ Προστασίας Κρίσιμων Οντοτήτων (Υπ. Προστασίας του Πολίτη)
- Τα παραπάνω συμπληρώνονται από διάφορες ΥΑ και νόμους, ενώ αναμένεται και η Εθνική Στρατηγική Κυβερνοασφάλειας 2026-2030.

Τι ισχύει για τις ΔΕΥΑ;

ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑ

Στο πεδίο εφαρμογής του Ν. 5160/2024 εμπίπτουν οι Δ.Ε.Υ.Α. εκείνες που χαρακτηρίζονται -κατ' ελάχιστο- ως μεσαίες επιχειρήσεις σύμφωνα με το άρθρο 2 του παραρτήματος της σύστασης 2003/361/ΕΚ.

(Αριθμός υπαλλήλων σε καθεστώς πλήρους απασχόλησης) ΚΑΙ [(Ετήσιος κύκλος εργασιών) ή (Ετήσιος συνολικός Ισολογισμός)]

Τεστ υπαγωγής: https://cyber.gov.gr/nis2-scope/

ΚΡΊΣΙΜΕΣ ΥΠΟΔΟΜΈΣ

Στο πεδίο εφαρμογής του Ν. 5236/2025 εμπίπτουν οι τομείς του Πόσιμου νερού και των Λυμάτων.

Ωστόσο, αναμένεται από τη Γενική Γραμματεία Προστασίας Κρίσιμων Οντοτήτων (Γ.Γ.Π.Κ.Ο.) του Υπουργείου Προστασίας του Πολίτη να προσδιορίσει, έως τη 17η Ιουλίου 2026, τις κρίσιμες οντότητες.

Τα επόμενα βήματα των Δ.Ε.Υ.Α.

Οι Δ.Ε.Υ.Α. που εμπίπτουν στο πεδίο εφαρμογής του Ν. 5160/2024 θα πρέπει να εγγραφούν στο Μητρώο της Εθνικής Αρχής Κυβερνοασφάλειας μέσω της Πλατφόρμας Εγγραφής Οντοτήτων του ν.5160/2024.

Για το σύνολο των Δ.Ε.Υ.Α. **προτείνεται**:

- Χρησιμοποιώντας τον Οδηγό αυτοαξιολόγησης της κυβερνοασφάλειας οργανισμών (CYBERSECURITY SELF ASSESSMENT TOOL) της Εθνικής Αρχής Κυβερνοασφάλειας να διενεργήσουν αυτοαξιολόγηση του επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών τους.
- Να ξεκινήσετε καταρτίζοντας ένα απλό, αλλά ρεαλιστικό πλάνο που να κλείνει γρήγορα τις πιο επικίνδυνες «τρύπες» — ειδικά εκεί όπου έχουμε συστήματα τηλεμετρίας.

Ενδεικτικά «πρώτα» βήματα

1. Ορίστε **υπεύθυνο κυβερνοασφάλειας** (έστω part-time)
2. Καταγραφή και αποτύπωση στοιχείων **Information Technology** (IT) & **Operational Technology** (OT):
   OT: συστήματα που ελέγχουν και παρακολουθούν φυσικές διεργασίες όπως αντλίες, αισθητήρες κτλ.
   IT: συστήματα που χειρίζονται δεδομένα & επιχειρησιακές λειτουργίες γραφείου όπως ERP, email, file servers κτλ.
3. Δημιουργείτε **Αντίγραφα Ασφαλείας**
4. Εφαρμόστε Πολυπαραγοντικό Έλεγχο Ταυτότητας – **MFA**
5. Ενεργοποιήστε **antivirus**,τοπικό **firewall**, απαγόρευση **USB**
6. Εκπαίδευση στελεχών: κανόνες anti-phishing, αναφορά ύποπτου email, μην ανοίγετε .exe/.js αρχεία
7. Καταστρώστε ένα μικρό **σχέδιο αντιμετώπισης:** ποιον καλώ αν έχω ransomware, email-compromise ή πτώση SCADA, πώς απομονώνω γρήγορα δίκτυα/σταθμούς, σε ποιον δηλώνω το συμβάν (εθνική αρχή/CSIRT)
8. Ανατρέξτε στο https://cyber.gov.gr/ για περισσότερες και πιο εξειδικευμένες συμβουλές

Σας ευχαριστώ για την προσοχή σας!!!