Υβριδικές απειλές - Η Νέα Πραγματικότητα

κυβερνο-Απειλές /Εισβολές - κυβερνο-Επιθέσεις

- **Ψυγεία Κρεοπωλείων**
- **Μονάδες Επεξεργασίας κρέατος**
- **Super Market**



- **Στρατηγική, Αρχιτεκτονική & Επιχειρησιακή Αντιμετώπιση απειλών**
- **(Cyber-HACCP) : Ανάλυση κινδύνων / Αρχιτεκτονική θωράκισης**
-

Συντάκτης :
Βασίλειος Τσουκαλάς
δρ. Χημικός

Επικοινωνία :
κιν. **:** +30 6944861418
email : qualitec46@gmail.com
www.fsp-tsoukalas.com

Εισαγωγικό σημείωμα :

Η εργασία αυτή είναι προϊόν βιβλιογραφικής ανασκόπησης / διαδικτυακής έρευνας σχετικά με την **νέα πραγματικότητα** των **Υβριδικών απειλών** και των **Τεχνικών δυνατοτήτων αντιμετώπισής** τους σε χώρους **παραγωγής** και **εμπορίας Κρέατος** και **Προϊόντων κρέατος.**

Η εργασία περιλαμβάνει 3 τομείς (κλάδους **) προσέγγισης :**

Μέρος 1ο : Συνοικιακό κρεοπωλείο

Μέρος 2ο : Βιομηχανικές Μονάδες Επεξεργασίας Κρέατος

Μέρος 3ο : Μικρή Αλυσίδα Super Market

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Η αρχιτεκτονική της εργασίας :

Στην **Εισαγωγή** : περιγράφονται εισαγωγικά στοιχεία για το πλαίσιο απειλών κυβερνοεπιθέσεων σε συνδυασμό με σχετική εικόνα που περιέχει **λέξεις κλειδιά** και αφορούν σε κατηγορίες **στόχων** και στρατηγικού σχεδιασμού, αρχιτεκτονικής θωράκισης και επιχειρησιακής απόκρισης , εκ μέρους απειλούμενων εταιρειών.

Η εικόνα περιγράφει ,ακόμη, τον **σχεδιασμό της Εργασίας**, που περιλαμβάνει **Στρατηγική, αρχιτεκτονική** και **Επιχειρησιακή αντιμετώπιση Απειλών** σε Εμπορικές και Βιομηχανικές εγκαταστάσεις . Η εργασία πραγματεύεται **Ανάλυση κινδύνων** , **Αμυντική θωράκιση** , **Πρακτικά Checklist** (Λίστες ελέγχου) και **KPL's** (Δείκτες Απόδοσης) , που συνολικά για κάθε κατηγορία επιχείρησης θα μπορούσαν να αποτελέσουν μια πρώτη **Οδηγία προσέγγισης** του επίμαχου θέματος για τις απειλούμενες τρεις επι μέρους κατηγορίες επιχειρήσεων. Ωστόσο, η εργασία , δεν αποτελεί πρόταση εφαρμογής .

Για διευκόλυνση κατανόησης των διαφορων στοιχείων επεξεργασίας , στην εργασία χρησιμοποιούται εικόνες που προέκυψαν από κείμενα επεξεργασίας του συντάκτη προκύπτουν με τη βοήθεια της AI και συνοδεύονται κάθε φορά από σχετικό σχολιασμό των διαδικασιών που περιγράφουν.

Για την διευκόλυνση κατανόησης των τεχνικών διαδικασιών (κειμένων) της εργασίας ο αναγνώστης ίσως χρειαστεί να διαθέτει βασικές γνώσεις των χρησιμοποιούμενων όρων (τεχνικών εργαλείων) εντοπισμού και αντιμετώπισης των "**απειλών**" .

Σημαντικό εργαλείο της εργασίας αποτελεί το εκτεταμένο και πλούσιο ,σημαντικότατο εργαλείο ,το **Παράρτημα**-**Γλωσσάρι - Ερμηνείας Δεικτών, τεχνικών όρων - εργαλείων εντοπισμού και αντιμετώπισης κυβερνο-απειλών –** όπου το συνοδευτικό στοιχειο [*] στο όνομα τεχνικού όρου-δείκτη σημαίνει παραπομπή στο **"Γλωσσάρι",** για εξήγηση όρου ή φράσης που επισημαίνεται. πχ. βιομηχανικό δίκτυο **(OT*).**
Επιπλέον την εργασία τεκμηριώνουν εκτεταμένες βιβλιογραφικές αναφορές ανα κατηγοτρία δείκτη, στην οποία βασίστηκε.

Τέλος, για την εμπέδωση των εννοιών, των **δεικτών (KPIs)** και της βιβλιογραφικής τους τεκμηρίωσης, το Παράρτημα είναι εμπλουτισμένο μια **συνοπτική χαρτογράφηση (Cheat Sheet),** που συνδέει το «**τι μετράμε**» με το «**ποιο πρότυπο το επιβάλλε**ι» και «**γιατί έχει κρίσιμη σημασία στην πράξη**»:

Καλή αρχή ....

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

1. Εισαγωγή & Πλαίσιο Απειλής *

Οι πρόσφατες **κυβερνοεπιθέσεις** σε ευρωπαϊκά σούπερ μάρκετ αλλά και σε ελληνικές επιχειρήσεις έδειξαν ότι οι “επιτιθέμενοι” στοχεύουν πλέον απευθείας σε διασυνδεδεμένους “**ελεγκτές εμπορικής ψύξης”*** (controllers) των εγκαταστάσεων , σε διασυνδεδεμένους αισθητήρες IoT* και σε συστήματα αυτοματισμού (SCADA/BMS*) αλλά και εργαλείων τεχνητής νοημοσύνης - **AI**.

Ενεργοποιώντας εξ’αποστάσεως ή παραποιώντας τη λειτουργία απόψυξης (defrost mode) ή απενεργοποιώντας τους συναγερμούς, **ανεβάζουν τη θερμοκρασία** έως και τους 50°C και πλέον , προκαλώντας καταστροφή αποθεμάτων προϊόντων / α΄υλών , κίνδυνο πυρκαγιάς και σοβαρά ζητήματα δημόσιας υγείας.



Η αντιμετώπιση αυτών των απειλών προβλέπει , κατάρχάς, την **ενσωμάτωση** της **κυβερνοασφάλειας** στα συστήματα διαχείρισης ασφάλειας τροφίμων (**Cyber-HACCP**), προσαρμογή της αρχιτεκτονικής, **άμεση απομόνωση των “ελεγκτών” από το δημόσιο**

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

διαδίκτυο και **αυστηρό διαχωρισμό των βιομηχανικών δικτύων (OT*) από τα εταιρικά (IT*)**, συνδυάζοντας τεχνικές δικλίδες και στρατηγικό σχεδιασμό.

Ελεγκτές Εμπορικής Ψύξης (Controllers): Ρόλος & Ευπάθειες

1. Τι είναι & Τι ελέγχουν (Ο «Εγκέφαλος»)

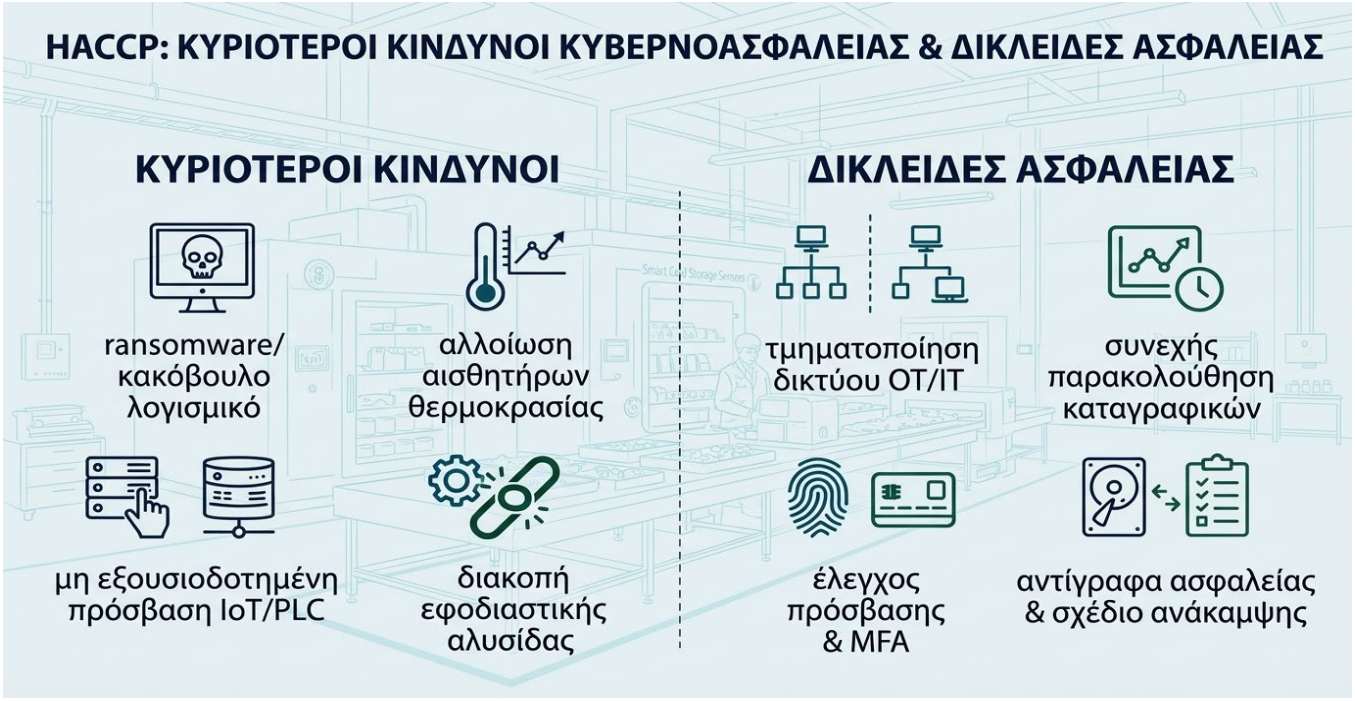
- **Ρύθμιση Θερμοκρασίας:** Διαβάζουν αισθητήρες και ενεργοποιούν/σταματούν συμπιεστές & ανεμιστήρες.
- **Κύκλοι Απόψυξης (Defrost):** Ελέγχουν τις αντιστάσεις απόψυξης για να μην πιάνει πάγο ο εξατμιστής.
- **Συναγερμοί (Alarms):** Εντοπίζουν αποκλίσεις θερμοκρασίας, ανοιχτές πόρτες ή βλάβες.
- **Καταγραφή HACCP:** Αποθηκεύουν ιστορικά δεδομένα θερμοκρασίας για υγειονομικούς ελέγχους.

2. Γιατί αποτελούν στόχο κυβερνοεπιθέσεων

- **Εργοστασιακοί Κωδικοί:** Πολλοί ελεγκτές παραμένουν με προεπιλεγμένους κωδικούς (0000, 1234, admin).
- **Έκθεση στο Internet:** Συνδέονται μέσω απλού port forwarding χωρίς VPN, ορατοί σε μηχανές σάρωσης.
- **Μη Κρυπτογραφημένα Πρωτόκολλα:** Πρωτόκολλα όπως το κλασικό Modbus επιτρέπουν αλλαγή εντολών χωρίς έλεγχο.
- **Απομακρυσμένο Defrost:** Οι επιτιθέμενοι ενεργοποιούν τη θέρμανση απόψυξης και σιγάζουν τα alarms.

Ενδεικτικοί Κατασκευαστές: Dixell • Carel • Danfoss • Eliwell • EVCO | Το πρόβλημα δεν είναι η συσκευή, αλλά η απροστάτευτη σύνδεσή της.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.



[Η εικόνα αποτυπώνει με σαφήνεια τη σύγχρονη πρόκληση της ασφάλειας τροφίμων, όπου το "κλασικό " σύστημα **HACCP** συναντά την ψηφιακή πραγματικότητα της κυβερνοασφάλειας. Αναδεικνύονται οι κρίσιμες ψηφιακές απειλές, που μπορούν να υπονομεύσουν την παραγωγή και την συντήρηση των προϊόντων, όπως οι επιθέσεις **ransomware***, η **αλλοίωση των ενδείξεων στους αισθητήρες θερμοκρασίας,** η **μη εξουσιοδοτημένη πρόσβαση στα βιομηχανικά συστήματα ελέγχου (IoT/PLC)*** και οι ευρύτερες **διακοπές στην εφοδιαστική αλυσίδα**. Απέναντι σε αυτούς τους κινδύνους (δεξιά πλευρά) προβάλλονται οι απαραίτητες **δικλείδες ασφαλείας** για την προστασία της επιχειρησιακής συνέχειας και της **υγιεινής των τροφίμων**. Μέσα από τον διαχωρισμό των δικτύων OT* και IT*, τη συνεχή παρακολούθηση των καταγραφικών δεδομένων, τον αυστηρό έλεγχο πρόσβασης με πολυπαραγοντική ταυτοποίηση (MFA*) και την ύπαρξη αξιόπιστων αντιγράφων ασφαλείας και σχεδίων ανάκαμψης, διασφαλίζεται ότι **η τεχνολογία παραμένει σύμμαχος** και **όχι αδύναμος κρίκος στην αλυσίδα των τροφίμων**.]

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.



[Η εικόνα αποτυπώνει οπτικά την κρίσιμη ανάγκη θωράκισης της εφοδιαστικής αλυσίδας τροφίμων απέναντι στις σύγχρονες κυβερνοαπειλές. Μέσα από ένα περιβάλλον βιομηχανικής ψύξης και αυτοματοποιημένης επεξεργασίας κρέατος, αναδεικνύεται πώς οι ψηφιακές ασπίδες προστατεύουν ευαίσθητες υποδομές, όπως τα ψυγεία κρεοπωλείων, τις μονάδες παραγωγής και τα super markets, από επιθέσεις που θα μπορούσαν να διαταράξουν τη συντήρηση και τη διανομή των προϊόντων. Παράλληλα, τα συνοδευτικά πλαίσια οργανώνουν τη λύση σε ένα ολοκληρωμένο πλαίσιο δράσης, συνδέοντας τη στρατηγική πλοήγηση και την αρχιτεκτονική θωράκιση με την επιχειρησιακή απόκριση, ενώ καταλήγουν στη δημιουργία ενός δομημένου οδηγού, που ενοποιεί την ανάλυση κινδύνων, τα πρακτικά checklists και τους δείκτες απόδοσης (KPIs*)] .

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Παραδείγματα αντιμετώπισης κυβερνο-απειλών

(3 αντιπροσωπευτικοί κλάδοι) :

Μέρος 1ο : Κρεοπωλείο / Συνοικιακό Κατάστημα



Σύντομη προσέγγιση :

Ο **βασικός κίνδυνος** προέρχεται από την ευκολία με την οποία ένας **σύγχρονος ελεγκτής ψύξης** (controller) συνδέεται στο internet για να προσφέρει απομακρυσμένο έλεγχο, αφήνοντας, όμως, ανοιχτή μια «πίσω πόρτα» με εργοστασιακούς κωδικούς.

Αποποίηση ευθύνης :

Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Η στρατηγική άμυνας ,εδώ, ακολουθεί τη λογική του «**κλειδώματος**»: αν το ψυγείο δεν χρειάζεται να «μιλάει» με το διαδίκτυο, **αποσυνδέεται πλήρως**.

Για να μην χαθεί , όμως , η εποπτεία της θερμοκρασίας, η παρακολούθηση μεταφέρεται σε ένα εντελώς ανεξάρτητο, παράλληλο κανάλι επικοινωνίας.

Σε ένα μικρό συνοικιακό κρεοπωλείο , η **ασφάλεια δεν βασίζεται** σε ακριβά συστήματα πληροφορικής, αλλά στην απλότητα και την εξάλειψη της επιφάνειας επίθεσης.

2. Ανάλυση : Αρχιτεκτονική & Checklists * (Checklists)

2.1 Αρχιτεκτονική «Ψηφιακής Απομόνωσης»* (Air-Gapping & Out-of-Band Monitoring)

- **Προσέγγιση παραδείγματος:** Σε ένα μικρό κατάστημα (κρεοπωλείο) χωρίς τμήμα IT , η ασφάλεια βασίζεται στην απλότητα.

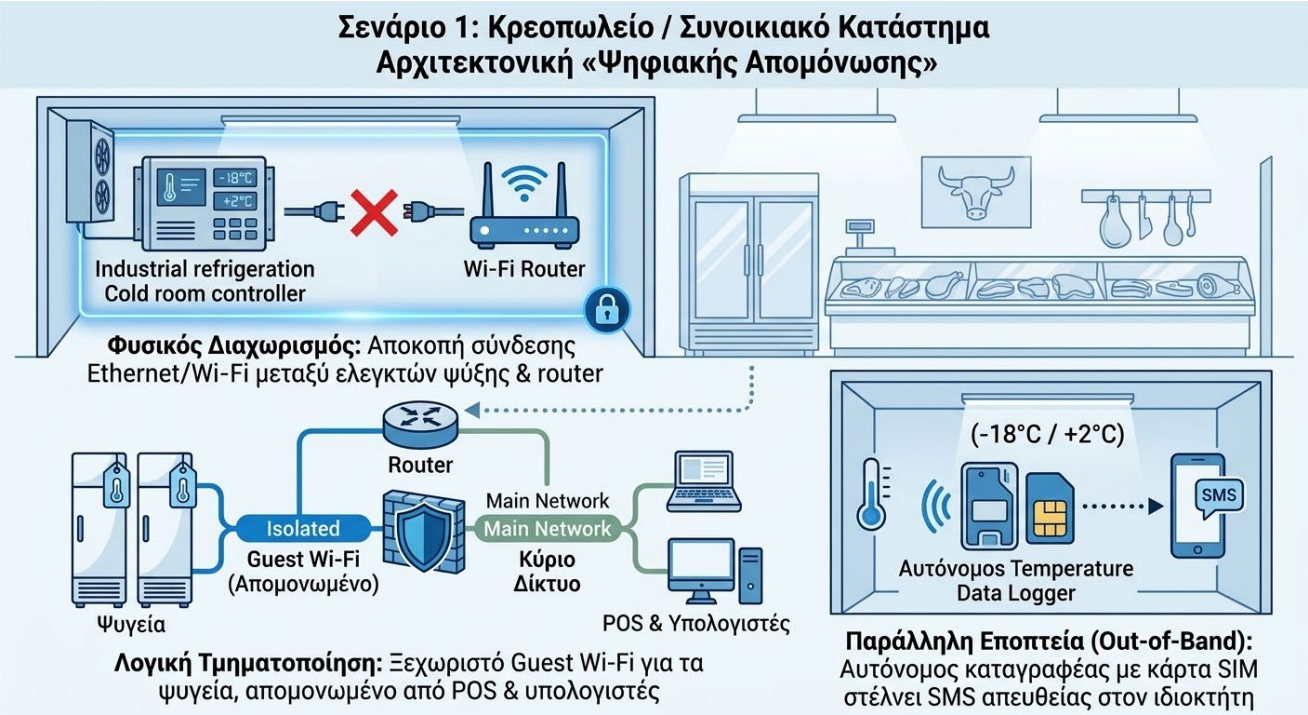
  Αν οι "**ελεγκτές ψύξης**" δεν χρειάζονται απομακρυσμένο έλεγχο, αποσυνδέονται πλήρως από το διαδίκτυο. Η εποπτεία της θερμοκρασίας μεταφέρεται σε ένα εντελώς ανεξάρτητο, παράλληλο κανάλι επικοινωνίας (μέσω δικτύου κινητής τηλεφωνίας), ώστε **καμία επίθεση στο τοπικό router* να μην μπορεί να "σιγάσει" τους συναγερμούς.**

Περιγραφή Αρχιτεκτονικής:

- **Φυσικός Διαχωρισμός:** Αποκοπή της σύνδεσης Ethernet/Wi-Fi* μεταξύ **ελεγκτών ψύξης** και **router**.
- **Λογική Τμηματοποίηση** (αν απαιτείται σύνδεση)**:** Σύνδεση των ψυγείων σε απομονωμένο *Guest Wi-Fi**, ξεχωριστό από το POS* και τους υπολογιστές.
- **Παράλληλη Εποπτεία** (Out-of-Band)**:** Εγκατάσταση αυτόνομου καταγραφέα θερμοκρασίας με κάρτα SIM* εντός των θαλάμων, ο οποίος στέλνει SMS* απευθείας στον ιδιοκτήτη του καταστήματος.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Πηγή : **Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ)**



[Η εικόνα παρουσιάζει με απλό και κατανοητό τρόπο πώς ένα συνοικιακό κρεοπωλείο μπορεί να προστατεύσει τα ψυγεία του μέσω της αρχιτεκτονικής **«Ψηφιακής Απομόνωσης*».** Πρόκειται για **τρία πρακτικά βήματα ασφαλείας**: αρχικά προτείνεται ο **φυσικός διαχωρισμός**, αποσυνδέοντας εντελώς τους ελεγκτές ψύξης από το δίκτυο και το **router*** του καταστήματος.

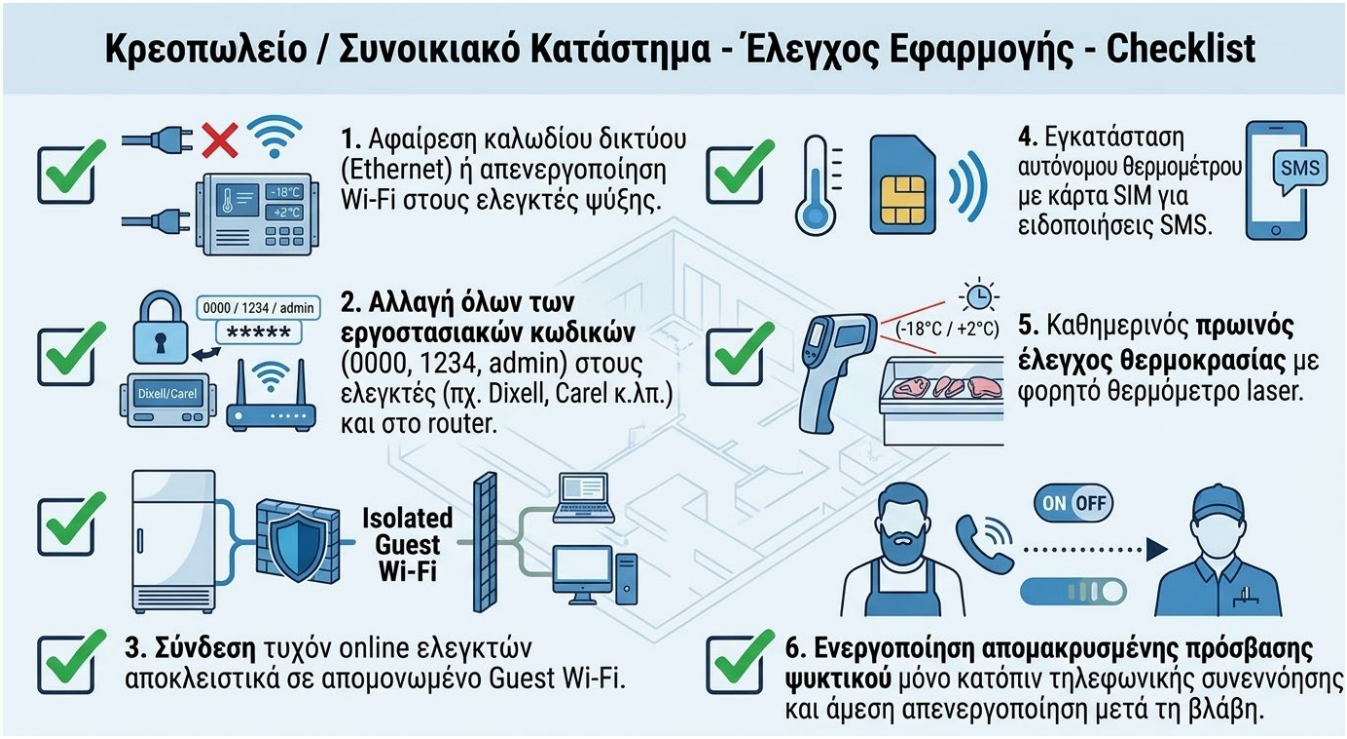
Στην περίπτωση , που η δικτύωση είναι απαραίτητη, προκρίνεται η **Λογική τμηματοποίηση***, όπου τα ψυγεία συνδέονται σε ένα ξεχωριστό, απομονωμένο Guest Wi-Fi*, ώστε να μην επικοινωνούν με το κύριο δίκτυο, που φιλοξενεί το POS* και τους υπολογιστές.

Τέλος, η ασφάλεια ενισχύεται με την **παράλληλη εποπτεία** (Out-of-Band), μέσω ενός αυτόνομου καταγραφέα θερμοκρασίας με κάρτα SIM, που λειτουργεί ανεξάρτητα από το τοπικό ίντερνετ και **ειδοποιεί άμεσα τον ιδιοκτήτη του κρεοπωλείου με SMS σε περίπτωση απόκλισης**.]

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Έλεγχος Εφαρμογής- Checklist *

- Αφαίρεση καλωδίου δικτύου (Ethernet) ή απενεργοποίηση Wi-Fi στους **ελεγκτές ψύξης**.
- Αλλαγή όλων των εργοστασιακών κωδικών (0000, 1234, admin) στους **ελεγκτές** (πχ.Dixell, Carel κ.λπ.) και στο **router** *.
- Σύνδεση τυχόν online ελεγκτών **αποκλειστικά** σε απομονωμένο **Guest Wi-Fi**.*
- Εγκατάσταση αυτόνομου θερμομέτρου με κάρτα SIM* για ειδοποιήσεις SMS*.
- Καθημερινός πρωινός **έλεγχος θερμοκρασίας** με φορητό θερμόμετρο **laser***.
- Ενεργοποίηση απομακρυσμένης πρόσβασης ψυκτικού μόνο κατόπιν τηλεφωνικής συνεννόησης και άμεση απενεργοποίηση μετά τη βλάβη.



Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

[Επανάληψη περιγραφής διαδικασίας.- *εμπέδωση* -: Η εικόνα λειτουργεί ως ένας πρακτικός οπτικός οδηγός ελέγχου (checklist) έξι βημάτων, σχεδιασμένος για να θωρακίσει ψηφιακά ένα συνοικιακό κρεοπωλείο με απλό και άμεσο τρόπο.
Αρχικά, εστιάζει στη βασική ασφάλεια του δικτύου, προτείνοντας την αποσύνδεση των ελεγκτών ψύξης από το ίντερνετ, την αλλαγή όλων των ευάλωτων εργοστασιακών κωδικών και τη χρήση απομονωμένου **Guest Wi-Fi***, όπου η σύνδεση είναι απαραίτητη.

Στη συνέχεια, η προσοχή μεταφέρεται στην ανεξάρτητη παρακολούθηση και την καθημερινή ρουτίνα, μέσα από την τοποθέτηση αυτόνομου θερμομέτρου με κάρτα SIM για ειδοποιήσεις SMS*, αλλά και τη χειροκίνητη επιβεβαίωση της θερμοκρασίας κάθε πρωί με φορητό θερμόμετρο **laser** *.

Τέλος, το διάγραμμα υπογραμμίζει τον αυστηρό έλεγχο στην **εξωτερική τεχνική υποστήριξη**, ορίζοντας ότι η απομακρυσμένη πρόσβαση του ψυκτικού πρέπει να ενεργοποιείται μόνο κατόπιν τηλεφωνικής συνεννόησης και να απενεργοποιείται αμέσως μετά την αποκατάσταση της βλάβης.]
Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ)

Περισσότερα σύμφωνα με την *Εθνική Αρχής Κυβερνοασφάλειας (ΕΑΚ)*

Οι **ελεγκτές ψύξης** δεν πρέπει ποτέ να είναι άμεσα προσβάσιμοι (exposed) στο **δημόσιο internet**. Η απομακρυσμένη διαχείριση επιτρέπεται μόνο μέσω κρυπτογραφημένου VPN* και πολυπαραγοντικής αυθεντικοποίησης (MFA)*.

- Κατάργηση προεπιλεγμένων κωδικών (Default Passwords) με άμεση αλλαγή όλων των εργοστασιακών κωδικών πρόσβασης στους **ελεγκτές**, τα **routers** και το **λογισμικό διαχείρισης** (SCADA/BMS*).

- Τμηματοποίηση Δικτύου (Network Segmentation / VLANs*): Το **δίκτυο των ψυγείων** και **των αισθητήρων** (OT* - Operational Technology) πρέπει να είναι αυστηρά απομονωμένο από το εταιρικό Wi-Fi*, τα ταμεία (POS*) και τους υπολογιστές γραφείου (IT*).

Σε περιπτώσεις, που η συνδεσιμότητα είναι απαραίτητη, το router* του καταστήματος διαμορφώνεται, ώστε να δημιουργεί ένα απομονωμένο υποδίκτυο (Guest Wi-Fi *). Τα ψυγεία τοποθετούνται σε αυτή τη ζώνη, αποκομμένα από το εσωτερικό δίκτυο (LAN*), όπου βρίσκονται το POS* και ο υπολογιστής της επιχείρησης.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Το POS* *(περισσότερα βλ. συνημμένο παράρτημα)* **αποτελεί κρίσιμο κίνδυνο για τους ελεγκτές ψύξης. Ειδικότερα ....**

- **Διαρκής Έκθεση στο Διαδίκτυο:**

  Τα συστήματα POS* είναι μόνιμα συνδεδεμένα στο ίντερνετ (για επικοινωνία με τράπεζες, ΑΑΔΕ/myDATA, παρόχους λογισμικού και email), γεγονός ,που τα καθιστά τον υπ' αριθμόν ένα στόχο κυβερνοεπιθέσεων (phishing*, ransomware*, κακόβουλα USB*).

- **Κίνδυνος Πλευρικής Κίνησης** (Lateral Movement*)**:** Αν οι **ελεγκτές** θερμοκρασίας των ψυγείων βρίσκονται στο **ίδιο τοπικό δίκτυο (LAN/Wi-Fi*)** με το **POS*** και τους υπολογιστές του ταμείου, ένας **ιός,** που θα **μολύνει** το **ταμείο** μπορεί να **«πηδήξει»** αυτόματα στους **ελεγκτές ψύξης**, να αλλάξει τις θερμοκρασίες ή να κλειδώσει τη λειτουργία τους.

- **Διαφορετικές Απαιτήσεις Ασφαλείας (IT* vs OT*):** Το **POS*** ανήκει στο δίκτυο πληροφορικής γραφείου (IT* – Information Technology), ενώ τα ψυγεία και τα SCADA* ανήκουν στην επιχειρησιακή τεχνολογία (**OT – Operational Technology***). Τα διεθνή πρότυπα κυβερνοασφάλειας (όπως το NIST SP 800-82 *) επιβάλλουν αυτά τα δύο δίκτυα να μην επικοινωνούν ποτέ απευθείας μεταξύ τους.

Παράλληλη Εποπτεία (Out-of-Band Alerting)* : Εντός των ψυκτικών θαλάμων εγκαθίσταται ένα **αυτόνομο σύστημα τηλεμετρίας *** (καταγραφέας με ενσωματωμένη κάρτα SIM). Το σύστημα αυτό δεν επικοινωνεί ηλεκτρονικά με τον ελεγκτή του ψυγείου· μετρά τη φυσική θερμοκρασία του χώρου και, μέσω δικτύου κινητής τηλεφωνίας (GSM/4G *), αποστέλλει ειδοποιήσεις SMS απευθείας στον ιδιοκτήτη, παρακάμπτοντας οποιαδήποτε κυβερνοεπίθεση στο τοπικό δίκτυο.

- Ενημερώσεις & Απόσυρση Παλαιού Εξοπλισμού: Εγκατάσταση όλων των διαθέσιμων **firmware*** updates. Παλαιοί **ελεγκτές,** που δεν υποστηρίζονται πλέον από τον κατασκευαστή (*End-of-Life*) πρέπει να αντικαθίστανται ή να αποσυνδέονται πλήρως από το δίκτυο.

- Ανεξάρτητο Σύστημα Συναγερμού (*Out-of-Band Monitoring*)* : Εγκατάσταση ανεξάρτητων, αναλογικών ή ξεχωριστού δικτύου αισθητήρων θερμοκρασίας (π.χ. μέσω LoRaWAN* ή 5G/GSM)*, που ειδοποιούν με SMS/κλήση τον υπεύθυνο ασφαλείας, ακόμα κι αν ο **κεντρικός ελεγκτής** παραβιαστεί και σιγήσουν οι δικοί του συναγερμοί.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- Φυσικά Όρια Ασφαλείας (*Hardware Failsafes*): Ρύθμιση φυσικών/μηχανικών θερμοστατών ασφαλείας που διακόπτουν την παροχή ρεύματος στις αντιστάσεις απόψυξης αν η θερμοκρασία ξεπεράσει ένα κρίσιμο όριο (αποτρέποντας υπερθέρμανση και πυρκαγιές).



[Η εικόνα παρουσιάζει σε τρία διαδοχικά πεδία την **αρχιτεκτονική θωράκισης των συστημάτων ψύξης, περιγράφοντας μια κλιμακωτή στρατηγική απομόνωσης και ανεξάρτητης επιτήρησης.**

Στο πρώτο πεδίο, με τίτλο «1. Φυσικός Διαχωρισμός», αποτυπώνεται η απόλυτη γραμμή άμυνας μέσω της πλήρους αποκοπής της σύνδεσης Ethernet* ή Wi-Fi* μεταξύ του ψηφιακού ελεγκτή ψύξης και του δρομολογητή (router*), δημιουργώντας ένα φυσικό κενό ασφαλείας (air-gap) , που εκμηδενίζει την εξωτερική δικτυακή έκθεση.

Στο δεύτερο πεδίο, με τίτλο «2. Λογική Τμηματοποίηση (αν απαιτείται σύνδεση)», παρουσιάζεται η εναλλακτική προσέγγιση για τις περιπτώσεις όπου η δικτύωση κρίνεται αναγκαία· η εικόνα δείχνει πώς ένα τείχος προστασίας (firewall*) διαχωρίζει αυστηρά το κύριο εταιρικό δίκτυο (**M**ain **B**usiness **N**etwork) των υπολογιστών και του POS* από την

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

απομονωμένη ζώνη επισκεπτών (Guest Wi-Fi Zone*), μέσα στην οποία τοποθετούνται οι **ελεγκτές των ψυγείων** , ώστε να αποτρέπεται η **πλευρική κίνηση απειλών** *.

Τέλος, στο τρίτο πεδίο, με τίτλο «3. Παράλληλη Εποπτεία (Out-of-Band)*», αναδεικνύεται ο μηχανισμός αδιάλειπτης επιτήρησης μέσω της εγκατάστασης ενός αυτόνομου καταγραφέα θερμοκρασίας με ενσωματωμένη κάρτα SIM εντός των ψυκτικών θαλάμων, ο οποίος επικοινωνεί ανεξάρτητα μέσω κεραίας κινητής τηλεφωνίας και αποστέλλει άμεση ειδοποίηση SMS απευθείας στο κινητό του ιδιοκτήτη.]

<u>Checklist Εφαρμογής (</u> <u>σύνοψη του σχολιασμού της εικόνας</u> **<u>)</u>**

- Αφαίρεση καλωδίου δικτύου (Ethernet) ή απενεργοποίηση Wi-Fi στους ελεγκτές ψύξης.
- Αλλαγή όλων των εργοστασιακών κωδικών (0000, 1234, admin) στους ελεγκτές (Dixell, Carel κ.λπ.) και στο router.
- Σύνδεση τυχόν online ελεγκτών αποκλειστικά σε απομονωμένο *Guest Wi-Fi*.
- Εγκατάσταση αυτόνομου θερμομέτρου με κάρτα SIM για ειδοποιήσεις SMS.
- Καθημερινός πρωινός έλεγχος θερμοκρασίας με φορητό θερμόμετρο laser.
- Ενεργοποίηση απομακρυσμένης πρόσβασης ψυκτικού μόνο κατόπιν τηλεφωνικής συνεννόησης και άμεση απενεργοποίηση μετά τη βλάβη.



Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

[Η εικόνα αναλύει με σαφήνεια τους λόγους για τους οποίους η σύνδεση του συστήματος POS στο ίδιο δίκτυο με τους ελεγκτές ψύξης αποτελεί σοβαρή απειλή κυβερνοασφάλειας. Αρχικά, αναδεικνύει τη συνεχή έκθεση του POS στο διαδίκτυο λόγω της επικοινωνίας του πχ. με τράπεζες, την πλατφόρμα ΑΑΔΕ/myDATA, email και παρόχους λογισμικού, **γεγονός που το καθιστά ευάλωτο σε επιθέσεις phishing, ransomware και κακόβουλα USB.** Στη συνέχεια, απεικονίζεται ο κίνδυνος της πλευρικής κίνησης (Lateral Movement), δείχνοντας πώς ένας ιός που μολύνει το ταμείο μπορεί να εξαπλωθεί αυτόματα μέσω του κοινού τοπικού δικτύου στους ελεγκτές θερμοκρασίας, αλλοιώνοντας τις ρυθμίσεις ή κλειδώνοντας τη λειτουργία των ψυγείων.

Τέλος, το διάγραμμα υπογραμμίζει την αναγκαιότητα αυστηρού διαχωρισμού μεταξύ του δικτύου πληροφορικής γραφείου (IT) και της επιχειρησιακής τεχνολογίας (OT), επισημαίνοντας ότι τα διεθνή πρότυπα, όπως το **NIST SP 800-82** (βλ. παράρτημα), επιβάλλουν την πλήρη απομόνωσή τους , ώστε να μην επικοινωνούν ποτέ απευθείας μεταξύ τους.]

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Μέρος 2ο: Βιομηχανικές Μονάδες Επεξεργασίας Κρέατος



Αρχιτεκτονική «Βαθιάς Άμυνας»* **(**Defense-in-Depth & Purdue Model**)**

Στη βιομηχανία επεξεργασίας κρέατος , η ψύξη αποτελεί την καρδιά της παραγωγής και της δημόσιας υγείας.
Τα συστήματα ψύξης (PLCs*/SCADA*) αποτελούν κρίσιμη υποδομή (υπαγόμενη και στην οδηγία NIS2*). Η στρατηγική εδώ δημιουργεί ψηφιακά «στεγανά» μεταξύ των γραφείων και της παραγωγής, ενώ προσθέτει **φυσικούς**, αναλογικούς «**κόφτες**» που εμποδίζουν οποιαδήποτε κακόβουλη εντολή να υπερθερμάνει τους θαλάμους.

Μια **κυβερνοεπίθεση** δεν απειλεί απλώς το εμπόρευμα, αλλά μπορεί να προκαλέσει **βιομηχανικό ατύχημα** ή **μαζική διάθεση αλλοιωμένων προϊόντων στην αγορά**.

Η **αρχιτεκτονική αντιμετώπισης** βασίζεται στην **αυστηρή ιεράρχηση των δικτύων**: χτίζονται **ψηφιακά «στεγανά»** μεταξύ των γραφείων και της παραγωγής, ενώ τοποθετούνται φυσικοί, αναλογικοί «κόφτες» , που εμποδίζουν οποιαδήποτε κακόβουλη ψηφιακή εντολή να υπερθερμάνει τους θαλάμους.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Περιγραφή της Αρχιτεκτονικής:

1. **Τμηματοποίηση Purdue Model* & Industrial DMZ*:** Διαχωρισμός εταιρικού δικτύου (IT) από το βιομηχανικό δίκτυο ψύξης (OT*) μέσω βιομηχανικών Firewalls*.

2. **Κρυπτογραφημένη Διασύνδεση (Site-to-Site IPsec VPN):** Ασφαλής επικοινωνία μεταξύ των δύο εργοστασίων χωρίς έκθεση βιομηχανικών πρωτοκόλλων στο διαδίκτυο.

3. **Επίπεδο Φυσικής Ασφάλειας (Hardware Failsafes):** Αναλογικοί θερμοστάτες ασφαλείας που κόβουν μηχανικά το ρεύμα στις αντιστάσεις απόψυξης σε περίπτωση υπερθέρμανσης.

4. **Ελεγχόμενη Πρόσβαση & Ανίχνευση (PAM & OT-IDS):** Χρονομετρημένη πρόσβαση συνεργατών (Just-in-Time) και παθητική παρακολούθηση δικτύου για ύποπτες εντολές προς τα PLCs.

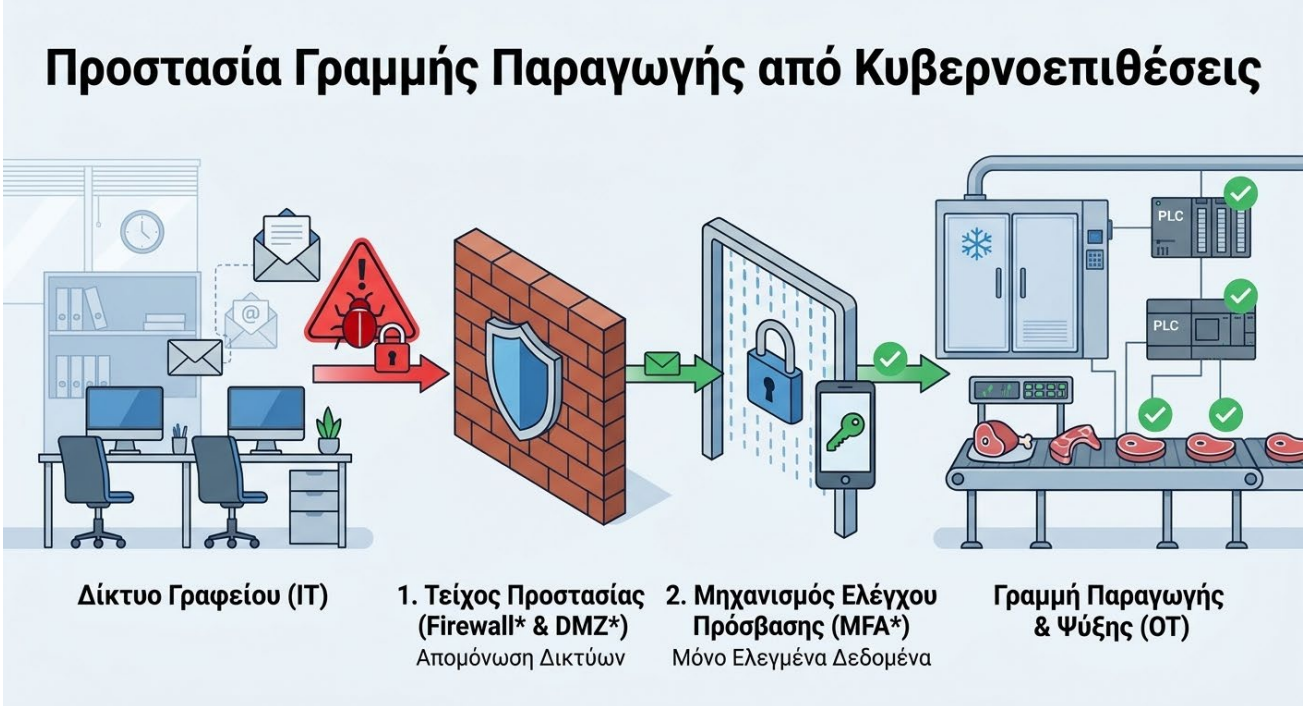


Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Η εικόνα αποτυπώνει την **αρχιτεκτονική σύνδεσης ανάμεσα στο διοικητικό κομμάτι (IT*) και τον χώρο παραγωγής (OT*)** πχ. μιας βιομηχανίας επεξεργασίας κρέατος , αναδεικνύοντας πώς προστατεύεται η ομαλή λειτουργία και η ασφάλεια των προϊόντων. Στα αριστερά βρίσκεται το **Επίπεδο IT* (ERP*)**, όπου η διοίκηση διαχειρίζεται τις παραγγελίες, την αποθήκη και την ιχνηλασιμότητα των παρτίδων, ενώ στα δεξιά βρίσκεται το **Επίπεδο OT**, που περιλαμβάνει τα φυσικά μηχανήματα, τους αισθητήρες θερμοκρασίας ψυγείων και τις γραμμές συσκευασίας.

Ανάμεσά τους λειτουργεί ως «γέφυρα» η **Ενδιάμεση Ζώνη (MES)***, η οποία μεταφράζει τις εμπορικές εντολές παραγωγής προς τα μηχανήματα και επιστρέφει πίσω **κρίσιμα δεδομένα ελέγχου και θερμοκρασιών** για το **HACCP**.

Για να μην περάσει μια κυβερνοεπίθεση από το γραφείο στη γραμμή παραγωγής, παρεμβάλλονται **δύο αυστηρές δικλίδες ασφαλείας**: ένα **τείχος προστασίας (Firewall* & DMZ*),** που απομονώνει τα δίκτυα και ένας μηχανισμός **ελέγχου πρόσβασης (MFA*),** που **επιτρέπει την κυκλοφορία αποκλειστικά και μόνο ελεγμένων δεδομένων**.



Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

[DMZ* : Πώς λειτουργεί στην πράξη

*Αντί τα συστήματα του γραφείου (ERP) να μιλούν απευθείας με τα μηχανήματα του εργοστασίου (PLCs/αισθητήρες), και οι δύο πλευρές συνδέονται **μόνο** με τον ενδιάμεσο server (όπως το MES*) που βρίσκεται μέσα στη ζώνη DMZ:*

- ***Δεν υπάρχει απευθείας διέλευση:** Ένας χρήστης ή ένας ιός από το IT δεν μπορεί ποτέ να «δει» ή να αγγίξει απευθείας το **OT**.*
- ***Ελεγχόμενη ανταλλαγή:** Το **OT*** «αφήνει» τα δεδομένα (π.χ. θερμοκρασίες ψυγείων) στη DMZ, και το IT έρχεται και τα «παίρνει» από εκεί.*
- ***Περιορισμός ζημιάς (Containment):** Αν ένα κακόβουλο λογισμικό καταφέρει να παραβιάσει το δίκτυο των γραφείων, «σκοντάφτει» στα τείχη προστασίας (Firewalls) της DMZ και η γραμμή παραγωγής συνεχίζει να λειτουργεί κανονικά χωρίς να κινδυνεύει η ασφάλεια των τροφίμων* **]**

[MFA* *(Multi-Factor Authentication – Πολυπαραγοντική Ταυτοποίηση)- Πως λειτουργεί στην πράξη : Αντί να αρκεί μόνο ένας κωδικός πρόσβασης (που μπορεί να κλαπεί ή να μαντευτεί), το MFA συνδυάζει στοιχεία από διαφορετικές κατηγορίες:*

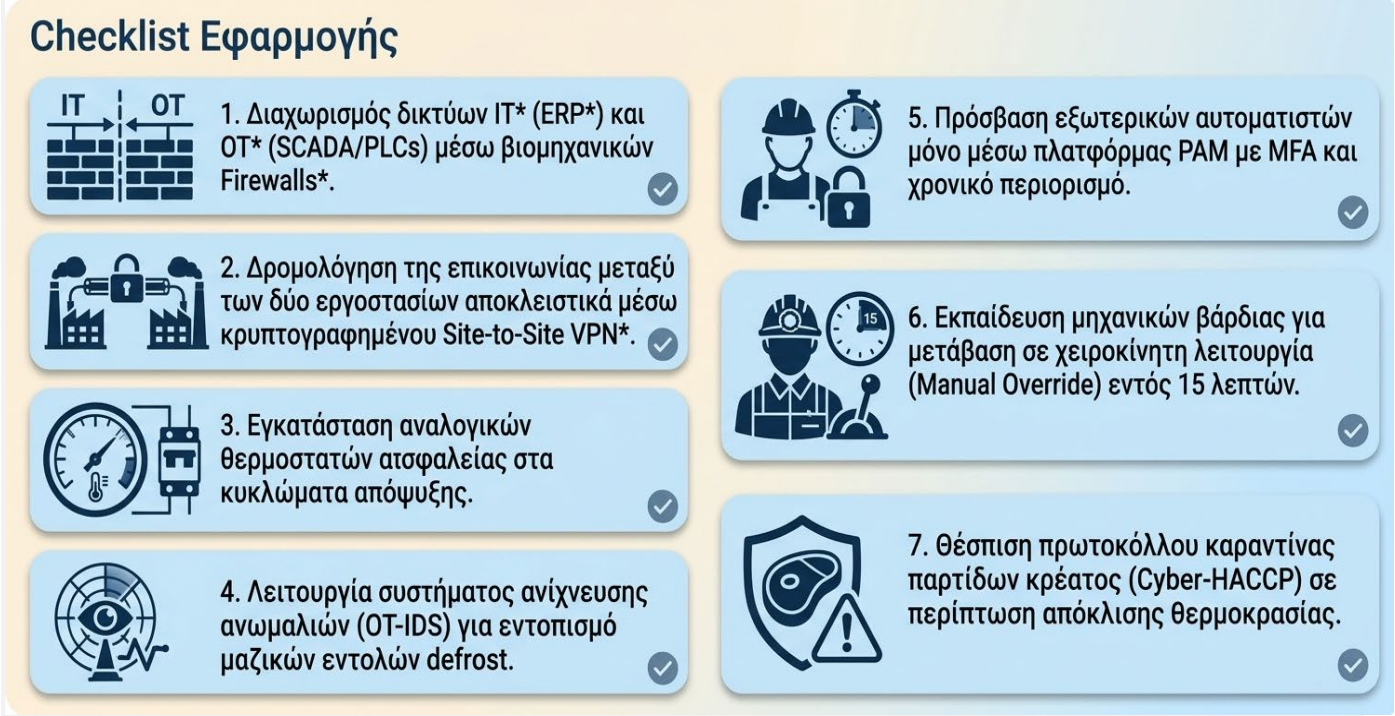
- ***Κάτι που γνωρίζετε:** Ο κωδικός πρόσβασης (password) ή ένα PIN*.*
- ***Κάτι που έχετε:** Το εταιρικό κινητό τηλέφωνο (για έγκριση μέσω εφαρμογής/SMS) ή ένα φυσικό κλειδί ασφαλείας (USB token* / έξυπνη κάρτα).*
- ***Κάτι που είστε:** Βιομετρικά στοιχεία, όπως δακτυλικό αποτύπωμα ή αναγνώριση προσώπου.***]**

Checklist Εφαρμογής

Checklist Εφαρμογής

- Διαχωρισμός **δικτύων IT*** (ERP*) και **OT*** (SCADA/PLCs) μέσω βιομηχανικών Firewalls *.
- Δρομολόγηση της επικοινωνίας μεταξύ των δύο εργοστασίων αποκλειστικά μέσω κρυπτογραφημένου Site-to-Site VPN*.
- Εγκατάσταση αναλογικών θερμοστατών ασφαλείας στα κυκλώματα απόψυξης.
- Λειτουργία συστήματος ανίχνευσης ανωμαλιών (OT-IDS) για εντοπισμό μαζικών εντολών *defrost*.
- Πρόσβαση εξωτερικών αυτοματιστών μόνο μέσω πλατφόρμας PAM με MFA και χρονικό περιορισμό.
- Εκπαίδευση μηχανικών βάρδιας για μετάβαση σε χειροκίνητη λειτουργία (*Manual Override*) εντός 15 λεπτών.
- Θέσπιση πρωτοκόλλου καραντίνας παρτίδων κρέατος (Cyber-HACCP) σε περίπτωση απόκλισης θερμοκρασίας.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.



Η εικόνα δείχνει με απόλυτη σαφήνεια και καθαρή διάταξη ένα **πρακτικό Checklist Εφαρμογής επτά διακριτών βημάτων για τη θωράκιση των συστημάτων ψύξης σε βιομηχανία επεξεργασίας κρέατος.**

Αρχικά, το διάγραμμα – εικόνα εστιάζει στη δικτυακή ασφάλεια, ορίζοντας τον αυστηρό διαχωρισμό των δικτύων γραφείου (IT*) και παραγωγής (OT*) μέσω βιομηχανικών firewalls*, καθώς και την αποκλειστική δρομολόγηση της επικοινωνίας μεταξύ των δύο εργοστασίων μέσω κρυπτογραφημένου **Site-to-Site VPN***. Στη συνέχεια, συνδυάζει τη φυσική προστασία με την ενεργή επιτήρηση, προτείνοντας την εγκατάσταση αναλογικών θερμοστατών ασφαλείας στα κυκλώματα απόψυξης και τη λειτουργία συστήματος ανίχνευσης ανωμαλιών (OT*-IDS*) για τον έγκαιρο εντοπισμό μαζικών εντολών defrost.

Τέλος, η διαδικασία ολοκληρώνεται με τον έλεγχο πρόσβασης, την επιχειρησιακή ετοιμότητα και την προστασία της δημόσιας υγείας, επιβάλλοντας την **πρόσβαση των εξωτερικών αυτοματιστών μόνο μέσω πλατφόρμας PAM* με MFA*** και **χρονικό περιορισμό**, την **εκπαίδευση των μηχανικών βάρδιας** για άμεση μετάβαση σε χειροκίνητη λειτουργία (Manual Override) εντός 15 λεπτών, καθώς και τη **θέσπιση πρωτοκόλλου καραντίνας παρτίδων κρέατος** (Cyber-HACCP*) σε περίπτωση απόκλισης της θερμοκρασίας.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

ERP* : *Γιατί αφορά την κυβερνοασφάλεια;*
Αν μια κυβερνοεπίθεση (όπως το ransomware) κλειδώσει το ERP, η επιχείρηση «τυφλώνεται» επιχειρησιακά: δεν μπορεί να εκδώσει τιμολόγια, χάνει τα στοιχεία ιχνηλασιμότητας των παρτίδων και σταματά η διακίνηση των προϊόντων στην εφοδιαστική αλυσίδα.*

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Μέρος 3ο : Μικρή Αλυσίδα Super Market



Αρχιτεκτονική «Μηδενικού Ελέγχου Εμπιστοσύνης» (Zero-Trust Architecture**)**

Αφηγηματική προσέγγιση: Σε μια αλυσίδα καταστημάτων, ο μεγαλύτερος κίνδυνος είναι η ταυτόχρονη κατάρρευση όλων των υποκαταστημάτων. Η αρχιτεκτονική σχεδιάζεται ώστε κάθε κατάστημα να λειτουργεί ως απομονωμένο «νησί» (περιορισμός ακτίνας ζημιάς), ενώ ένα ανεξάρτητο ασύρματο δίκτυο αισθητήρων μεταφέρει την πραγματική θερμοκρασία στα κεντρικά, ακόμη κι αν το τοπικό δίκτυο παραβιαστεί.

Αρχιτεκτονική «Μηδενικού Ελέγχου Εμπιστοσύνης» (Zero-Trust Architecture)

Περιγραφή Αρχιτεκτονικής:

- **Απομόνωση Καταστημάτων (Micro-Segmentation / VLANs):** Κάθε υποκατάστημα διαθέτει απομονωμένο υποδίκτυο ψύξης χωρίς δυνατότητα επικοινωνίας μεταξύ καταστημάτων.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- **Κεντρική Διαχείριση Ταυτοτήτων (IAM / RBAC & MFA):** Υποχρεωτικό MFA στο κεντρικό BMS και περιορισμός δικαιωμάτων των τεχνικών ανά γεωγραφική ζώνη.

- **Ανεξάρτητη Τηλεμετρία (LPWAN / NB-IoT Overlay):** Δευτερεύον δίκτυο ασύρματων αισθητήρων θερμοκρασίας (ανεξάρτητο από το τοπικό Wi-Fi/LAN) που στέλνει μετρήσεις απευθείας στο Cloud της διοίκησης.

- **Αυτόνομη Λειτουργία Άκρων (Decoupled Edge Operation):** Οι τοπικοί ελεγκτές διατηρούν τις τελευταίες έγκυρες ρυθμίσεις ψύξης στη μνήμη τους, επιτρέποντας την άμεση φυσική αποσύνδεση από το δίκτυο χωρίς διακοπή της ψύξης.



Η εικόνα αποτυπώνει σε τέσσερις διακριτούς πυλώνες την αρχιτεκτονική «**Μηδενικού Ελέγχου Εμπιστοσύνης**» (Zero-Trust Architecture*), σχεδιασμένη ειδικά για τη **θωράκιση των συστημάτων ψύξης** σε μια μικρή αλυσίδα Super Market.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Στο πρώτο βήμα εφαρμόζεται η απομόνωση των καταστημάτων μέσω μικρο-τμηματοποίησης δικτύου (Micro-Segmentation* / VLANs*), ώστε κάθε υποκατάστημα να διαθέτει το δικό του ανεξάρτητο υποδίκτυο ψύξης χωρίς καμία δυνατότητα οριζόντιας επικοινωνίας μεταξύ των καταστημάτων.

Στο δεύτερο στάδιο, η κεντρική διαχείριση ταυτοτήτων (IAM* / RBAC* & MFA*) επιβάλλει υποχρεωτική επαλήθευση πολλαπλών παραγόντων στο κεντρικό σύστημα διαχείρισης (BMS*) και περιορίζει αυστηρά τα δικαιώματα πρόσβασης των τεχνικών ανά γεωγραφική ζώνη.

Παράλληλα, ο τρίτος πυλώνας εξασφαλίζει την αδιάλειπτη παρακολούθηση μέσω ανεξάρτητης τηλεμετρίας (LPWAN* / NB-IoT* Overlay), αξιοποιώντας ένα δευτερεύον δίκτυο ασύρματων αισθητήρων θερμοκρασίας που παρακάμπτει το τοπικό Wi-Fi/LAN* και στέλνει μετρήσεις απευθείας στο Cloud της διοίκησης.

Τέλος, το τέταρτο στάδιο εγγυάται την επιχειρησιακή συνέχεια μέσω της αυτόνομης λειτουργίας των άκρων (Decoupled Edge Operation*), καθώς οι τοπικοί ελεγκτές διατηρούν στη μνήμη τους τις τελευταίες έγκυρες ρυθμίσεις ψύξης, επιτρέποντας την άμεση φυσική αποσύνδεσή τους από το δίκτυο χωρίς να διακοπεί η συντήρηση των προϊόντων.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Checklist Εφαρμογής :

- Διαμόρφωση ανεξάρτητων VLANs ανά κατάστημα για αποτροπή εξάπλωσης επιθέσεων.
- Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης (MFA) και Role-Based Access (RBAC) στο κεντρικό BMS/SCADA.
- Εγκατάσταση δευτερεύοντος δικτύου ασύρματων αισθητήρων θερμοκρασίας (NB-IoT / LoRaWAN) ανεξάρτητου από το δίκτυο του καταστήματος.
- Ευδιάκριτη σήμανση (κόκκινο ταμπελάκι) στο καλώδιο δικτύου των ψυγείων στο rack κάθε καταστήματος για άμεση αποσύνδεση σε κρίση.
- Ρύθμιση αυτόματων alerts (SMS/Email) αν ενεργοποιηθεί *defrost* σε πολλά ψυγεία ταυτόχρονα ή εκτός ωραρίου.
- Συμφωνία ετοιμότητας με εταιρείες ψυγείων μεταφοράς για άμεση εκκένωση ευπαθών αποθεμάτων.



Η εικόνα αποτυπώνει με απόλυτη σαφήνεια ένα πρακτικό Checklist Εφαρμογής έξι βημάτων, ειδικά σχεδιασμένο για τη θωράκιση των συστημάτων ψύξης και την επιχειρησιακή συνέχεια σε μια μικρή αλυσίδα Super Market.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Αρχικά, το διάγραμμα εστιάζει στη δικτυακή απομόνωση και τον έλεγχο πρόσβασης, ορίζοντας τη διαμόρφωση ανεξάρτητων VLANs* ανά κατάστημα για την αποτροπή εξάπλωσης επιθέσεων, καθώς και την ενεργοποίηση πολυπαραγοντικής αυθεντικοποίησης (MFA*) και ελέγχου πρόσβασης βάσει ρόλων (RBAC*) στο κεντρικό σύστημα BMS/SCADA*.
Στη συνέχεια, η προσοχή στρέφεται στην ανεξάρτητη επιτήρηση και την άμεση φυσική αντίδραση, μέσα από την εγκατάσταση ενός δευτερεύοντος δικτύου ασύρματων αισθητήρων θερμοκρασίας (NB-IoT / LoRaWAN*) ανεξάρτητου από το τοπικό δίκτυο, αλλά και την τοποθέτηση ευδιάκριτης σήμανσης (κόκκινο ταμπελάκι) στο καλώδιο δικτύου των ψυγείων στο rack κάθε καταστήματος για ακαριαία αποσύνδεση σε περίπτωση κρίσης.
Τέλος, η θωράκιση ολοκληρώνεται με τη ρύθμιση αυτόματων ειδοποιήσεων (SMS/Emai*l) σε περίπτωση μαζικής ή εκτός ωραρίου ενεργοποίησης του -defrost-, καθώς και τη σύναψη συμφωνίας ετοιμότητας με εταιρείες ψυγείων μεταφοράς για την άμεση εκκένωση και διάσωση των ευπαθών αποθεμάτων.



Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

4. Βασικοί Δείκτες Απόδοσης (KPIs) Κυβερνοασφάλειας

Για τη συνεχή αξιολόγηση της ετοιμότητας των εγκαταστάσεων παρακολουθούνται οι εξής μετρήσιμοι δείκτες (Key Performance Indicators):

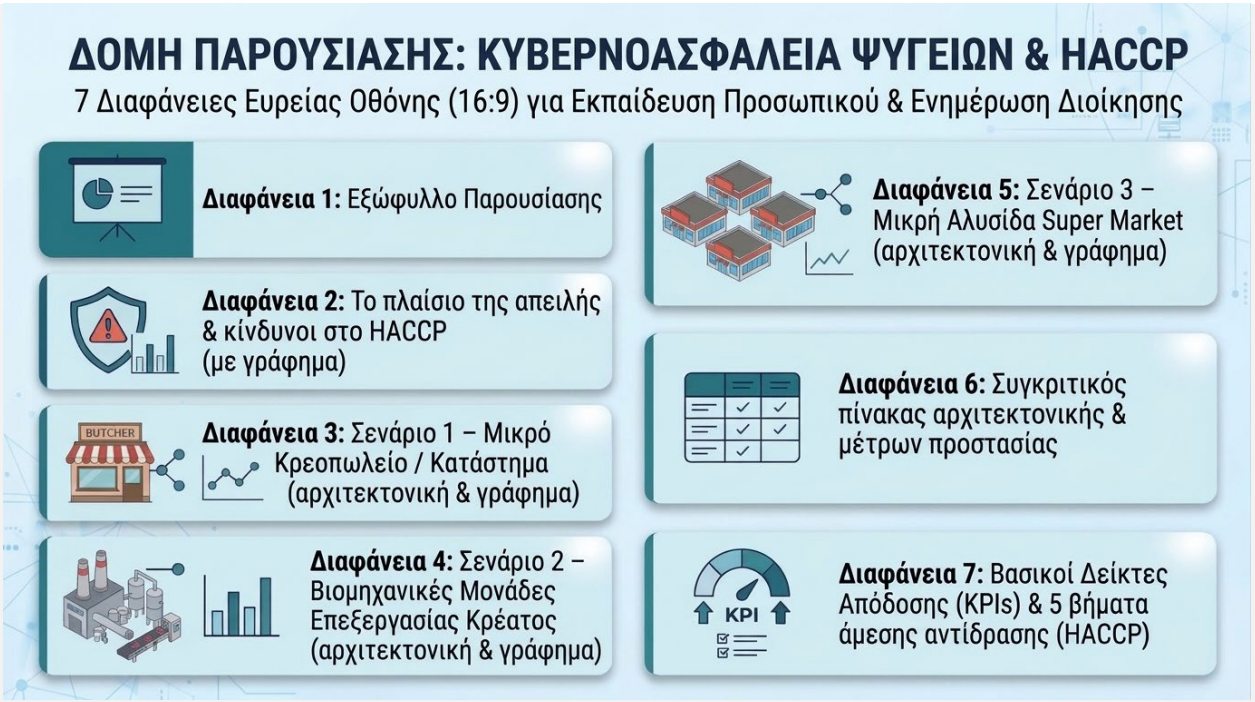
1. MTTD (Mean Time to Detect):
Μέσος χρόνος εντοπισμού μη εξουσιοδοτημένης αλλαγής θερμοκρασίας ή εντολής defrost.

2. MTTR (Mean Time to Recover):
Μέσος χρόνος απομόνωσης του δικτύου και επαναφοράς της ψύξης σε ασφαλή λειτουργία.

3. False Negative Rate (Για συστήματα HACCP-AI): Ποσοστό πραγματικών υγειονομικών αποκλίσεων που δεν ανιχνεύθηκαν λόγω αλλοίωσης δεδομένων (Data Poisoning).

4. Out-of-Band Alerting Uptime: Ποσοστό διαθεσιμότητας των ανεξάρτητων αισθητήρων (SIM / NB-IoT) σε σχέση με το κύριο δίκτυο.

5. Patch & Password Compliance Rate: Ποσοστό ελεγκτών που διαθέτουν ενημερωμένο λογισμικό και μη-εργοστασιακούς κωδικούς πρόσβασης.



Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Η εικόνα παρουσιάζει μια ολοκληρωμένη και λογικά δομημένη πρόταση παρουσίασης 7 διαφανειών με θέμα τη κυβερνοασφάλεια ψυγείων και τα συστήματα HACCP.
Η παρουσίαση της εικόνας ξεκινά με το εισαγωγικό εξώφυλλο και προχωρά στη θεμελίωση του προβλήματος, αναλύοντας στη δεύτερη διαφάνεια το πλαίσιο των κυβερνοαπειλών και τους κινδύνους που ελλοχεύουν για την ασφάλεια των τροφίμων. Στη συνέχεια, η δομή κλιμακώνεται έξυπνα σε επίπεδο πολυπλοκότητας, παρουσιάζοντας τρία ρεαλιστικά σενάρια εφαρμογής, ξεκινώντας από ένα μικρό κρεοπωλείο, περνώντας σε μεγάλες βιομηχανικές μονάδες επεξεργασίας κρέατος και καταλήγοντας σε μια μικρή αλυσίδα σούπερ μάρκετ, συνοδεύοντας κάθε περίπτωση με την αντίστοιχη αρχιτεκτονική και γραφήματα.
Η παρουσίαση ολοκληρώνεται με πρακτικό και στρατηγικό προσανατολισμό, προσφέροντας αρχικά έναν συγκριτικό πίνακα αρχιτεκτονικής και μέτρων προστασίας που βοηθά τη διοίκηση στη λήψη αποφάσεων. Στην τελευταία διαφάνεια, αφορά μετρήσιμους **δείκτες απόδοσης** (KPIs) και πέντε συγκεκριμένα βήματα άμεσης αντίδρασης, συνδέοντας, έτσι, τη θεωρητική ενημέρωση με την επιχειρησιακή ετοιμότητα του προσωπικού

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

ΕΝΤΥΠΟ ΚΑΤΑΓΡΑΦΗΣ ΚΥΒΕΡΝΟ-ΠΕΡΙΣΤΑΤΙΚΟΥ & ΔΙΑΧΕΙΡΙΣΗΣ ΑΠΟΚΛΙΣΗΣ ΨΥΞΗΣ (CYBER-HACCP)

Παράρτημα Αρχείου Ασφάλειας Τροφίμων (ISO 22000 / HACCP)

1. ΣΤΟΙΧΕΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ & ΕΝΤΟΠΙΣΜΟΥ ΠΕΡΙΣΤΑΤΙΚΟΥ

Επωνυμία Επιχείρησης / Καταστήματος: _____	**Εγκατάσταση / Μονάδα / Υποκατάστημα:** _____
Ημερομηνία & Ώρα Εντοπισμού: _____	**Εκτιμώμενη Ώρα Έναρξης Ανωμαλίας:** _____
Ονοματεπώνυμο Υπευθύνου Καταγραφής: _____	**Θέση / Ρόλος (π.χ. Υπ. Ποιότητας, Δ/ντής):** _____

2. ΦΥΣΗ ΚΥΒΕΡΝΟ-ΠΕΡΙΣΤΑΤΙΚΟΥ & ΕΠΗΡΕΑΖΟΜΕΝΑ ΣΥΣΤΗΜΑΤΑ

Τύπος Εντοπισμένης Ανωμαλίας (Σημειώστε ☑ όσα ισχύουν):

☐ Μη εξουσιοδοτημένη ενεργοποίηση απόψυξης (Defrost) ☐ Απενεργοποίηση / Σίγαση συναγερμών ψύξης

☐ Αλλοίωση ορίων θερμοκρασίας (Setpoints) ☐ Απώλεια επικοινωνίας / Κλείδωμα SCADA-BMS (Ransomware)

☐ Αλλοίωση δεδομένων αισθητήρων (Data Poisoning) ☐ Άλλο: _____

Μέσο Εντοπισμού:

☐ Ανεξάρτητος αισθητήρας (SIM / NB-IoT / LoRaWAN) ☐ Σύστημα ανίχνευσης OT-IDS / SOC ☐ Φυσικός έλεγχος προσωπικού ☐ Άλλο: _____

Επηρεαζόμενοι Ψυκτικοί Θάλαμοι / Βιτρίνες / Γραμμές Παραγωγής (Κωδικοί & Περιγραφή):

_____

3. ΚΑΤΑΓΡΑΦΗ ΘΕΡΜΟΚΡΑΣΙΩΝ & ΕΠΗΡΕΑΖΟΜΕΝΩΝ ΠΑΡΤΙΔΩΝ (CCP)

Θάλαμος / Ψυγείο	Είδος Προϊόντος & Αρ. Παρτίδας (Lot)	Κρίσιμο Όριο HACCP (°C)	Μέγιστη Θερμ. που Καταγράφη	Διάρκεια Απόκλισης

4. ΑΜΕΣΕΣ ΕΝΕΡΓΕΙΕΣ ΑΝΑΧΑΙΤΙΣΗΣ & ΔΙΟΡΘΩΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ

Τεχνικές & Επιχειρησιακές Ενέργειες που Εκτελέστηκαν (Σημειώστε ☑):

☐ Φυσική αποσύνδεση καλωδίου δικτύου (LAN/WAN) / Wi-Fi ☐ Μετάβαση ψυκτικών συγκροτημάτων σε Manual Override

☐ Δέσμευση & σήμανση επηρεαζόμενων παρτίδων (Καραντίνα) ☐ Μεταφορά ευπαθών αποθεμάτων σε εφεδρικούς θαλάμους

☐ Ειδοποίηση Ομάδας IT / Τεχνικού Ψύξης / Διοίκησης ☐ Δειγματοληψία για εργαστηριακό / μικροβιολογικό έλεγχο

Συμπληρωματικές Παρατηρήσεις / Μέτρα Αποτροπής Επανεμφάνισης (Αλλαγή κωδικών, Firmware update, Αναφορά NIS2/ΕΑΚ):

_____

_____

5. ΕΠΑΛΗΘΕΥΣΗ ΑΠΟΚΑΤΑΣΤΑΣΗΣ & ΥΠΟΓΡΑΦΕΣ ΕΓΚΡΙΣΗΣ

Υπεύθυνος Εντοπισμού / Βάρδιας	Υπεύθυνος Τεχνικής Υποστήριξης / IT	Υπεύθυνος Ασφάλειας Τροφίμων (HACCP)
Ονομ/μο: _____	Ονομ/μο: _____	Ονομ/μο: _____
Ημ/νία & Ώρα: _____	Ημ/νία & Ώρα: _____	Ημ/νία & Ώρα: _____
Υπογραφή: _____	Υπογραφή: _____	Υπογραφή: _____

Αποποίηση ευθύνης :

Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

ΓΙΑΤΙ Η ΚΥΒΕΡΝΟ-ΑΠΕΙΛΗ ΑΦΟΡΑ ΕΞΙΣΟΥ ΜΙΚΡΕΣ ΚΑΙ ΜΕΓΑΛΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Τύπος Επιχείρησης	Κύριο Σημείο Ευπάθειας	Μηχανισμός Επίθεσης	Κρίσιμες Επιπτώσεις
 **Μικρό Κρεοπωλείο**	Απλός ελεγκτής ψυγείου συνδεδεμένος στο router με εργοστασιακούς κωδικούς (0000, admin).	Απομακρυσμένη παραβίαση (hacking) και ενεργοποίηση απόψυξης (defrost) ή απενεργοποίηση ψύξης.	Ολική καταστροφή του εμπορεύματος μέσα σε μία νύχτα και άμεση οικονομική ζημιά.
 **Βιομηχανικές Μονάδες Επεξεργασίας Κρέατος**	Διασύνδεση γραμμών παραγωγής (IT/OT) και βιομηχανικών συστημάτων ψύξης (SCADA/PLCs).	Εισβολή στο βιομηχανικό δίκτυο, αλλοίωση εντολών ψύξης και σίγαση συναγερμών.	Μαζική αλλοίωση παρτίδων, διακοπή παραγωγής, κίνδυνος βιομηχανικού ατυχήματος ή πυρκαγιάς λόγω υπερθέρμανσης.
 **Αλυσίδα Super Market**	Κεντρική διαχείριση (BMS) δεκάδων διασυνδεδεμένων καταστημάτων.	Πολλαπλασιαστική επίθεση (ένα κενό ασφαλείας «ρίχνει» τα ψυγεία σε όλο το δίκτυο ταυτόχρονα).	Ανυπολόγιστη οικονομική ζημιά και σοβαρός κίνδυνος δημόσιας υγείας (προϊόντα που αποψύχθηκαν και επανακαταψύχθηκαν κρυφά).

Βασικό συμπέρασμα: Η κυβερνοασφάλεια δεν είναι πλέον υπόθεση μόνο των ειδικών της πληροφορικής (**IT**). Αποτελεί αναπόσπαστο κομμάτι της **ασφάλειας τροφίμων (Cyber-HACCP*)**, της επιχειρησιακής συνέχειας και της προστασίας του καταναλωτή.

«Η απειλή είναι κοινή, αλλά ο τρόπος που την αντιμετωπίζουμε δεν μπορεί να είναι ίδιος για όλους. Ένα συνοικιακό κρεοπωλείο δεν έχει ούτε τους ίδιους πόρους, ούτε την ίδια υποδομή με ένα βιομηχανικό εργοστάσιο ή μια αλυσίδα καταστημάτων.
Γι' αυτό, στη συνέχεια, θα εξετάσουμε **τρία διαφορετικά, ρεαλιστικά σενάρια** προστασίας, προσαρμοσμένα ακριβώς στις ανάγκες και την κλίμακα της κάθε επιχείρησης:

- Πρώτον, πώς θωρακίζουμε άμεσα και με ελάχιστο κόστος ένα **μικρό κρεοπωλείο**.
- Δεύτερον, πώς "χτίζεται" βιομηχανική άμυνα σε **δύο διασυνδεδεμένες μονάδες επεξεργασίας κρέατος**.
- Πώς προστατεύεται ένα δίκτυο καταστημάτων σε μια **μικρή αλυσίδα super market**, ώστε μια επίθεση σε ένα σημείο να μην εξαπλωθεί στα υπόλοιπα.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

ΠΑΡΑΡΤΗΜΑ :

Γλωσσάρι - Ερμηνεία τεχνικών όρων (εργαλεία εντιπισμού και αντιμετώπισης κυβερνο-απειλών

Cyber-HACCP *: δεν είναι επίσημος όρος του **NIST SP 800-82**, αλλά μια μεθοδολογική προσέγγιση στην **βιομηχανία τροφίμων και ποτών (Food & Beverage),** που "παντρεύει" τις αρχές ασφάλειας τροφίμων (**HACCP**) **με τις πρακτικές κυβερνοασφάλειας συστημάτων OT/ICS** (όπως ορίζονται στο NIST SP 800-82).
Ουσιαστικά, αναγνωρίζει ότι στη σύγχρονη αυτοματοποιημένη παραγωγή, μια **κυβερνοεπίθεση** ή αλλοίωση ψηφιακών δεδομένων μπορεί να προκαλέσει άμεσο **κίνδυνο στη δημόσια υγεία και την ασφάλεια των τροφίμων** (π.χ. αλλαγή θερμοκρασιών παστερίωσης, λανθασμένη δοσολογία χημικών/συντηρητικών).

Σύνδεση Cyber-HACCP με το NIST SP 800-82
Το NIST SP 800-82 εστιάζει στη διαχείριση κινδύνου με βάση τις **φυσικές συνέπειες** (consequence-driven risk management). Στον κλάδο των τροφίμων, αυτό μεταφράζεται στην προστασία των Κρίσιμων Σημείων Ελέγχου (CCPs):

- **Ανάλυση Κινδύνων (Hazard Analysis -> Cyber Risk Assessment).** Όπως το HACCP εντοπίζει βιολογικούς, χημικούς και φυσικούς κινδύνους, το **Cyber-HACCP** (ακολουθώντας το NIST SP 800-82) εντοπίζει ψηφιακές απειλές που μπορούν να αλλοιώσουν τις παραμέτρους παραγωγής (π.χ. παραβίαση PLC ή αισθητήρων θερμοκρασίας).
- **Κρίσιμα Σημεία Ελέγχου (CCPs -> Critical OT Assets).** Τα συστήματα που ελέγχουν κρίσιμες διαδικασίες (π.χ. ψύξη, αποστείρωση, ανάμειξη) ταξινομούνται ως υψηλής κρισιμότητας και απομονώνονται αυστηρά (Network Segmentation / Zones) από το εταιρικό δίκτυο (IT) και το διαδίκτυο.
- **Ακεραιότητα Δεδομένων και Παρακολούθηση (Monitoring & Logging).** Οι αυτοματοποιημένοι καταγραφείς (digital thermometers, SCADA historians) που αποδεικνύουν τη συμμόρφωση με το HACCP προστατεύονται από μη εξουσιοδοτημένες αλλαγές (tampering), διασφαλίζοντας την ιχνηλασιμότητα (traceability).
- **Διορθωτικές Ενέργειες (Corrective Actions -> Incident Response).** Όταν εντοπιστεί κυβερνοπεριστατικό σε γραμμή παραγωγής, το σχέδιο απόκρισης (Incident Response Plan) περιλαμβάνει άμεση καραντίνα της παρτίδας τροφίμων μέχρι να επιβεβαιωθεί η ασφάλειά της.

Ελεγκτές εμπορικής ψύξης* : ψηφιακές μονάδες που ρυθμίζουν τη θερμοκρασία, τον συμπιεστή, τους κύκλους απόψυξης (defrost) και τους συναγερμούς των ψυγείων. Παρότι οι ίδιες οι συσκευές είναι αξιόπιστες, η λανθασμένη διασύνδεσή τους στο διαδίκτυο (χωρίς VPN και με διατήρηση εργοστασιακών κωδικών όπως `0000` ή `1234`) επιτρέπει στους επιτιθέμενους να αποκτήσουν απομακρυσμένο έλεγχο, να ενεργοποιήσουν την απόψυξη εκτός προγράμματος και να απενεργοποιήσουν τις ειδοποιήσεις κινδύνου.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

LAN* : Στο πλαίσιο του **NIST SP 800-82**, το LAN (**L**ocal **A**rea **N**etwork) δεν αντιμετωπίζεται ως ένα ενιαίο, επίπεδο δίκτυο (flat network), αλλά ως μια **αυστηρά τμηματοποιημένη αρχιτεκτονική** (segmented architecture) που διαχωρίζει τα επιχειρηματικά συστήματα (IT) από τα συστήματα ελέγχου (OT), καθώς και τα επιμέρους επίπεδα του ίδιου του OT.

Το πρότυπο βασίζεται στο μοντέλο Purdue (Purdue Enterprise Reference Architecture) για να ορίσει πώς πρέπει να δομείται το LAN.

Ethernet/Wi-Fi* : Σύμφωνα με το **NIST SP 800-82**, η επιλογή και η ασφαλής χρήση μεταξύ **Ethernet (ενσύρματο)** και **Wi-Fi (ασύρματο)** σε περιβάλλοντα Operational Technology (OT) διέπεται από την αρχή της **μέγιστης αξιοπιστίας και ελέγχου πρόσβασης**.Το πρότυπο αντιμετωπίζει τα ενσύρματα δίκτυα ως τη βασική υποδομή για κρίσιμες λειτουργίες, ενώ για τα ασύρματα θέτει αυστηρές προϋποθέσεις πριν την υιοθέτησή τους

Guest Wi-Fi* : Στο πλαίσιο του **NIST SP 800-82**, ένα δίκτυο **Guest Wi-Fi** (ασύρματο δίκτυο επισκεπτών/εργολάβων) αντιμετωπίζεται ως μη έμπιστη ζώνη που πρέπει να παραμένει **απολύτως απομονωμένη** από τα συστήματα Operational Technology (OT). [https://nhimg.org/faq/what-is-the-difference-between-network-segmentation-and-simple-wi-fi-password-pr/]

Αν και το SP 800-82 δεν αποτελεί εγχειρίδιο ρύθμισης εταιρικών Wi-Fi (για τα οποία το NIST παραπέμπει σε εξειδικευμένα πρότυπα όπως το NIST SP 800-97), οι βασικές αρχές αρχιτεκτονικής του επιβάλλουν αυστηρούς κανόνες όταν υπάρχει ασύρματη πρόσβαση επισκεπτών σε εγκαταστάσεις με βιομηχανικά συστήματα ή αυτοματισμούς κτιρίων.

Το **ERP*** **(**Enterprise Resource Planning – Σχεδιασμός Επιχειρησιακών Πόρων**)** είναι το κεντρικό λογισμικό διαχείρισης μιας επιχείρησης που ενοποιεί όλες τις καθημερινές της λειτουργίες σε μία ενιαία βάση δεδομένων.
Στη βιομηχανία τροφίμων, το ERP αποτελεί τον «εγκέφαλο» της διοίκησης (κομμάτι του **IT**) και διαχειρίζεται:

- **Αποθήκη & Αποθέματα:** Ποιες πρώτες ύλες υπάρχουν, πότε λήγουν (FIFO/FEFO) και πόσα έτοιμα προϊόντα είναι έτοιμα προς αποστολή.
- **Ιχνηλασιμότητα (Traceability):** Κρίσιμο κομμάτι για το HACCP — καταγράφει από ποιον προμηθευτή ήρθε η κάθε παρτίδα κρέατος, σε ποια γραμμή επεξεργάστηκε και σε ποιο super market στάλθηκε.
- **Παραγγελίες & Πωλήσεις:** Τιμολόγηση, διαχείριση πελατών και προμηθευτών.
- **Προγραμματισμός Παραγωγής:** Πόσες ποσότητες πρέπει να παραχθούν ανάλογα με τη ζήτηση.
- **Οικονομικά & Λογιστήριο:** Έσοδα, έξοδα, κοστολόγηση προϊόντων και μισθοδοσία.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

IT* **(Τεχνολογία Πληροφορικής):** Αφορά τα συστήματα που διαχειρίζονται **δεδομένα και πληροφορίες**. Περιλαμβάνει τους υπολογιστές γραφείου, τους servers, τα εταιρικά δίκτυα, τα emails, τα λογισμικά διαχείρισης (ERP) και τις βάσεις δεδομένων της επιχείρησης.

OT* **(Επιχειρησιακή Τεχνολογία-Operational Technology):** είναι το σύνολο του υλικού (hardware) και του λογισμικού (software), που παρακολουθεί, ελέγχει και διαχειρίζεται **βιομηχανικές διεργασίες** σε πραγματικό χρόνο στην παραγωγή.
Ειδικότερα , στη βιομηχανία τροφίμων και το **HACCP**, περιλαμβάνει τους αισθητήρες θερμοκρασίας, τους ελεγκτές ψυκτικών θαλάμων (**PLCs**), τις γραμμές παραγωγής, τις συσκευαστικές μηχανές και τα αυτοματοποιημένα καταγραφικά, **συμπιεστές, τις βαλβίδες και τα συστήματα SCADA*/BMS***.

Σημ. : «τμηματοποίηση δικτύου OT/IT»
Παλαιότερα, τα δύο αυτά δίκτυα ήταν εντελώς ξεχωριστά. Σήμερα, όμως, συνδέονται μεταξύ τους (π.χ. για να στέλνει ένας αισθητήρας θερμοκρασίας δεδομένα στο σύστημα του γραφείου). ***Αν δεν υπάρχει τμηματοποίηση (διαχωρισμός)****, ένας* ***χάκερ*** *που θα παραβιάσει ένα απλό εταιρικό email (IT) μπορεί να «πηδήξει» στο δίκτυο παραγωγής (OT) και να αλλοιώσει τις θερμοκρασίες των ψυγείων ή να σταματήσει τη γραμμή παραγωγής.*

Το **POS*** **(Point of Sale – Σημείο Πώλησης)** είναι το σύστημα υλικού και λογισμικού που χρησιμοποιείται στα καταστήματα και τις επιχειρήσεις (π.χ. σούπερ μάρκετ, κρεοπωλεία, εστιατόρια, λιανεμπόριο) για την ολοκλήρωση των εμπορικών συναλλαγών, την έκδοση αποδείξεων/τιμολογίων, τη διαχείριση αποθεμάτων και την αποδοχή πληρωμών με κάρτα (τερματικά EFT/POS).
Στο πλαίσιο της **κυβερνοασφάλειας μιας εγκατάστασης ψύξης**, το POS αναφέρεται ως το **πιο ευάλωτο και εκτεθειμένο τμήμα του εταιρικού δικτύου** και για αυτόν τον λόγο απαιτείται αυστηρός διαχωρισμός (Network Segmentation) από τα ψυγεία.

- **PCI Security Standards Council (PCI DSS):** Ο διεθνής οργανισμός που ορίζει τα αυστηρά πρότυπα ασφαλείας για την απομόνωση και προστασία των τερματικών και δικτύων POS.
- **Stouffer et al. (2023) – NIST SP 800-82 Rev. 3:** Αναλύει την αναγκαιότητα διαχωρισμού των εταιρικών δικτύων (IT / POS) από τα βιομηχανικά δίκτυα ελέγχου (OT / Ψύξη).

* **VPN Server (Εξυπηρετητής Εικονικού Ιδιωτικού Δικτύου) :** εξειδικευμένος υπολογιστής ή λογισμικό που λειτουργεί ως **ασφαλής «πύλη εισόδου»** σε ένα τοπικό δίκτυο (όπως το δίκτυο μιας επιχείρησης ή μιας εγκατάστασης ψύξης) μέσω του διαδικτύου.
Αντί να παραμένουν οι συσκευές (π.χ. ελεγκτές θερμοκρασίας, κάμερες, υπολογιστές) εκτεθειμένες απευθείας στο ανοιχτό ίντερνετ, ο VPN Server δημιουργεί ένα **κρυπτογραφημένο «τούνελ»** μεταξύ της συσκευής του χρήστη (π.χ. του τεχνικού) και του τοπικού δικτύου.

Στην πράξη λειτουργεί για :

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- **Αυθεντικοποίηση (Ελεγχος Ταυτότητας):** Όταν ένας τεχνικός θέλει να ελέγξει τα ψυγεία από απόσταση, συνδέεται πρώτα στον VPN Server* δίνοντας κωδικούς και ψηφιακά πιστοποιητικά. Αν δεν έχει άδεια, ο server απορρίπτει τη σύνδεση.
- **Κρυπτογράφηση (Προστασία Δεδομένων):** Όλα τα δεδομένα και οι εντολές (π.χ. αλλαγή θερμοκρασίας) κλειδώνονται με ισχυρή κρυπτογράφηση (όπως AES-256*). Ακόμα κι αν κάποιος υποκλέψει τη σύνδεση, βλέπει μόνο ακατανόητους κωδικούς.
- **Ασφαλής Πρόσβαση στο Εσωτερικό Δίκτυο:** Μόλις επιβεβαιωθεί η σύνδεση, ο VPN Server* επιτρέπει στον τεχνικό να επικοινωνήσει με το απομονωμένο δίκτυο των ψυγείων (VLAN) σαν να βρισκόταν φυσικά μέσα στο κτίριο.

VPN Server* είναι κρίσιμος για την κυβερνοασφάλεια

- **Κρύβει τις ευαίσθητες συσκευές:** Οι **ελεγκτές ψύξης** (PLCs) **δεν φαίνονται καθόλου στο δημόσιο ίντερνετ**, αποτρέποντας αυτοματοποιημένες κυβερνοεπιθέσεις.
- **Αποτρέπει τις παραβιάσεις εντολών:** Εξασφαλίζει ότι κανένας εξωτερικός εισβολέας δεν μπορεί να στείλει ψεύτικες εντολές (π.χ. απενεργοποίηση ψύξης ή παρατεταμένο defrost).
- **Καταγράφει ποιος μπήκε και πότε:** Κρατάει ιστορικό συνδέσεων, ώστε να είναι γνωστό ανά πάσα στιγμή ποιος τεχνικός συνδέθηκε στο σύστημα.

Site-to-Site VPN* : Το Site-to-Site VPN (Virtual Private Network – Εικονικό Ιδιωτικό Δίκτυο) είναι μια ασφαλής, κρυπτογραφημένη «σήραγγα» (tunnel) επικοινωνίας μέσω του κοινού διαδικτύου, η οποία συνδέει μόνιμα τα τοπικά δίκτυα δύο ή περισσότερων διαφορετικών εγκαταστάσεων (π.χ. δύο εργοστασίων ή των κεντρικών γραφείων με τα υποκαταστήματα), κάνοντάς τα να λειτουργούν σαν να βρίσκονται στον ίδιο χώρο.

Στη βιομηχανία επεξεργασίας κρέατος και στις αλυσίδες Super Markets, αποτελεί τον ενδεδειγμένο τρόπο για την ανταλλαγή δεδομένων παραγωγής, θερμοκρασιών ψύξης και αποθεμάτων μεταξύ απομακρυσμένων μονάδων, χωρίς να εκτίθενται ευαίσθητα συστήματα στο ανοιχτό ίντερνετ.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

LoRaWAN* (Long Range Wide Area Network- Δίκτυο Ευρείας Περιοχής Μεγάλης Εμβέλειας) : ασύρματο πρωτόκολλο επικοινωνίας χαμηλής κατανάλωσης ενέργειας και μεγάλης εμβέλειας, ιδανικό για αισθητήρες IoT σε ψυκτικούς θαλάμους και βιομηχανικές εγκαταστάσεις.

Στο πλαίσιο της κυβερνοασφάλειας και της παράλληλης εποπτείας (Out-of-Band Monitoring) που εξετάζουμε, το **LoRaWAN*** αποτελεί εξαιρετική εναλλακτική ή συμπλήρωμα των αισθητήρων SIM* / NB-IoT*.

LoRaWAN* : Πώς εντάσσεται στην Αρχιτεκτονική Ασφαλείας

- **Διαθέτει Πλήρη Ανεξαρτησία από το Τοπικό Δίκτυο** (Out-of-Band)**:** Οι **αισθητήρες** θερμοκρασίας LoRaWAN* δεν συνδέονται στο εταιρικό Wi-Fi , ούτε στο **δίκτυο** των **ελεγκτών** (SCADA/VLAN). Επικοινωνούν ασύρματα σε ειδική συχνότητα (868 MHz στην Ευρώπη) με έναν δικό τους δέκτη (**LoRaWAN Gateway**), ο οποίος μπορεί να έχει δική του κάρτα SIM (4G/5G) για αποστολή δεδομένων στο cloud.

- **Διπλή Κρυπτογράφηση** (End-to-End Security)**:** Το πρωτόκολλο **LoRaWAN*** διαθέτει ενσωματωμένη κρυπτογράφηση **AES-128*** σε δύο επίπεδα:
  - **Network Session Key:** Εξασφαλίζει την αυθεντικότητα του αισθητήρα στο δίκτυο.
  - **Application Session Key:** Κρυπτογραφεί τα ίδια τα δεδομένα (τη θερμοκρασία), ώστε κανείς ενδιάμεσος να μην μπορεί να τα διαβάσει ή να τα αλλοιώσει (**αποτροπή Data Poisoning**).

- **Διείσδυση σε Ψυκτικούς Θαλάμους:** Σε αντίθεση με το **Wi-Fi,** που δυσκολεύεται να περάσει μέσα από χοντρά μονωτικά τοιχώματα ψυγείων και μεταλλικές πόρτες, το **σήμα LoRaWAN** έχει εξαιρετική διεισδυτικότητα και εμβέλεια χιλιομέτρων.

- **Αυτονομία Μπαταρίας Ετών:** Λόγω ελάχιστης κατανάλωσης, οι αισθητήρες λειτουργούν με μπαταρία για 3 έως 5 χρόνια, συνεχίζοντας να καταγράφουν και να στέλνουν ειδοποιήσεις ακόμα και σε περίπτωση γενικής διακοπής ρεύματος (εφόσον το Gateway έχει μικρό UPS).

Αισθητήρες Θερμοκρασίας (LoRaWAN / NB-IoT*): Τα δεδομένα θερμοκρασίας που στέλνουν οι ανεξάρτητοι αισθητήρες στο Cloud κρυπτογραφούνται με **AES-128***, ώστε κανείς να μην μπορεί να υποκλέψει ή να παραποιήσει τις ενδείξεις (Data Poisoning).

Το **NB-IoT* (Narrowband Internet of Things)** είναι μια εξειδικευμένη τεχνολογία ασύρματης επικοινωνίας κινητής τηλεφωνίας (**4G/5G**), σχεδιασμένη ειδικά για **αισθητήρες και συσκευές IoT** που χρειάζεται να στέλνουν μικρό όγκο δεδομένων (όπως μετρήσεις θερμοκρασίας και υγρασίας) με ελάχιστη κατανάλωση ενέργειας και πολύ μεγάλη εμβέλεια.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

DMZ*: **(Demilitarized Zone – Αποστρατιωτικοποιημένη Ζώνη)** είναι ένα απομονωμένο υποδίκτυο , που λειτουργεί ως **«ουδέτερη ζώνη» ή προθάλαμος ασφαλείας** ανάμεσα στο εταιρικό **δίκτυο (IT)** και το **δίκτυο παραγωγής (OT**).

MFA* (Multi-Factor Authentication – Πολυπαραγοντική Ταυτοποίηση) είναι μια μέθοδος ασφαλείας που απαιτεί από τον χρήστη να αποδείξει την ταυτότητά του με **δύο ή περισσότερους διαφορετικούς τρόπους,** πριν αποκτήσει πρόσβαση σε ένα σύστημα, λογισμικό ή μηχάνημα.

Πηγές πληροφόρησης :

– ***LoRa Alliance® – Επίσημη Ιστοσελίδα:*** *Ο οργανισμός που εκδίδει τις προδιαγραφές (specifications) και πιστοποιεί τις συσκευές LoRaWAN.*
– ***LoRaWAN® Technical Specifications:*** *Τα επίσημα τεχνικά εγχειρίδια του πρωτοκόλλου (όπως το LoRaWAN Link Layer Specification και οι Regional Parameters για τη ζώνη 868 MHz στην Ευρώπη).*
– ***LoRaWAN® Security Whitepaper (LoRa Alliance):*** *Η επίσημη τεχνική έκθεση που αναλύει την αρχιτεκτονική ασφαλείας, την αμοιβαία αυθεντικοποίηση (Mutual Authentication) και την κρυπτογράφηση **AES-128** (Network & Application Session*

NIST SP 800-82 * Το **NIST SP 800-82 (Guide to Operational Technology Security)** : πρότυπο οδηγιών από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) για την κυβερνοασφάλεια των συστημάτων **Operational Technology (OT).**

Το **AES-128*** (Advanced Encryption Standard με κλειδί 128-bit) είναι ένα από τα πιο διαδεδομένα και αξιόπιστα **πρότυπα συμμετρικής κρυπτογράφησης** παγκοσμίως. Χρησιμοποιείται ευρέως για την προστασία δεδομένων κατά τη μεταφορά τους σε δίκτυα (όπως VPN, Wi-Fi, LoRaWAN/NB-IoT αισθητήρες ψύξης) αλλά και κατά την αποθήκευσή τους.

Το **Firmware*** (Ενσωματωμένο Λογισμικό) είναι ένα εξειδικευμένο πρόγραμμα που είναι αποθηκευμένο μόνιμα στη μνήμη του υλικού (hardware) μιας ηλεκτρονικής συσκευής — όπως ένας **ελεγκτής θερμοκρασίας ψυγείου**, ένα **PLC**, ένα **router** ή ένας **αισθητήρας IoT** — και ελέγχει τις βασικές της λειτουργίες.
Με απλά λόγια, το firmware είναι ο **«εγκέφαλος» χαμηλού επιπέδου** της συσκευής: δίνει τις οδηγίες για το πώς θα διαβάσει τον αισθητήρα θερμοκρασίας, πότε θα ενεργοποιήσει τον συμπιεστή, πότε θα ξεκινήσει την απόψυξη (defrost) και πώς θα επικοινωνήσει με το δίκτυο.

MES* (Manufacturing Execution System – Σύστημα Εκτέλεσης Παραγωγής)

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

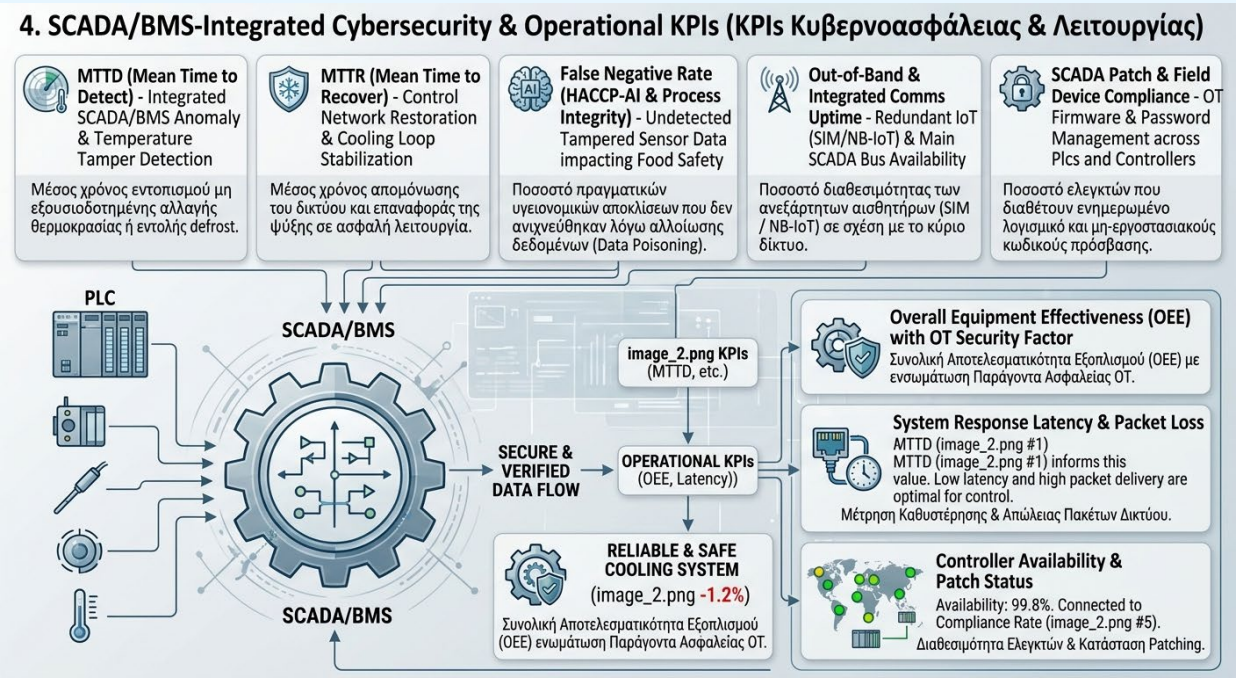
είναι το λογισμικό που λειτουργεί ως ο **«συντονιστής» στον χώρο της παραγωγής** και αποτελεί τη γέφυρα ανάμεσα στο **ERP** (διοίκηση/γραφείο) και το **OT** (μηχανήματα).
Ενώ το ERP λέει **«τι και πόσο»** πρέπει να παραχθεί, το MES αναλαμβάνει το **«πώς και πότε»** γίνεται αυτό στην πράξη, παρακολουθώντας τα πάντα σε πραγματικό χρόνο.

MES* : Τι κάνει στην πράξη στη βιομηχανία τροφίμων

- ***Εκτέλεση Συνταγών & Εντολών:*** *Στέλνει τις ακριβείς παραμέτρους στα μηχανήματα (π.χ. χρόνος ψησίματος/παστερίωσης, θερμοκρασία ψύξης, ποσότητα συστατικών).*
- **Αυτοματοποιημένο HACCP:** Συλλέγει συνεχώς δεδομένα από τους αισθητήρες (OT) και ειδοποιεί αμέσως αν υπάρξει απόκλιση σε κάποιο Κρίσιμο Σημείο Ελέγχου (CCP), μπλοκάροντας αν χρειαστεί την ελαττωματική παρτίδα.
- **Πλήρης Ιχνηλασιμότητα:** Καταγράφει ποιος χειριστής δούλεψε σε ποια βάρδια, ποια μηχανή χρησιμοποιήθηκε και ποια παρτίδα πρώτης ύλης μπήκε σε κάθε τελικό προϊόν.
- **Έλεγχος Απόδοσης (OEE):** Μετράει την ταχύτητα της γραμμής, τις απώλειες (φύρα) και τις καθυστερήσεις των μηχανημάτων

Guest Wi-Fi * (Δίκτυο Επισκεπτών) : είναι ένα ξεχωριστό, απομονωμένο ασύρματο δίκτυο που παρέχει πρόσβαση αποκλειστικά στο διαδίκτυο (Internet) σε εξωτερικούς επισκέπτες, χωρίς να τους επιτρέπει να «δουν» ή να επικοινωνήσουν με τα εσωτερικά δίκτυα της επιχείρησης (**IT** και **OT).**

Scada/BMS*- Integrated Cybersecurity Operational & KPIs (Κυβερνοασφάλειας & Λειτουργίας



Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Phishing* : Το ηλεκτρονικό «ψάρεμα» είναι μια μέθοδος κυβερνοεπίθεσης κατά την οποία οι επιτήδειοι προσποιούνται έναν αξιόπιστο φορέα (όπως την ΑΑΔΕ, μια τράπεζα, έναν πάροχο ενέργειας ή έναν προμηθευτή) για να εξαπατήσουν το θύμα και να υποκλέψουν ευαίσθητα δεδομένα ή χρήματα.

Κακόβουλα USB* : (γνωστά και ως **BadUSB** ή **USB Drops**) είναι τροποποιημένες συσκευές αποθήκευσης που χρησιμοποιούνται για την εκτέλεση κυβερνοεπιθέσεων μόλις συνδεθούν σε έναν υπολογιστή, ένα POS ή ένα βιομηχανικό σύστημα ελέγχου.

Παρότι εξωτερικά μοιάζουν με απλά, ακίνδυνα στικάκια μνήμης, ο εσωτερικός τους μικροελεγκτής έχει επαναπρογραμματιστεί ώστε να ξεγελά το λειτουργικό σύστημα.

Πώς δρουν τα Κακόβουλα USB:

- **Μίμηση Συσκευών (HID Spoofing):** Μόλις συνδεθούν, αναγνωρίζονται από τον υπολογιστή ως πληκτρολόγιο ή ποντίκι. Μέσα σε δευτερόλεπτα, «πληκτρολογούν» αυτόματα κακόβουλες εντολές (scripts) σε ταχύτητα που δεν προλαβαίνει να αντιδράσει ο χρήστης.
- **Εγκατάσταση Κακόβουλου Λογισμικού:** Μπορούν να κατεβάσουν κρυφά ιούς, λογισμικό κατασκοπείας (spyware) ή ransomware που κλειδώνει τα αρχεία και τα συστήματα μιας επιχείρησης.
- **Παράκαμψη Απομόνωσης (Air-Gap Jumping):** Αποτελούν τον κύριο τρόπο προσβολής κρίσιμων υποδομών (όπως ελεγκτές ψύξης, συστήματα παραγωγής ή ταμειακά συστήματα) που δεν είναι συνδεδεμένα στο διαδίκτυο, καθώς το κακόβουλο λογισμικό μεταφέρεται φυσικά από εξωτερικούς τεχνικούς ή ανυποψίαστους υπαλλήλους.
- **Φυσική Καταστροφή (USB Killers):** Ορισμένα ειδικά τροποποιημένα USB συσσωρεύουν ηλεκτρικό φορτίο από τη θύρα και το αποφορτίζουν απότομα, καταστρέφοντας μόνιμα τη μητρική πλακέτα της συσκευής.

Βασικά Μέτρα Προστασίας

- **Μηδενική Εμπιστοσύνη σε Άγνωστα USB:** Ποτέ σύνδεση τυχαίων USB (π.χ. στον χώρο στάθμευσης, σε εκθέσεις ή ως διαφημιστικά δώρα) σε επαγγελματικούς υπολογιστές.
- **Απενεργοποίηση Αυτόματης Εκτέλεσης (AutoRun):** Ρύθμιση λειτουργικά συστήματα ώστε να μην εκτελούν αυτόματα αρχεία από εξωτερικά μέσα.
- **Φυσικό Κλείδωμα Θυρών:** Σε ταμειακές μηχανές, POS και βιομηχανικών ελεγκτών, χρήση φυσικών καλυμμάτων (USB port blockers) ή απενεργοποίηση αχρησιμοποίητων θυρών μέσω λογισμικού.
- **Έλεγχος Εξωτερικών Τεχνικών:** Απαίτηση από τους εξωτερικούς συνεργάτες (π.χ. ψυκτικούς, τεχνικούς ERP/POS) να χρησιμοποιούν μόνο ελεγμένα μέσα αποθήκευσης της επιχείρησης για ενημερώσεις λογισμικού.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

KPIs * : Οι Δείκτες Απόδοσης (– Key Performance Indicators) κυβερνοασφάλειας για τα συστήματα ψύξης στην εφοδιαστική αλυσίδα τροφίμων μετρούν πόσο αποτελεσματικά προστατεύονται οι υποδομές και πόσο γρήγορα αντιδρά η επιχείρηση σε απειλές.

Αισθητήρες IoT* (Internet of Things – Διαδίκτυο των Πραγμάτων) : είναι έξυπνες, διασυνδεδεμένες συσκευές μέτρησης (θερμοκρασίας, υγρασίας, κατανάλωσης ενέργειας ή ανοίγματος θυρών) που συλλέγουν δεδομένα σε πραγματικό χρόνο και τα *αποστέλλουν αυτόματα μέσω διαδικτύου ή τοπικού* δικτύου σε κεντρικά συστήματα παρακολούθησης.

Αρχιτεκτονική «Ψηφιακής Απομόνωσης*- (Air-Gapping & Out-of-Band Monitoring) :

Η Αρχιτεκτονική «Ψηφιακής Απομόνωσης» (Air-Gapping & Out-of-Band Monitoring) είναι ένα μοντέλο κυβερνοασφάλειας που συνδυάζει την πλήρη φυσική αποσύνδεση κρίσιμων συστημάτων από το κύριο δίκτυο με έναν ανεξάρτητο, εξωτερικό μηχανισμό παρακολούθησης.
Είναι η ιδανική και πιο οικονομική στρατηγική προστασίας για μικρές και μεσαίες επιχειρήσεις τροφίμων (όπως συνοικιακά κρεοπωλεία), όπου η πολυπλοκότητα ενός βιομηχανικού δικτύου (IT/OT) δεν είναι απαραίτητη.

Παράλληλη Εποπτεία (Out-of-Band Alerting)* :

Η Παράλληλη Εποπτεία (Out-of-Band Alerting / Monitoring) είναι ένας ανεξάρτητος μηχανισμός παρακολούθησης και ειδοποίησης που λειτουργεί μέσω ενός εντελώς ξεχωριστού καναλιού επικοινωνίας (όπως το δίκτυο κινητής τηλεφωνίας GSM/4G), εκτός του κύριου τοπικού δικτύου και του router της επιχείρησης.
Επιτρέπει στον ιδιοκτήτη ή στον υπεύθυνο ασφαλείας να γνωρίζει ανά πάσα στιγμή την πραγματική κατάσταση των ψυκτικών θαλάμων, ακόμη και όταν το κύριο δίκτυο (IT) έχει καταρρεύσει ή δέχεται κυβερνοεπίθεση.

Αυτόνομο σύστημα τηλεμετρίας * :

Το αυτόνομο σύστημα τηλεμετρίας είναι μια ανεξάρτητη ηλεκτρονική συσκευή μέτρησης και απομακρυσμένης αποστολής δεδομένων (όπως θερμοκρασία, υγρασία και κατάσταση παροχής ρεύματος), η οποία λειτουργεί χωρίς να συνδέεται στο τοπικό δίκτυο (Wi-Fi/LAN) ή το router της επιχείρησης.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Στην προστασία της ψυκτικής αλυσίδας (κρεοπωλεία, βιομηχανίες κρέατος, super markets), αποτελεί τον βασικό εξοπλισμό που υλοποιεί την **Παράλληλη Εποπτεία (Out-of-Band Monitoring)**, λειτουργώντας ως αδιάβλητος, ανεξάρτητος «φύλακας» των ψυκτικών θαλάμων.

Η Λογική Τμηματοποίηση* **(**Logical Network Segmentation**)** είναι η τεχνική διαίρεσης ενός ενιαίου φυσικού δικτύου σε πολλαπλά, ψηφιακά απομονωμένα υποδίκτυα (όπως VLANs* ή Guest Wi-Fi*), ώστε οι συσκευές κάθε ομάδας να μην μπορούν να επικοινωνούν απευθείας με τις συσκευές άλλης ομάδας χωρίς αυστηρό έλεγχο.
Σε αντίθεση με τον φυσικό διαχωρισμό (όπου απαιτούνται ξεχωριστά καλώδια και ξεχωριστοί δρομολογητές), η λογική τμηματοποίηση αξιοποιεί τον υπάρχοντα δικτυακό εξοπλισμό (router, switches, firewalls) για να υψώσει «ψηφιακούς τοίχους» ανάμεσα στα συστήματα μιας επιχείρησης.

Site-to-Site VPN* :

Ανεξάρτητο Σύστημα Συναγερμού (*Out-of-Band Monitoring*)* : Το Ανεξάρτητο Σύστημα

Συναγερμού (Out-of-Band Monitoring / Alerting) είναι ένας αυτόνομος μηχανισμός επιτήρησης και ειδοποίησης έκτακτης ανάγκης, ο οποίος λειτουργεί μέσω ενός εντελώς ξεχωριστού καναλιού επικοινωνίας (όπως το δίκτυο κινητής τηλεφωνίας GSM/4G*), χωρίς καμία εξάρτηση από το τοπικό δίκτυο (Wi-Fi/LAN) ή το router της επιχείρησης.

Αυτόνομο Σύστημα Τηλεμετρίας*: Ανεξάρτητη ηλεκτρονική συσκευή μέτρησης και απομακρυσμένης αποστολής δεδομένων (με ενσωματωμένη κάρτα SIM και εφεδρική μπαταρία), η οποία λειτουργεί εκτός του τοπικού δικτύου (Wi-Fi/LAN) και του router της επιχείρησης, στέλνοντας ειδοποιήσεις SMS ή δεδομένα απευθείας στον ιδιοκτήτη.

NB-IoT / LoRaWAN * : Δίκτυα Ευρείας Περιοχής Χαμηλής Ισχύος): Εξειδικευμένες ασύρματες τεχνολογίες επικοινωνίας μεγάλου βεληνεκούς και χαμηλής κατανάλωσης ενέργειας, σχεδιασμένες για αισθητήρες IoT. Επιτρέπουν σε ασύρματα θερμόμετρα ψυγείων να στέλνουν μετρήσεις απευθείας στο Cloud της διοίκησης (μέσω δικτύων κινητής τηλεφωνίας ή αυτόνομων πυλών), παρακάμπτοντας εντελώς το τοπικό Wi-Fi/LAN του καταστήματος.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Για την εμπέδωση των εννοιών, των **δεικτών (KPIs)** και της βιβλιογραφικής τους τεκμηρίωσης, ακολουθεί μια **συνοπτική χαρτογράφηση (Cheat Sheet)** που συνδέει το «**τι μετράμε**» με το «**ποιο πρότυπο το επιβάλλει**» και «**γιατί έχει κρίσιμη σημασία στην πράξη**»:

Ο Χάρτης των KPIs & Προτύπων (Γρήγορη Ανασκόπηση)

Κατηγορία Άμυνας	Δείκτης (KPI)	Στόχος	Κύριο Πρότυπο	Πρακτική Ουσία
Αρχιτεκτονική & Πρόσβαση	Απομονωμένοι Ελεγκτές Ψύξης	100%	NIST SP 800-82 / IEC 62443-3-3	Αν «πέσει» ένα ταμείο (POS) ή ένα PC γραφείου, ο ιός δεν περνάει στα ψυγεία (OT).
	Εξάλειψη Εργοστασιακών Κωδικών	100%	IEC 62443-4-2 / ENISA IoT	Αποτρέπει αυτοματοποιημένα bots από το να μπουν στους ελεγκτές με default κωδικούς (π.χ. admin/1234).
	Ελεγχόμενες Απομακρυσμένες Συνδέσεις	100%	NIST SP 800-82 / CIS Control 6	Ο εξωτερικός ψυκτικός μπαίνει μόνο με MFA, για συγκεκριμένη ώρα (PAM) και με καταγραφή.
	Περιστατικά Άγνωστων USB	0	IEC 62443-3-3 (SR 2.3)	Κλείνει την πιο κλασική «κερκόπορτα» μόλυνσης βιομηχανικών δικτύων (air-gapped).
Απόκριση & Ανθεκτικότητα	Χρόνος Εντοπισμού (MTTD)	< 5'	ISO/IEC 27035 / MITRE ICS	Εντοπίζει αλλοίωση θερμοκρασίας πριν προλάβει να ξεπαγώσει/αλλοιωθεί το εμπόρευμα.
	Χρόνος Αποκατάστασης (MTTR)	< 15–30'	NIST SP 800-61 / ASHRAE G36	Απομονώνει το παραβιασμένο δίκτυο και επαναφέρει την ψύξη εντός ασφαλούς θερμικού ορίου.
Φυσική Ασφάλεια (Fail-Safe)	Ανεξάρτητη Εποπτεία (SIM / Αναλογικός)	100%	IEC 61511-1 / ISO 22000	Ακόμη κι αν «τυφλωθεί» το ψηφιακό σύστημα, ο αναλογικός θερμοστάτης & το SIM δίνουν συναγερμό.
	Επιτυχία Δοκιμών Αυτονομίας	100%	IEC 61511-1 / NIST CP-4	Εξασφαλίζει ότι το χειροκίνητο manual override δουλεύει πραγματικά σε ώρα κρίσης.
Επιχειρησιακός & Ανθρώπινος Παράγοντας	Απώλειες Εμπορεύματος	0%	Οδηγία NIS2 / N. 5160/2024	Μεταφράζει την κυβερνοασφάλεια σε προστασία εσόδων, αποθεμάτων και δημόσιας υγείας.
	Εκπαίδευση Προσωπικού	> 90%	ISO/IEC 27001 / NIST SP 800-50	Μειώνει την πιθανότητα να πατήσει κάποιος κακόβουλο link (phishing) ή να βάλει ξένο USB.

Σημείωση (*) : Για περισσότερη πληροφόρηση : *αναζήτηση των όρων με τη βοήθεια του βοηθού AI*

(A) Βιβλιογραφικές Αναφορές :

- Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security* (NIST Special Publication 800-55 Rev. 1). National Institute of Standards and Technology.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- de Carvalho Silva, J., Rodrigues, J. J. P. C., Alberti, A. M., Solic, P., & Aquino, A. L. L. (2017). LoRaWAN — A low power WAN protocol for Internet of Things: A review and opportunities. In *Proceedings of the 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)* (pp. 1–6). IEEE.
- Εθνική Αρχή Κυβερνοασφάλειας (Ε.Α.Κ.). (2026). *Εγχειρίδιο κυβερνοασφάλειας για μικρομεσαίες επιχειρήσεις (ΜμΕ)*. Ε.Α.Κ. Εγχειρίδιο Κυβερνοασφάλειας
- European Union Agency for Cybersecurity (ENISA). (2018). *Good practices for security of Internet of Things in the context of smart manufacturing*. ENISA Good Practices for Security of IoT
- Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W., & Sharma, S. R. (2020). *Guide to IPsec VPNs* (NIST Special Publication 800-77 Rev. 1). National Institute of Standards and Technology. NIST SP 800-77 Rev. 1
- Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2025). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). National Institute of Standards and Technology. NIST SP 800-63B
- Kent, K., & Souppaya, M. (2006). *Guide to computer security log management* (NIST Special Publication 800-92). National Institute of Standards and Technology. NIST SP 800-92
- LoRa Alliance. (2020). *LoRaWAN® security whitepaper*. LoRa Alliance Technical Specifications
- Scarfone, K., & Hoffman, P. (2009). *Guidelines on firewalls and firewall policy* (NIST Special Publication 800-41 Rev. 1). National Institute of Standards and Technology.
- Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. NIST SP 800-82 Rev. 3

(Β) Βασικές βιβλιογραφικές πηγές ομαδοποιημένες ανά κατηγορία δείκτη:

1. Αρχιτεκτονική Δικτύων, PLCs & Απομόνωση IT/OT

(Τεκμηριώνει: Απομονωμένοι Ελεγκτές Ψύξης, Εξάλειψη Εργοστασιακών Κωδικών, Απομακρυσμένες Συνδέσεις PAM/MFA, Περιστατικά USB)

- **ISA/IEC 62443 (Series):** *Industrial Communication Networks – Network and System Security*. Κορυφαίο διεθνές πρότυπο για την ασφάλεια των συστημάτων αυτοματισμού και ελέγχου (IACS). Ειδικότερα *τα μέρη **IEC 62443-3-3** (System security requirements) και **IEC 62443-4-2** (Technical security requirements for IACS components) τεκμηριώνουν τον διαχωρισμό δικτύων (Zones & Conduits), την κατάργηση των default κωδικών, τον έλεγχο φυσικών θυρών (USB) και την ασφαλή απομακρυσμένη πρόσβαση.*

- **NIST SP 800-82 Rev. 3 (2023):** *Guide to Operational Technology (OT) Security* (National Institute of Standards and Technology). *Η πιο ολοκληρωμένη αμερικανική οδηγία για την ασφάλεια OT/ICS. Περιγράφει αναλυτικά την τμηματοποίηση δικτύου (Network Segmentation) μεταξύ IT και OT/POS, καθώς και τη διαχείριση ταυτοτήτων και πρόσβασης (PAM/MFA) για εξωτερικούς συντηρητές.*

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- **ENISA (European Union Agency for Cybersecurity):** *Good Practices for Security of Internet of Things in the context of Smart Manufacturing* & *Baseline Security Recommendations for IoT*. *Παρέχει κατευθύνσεις για την αλλαγή εργοστασιακών διαπιστευτηρίων και την προστασία έξυπνων ελεγκτών (Smart Controllers).*

---

2. Χρόνοι Απόκρισης (MTTD / MTTR) & Διαχείριση Περιστατικών

(Τεκμηριώνει: Μέσος Χρόνος Εντοπισμού MTTD, Μέσος Χρόνος Αποκατάστασης MTTR)

- **NIST SP 800-61 Rev. 2 (ή Rev. 3 Draft):** *Computer Security Incident Handling Guide*. Ορίζει το πλαίσιο διαχείρισης συμβάντων ασφαλείας, τον κύκλο ζωής της απόκρισης (Detection, Containment, Eradication, Recovery) και τη σημασία της ελαχιστοποίησης του χρόνου αντίδρασης για τον περιορισμό της ζημιάς.
- **ISO/IEC 27035 (Parts 1-3):** *Information technology — Security techniques — Information security incident management*. Διεθνές πρότυπο που ορίζει τις διαδικασίες και τις μετρικές αξιολόγησης (όπως MTTD και MTTR) της αποτελεσματικότητας της ομάδας απόκρισης.
- **MITRE ATT&CK® for ICS:** Πλαίσιο γνώσης που καταγράφει τις τακτικές και τεχνικές επιθέσεων σε βιομηχανικά συστήματα (π.χ. *Impair Process Control*), υπογραμμίζοντας την ανάγκη άμεσου εντοπισμού ανωμαλιών πριν προκληθεί φυσική βλάβη.

---

3. Φυσικές Δικλίδες Ασφαλείας, Δοκιμές Fail-Safe & Απώλειες Εμπορεύματος (Cold Chain)

(Τεκμηριώνει: Ανεξάρτητη Εποπτεία/Αναλογικοί Θερμοστάτες, Δοκιμές Αυτόνομης Λειτουργίας, Απώλειες Εμπορεύματος)

- **ISO 22000 / HACCP (Hazard Analysis and Critical Control Points):** Διεθνές πρότυπο ασφάλειας τροφίμων. Απαιτεί την ύπαρξη Κρίσιμων Σημείων Ελέγχου (CCPs — όπως η θερμοκρασία ψύξης), ανεξάρτητων συστημάτων καταγραφής/επαλήθευσης και διορθωτικών ενεργειών (Manual Override) ώστε να αποτρέπεται η αλλοίωση προϊόντων.
- **EU GMP Annex 11 & GDP (Good Distribution Practice):** Κατευθυντήριες γραμμές της ΕΕ (για φαρμακευτικά/ευαίσθητα προϊόντα ψυχρής αλυσίδας) που επιβάλλουν ανεξάρτητα συστήματα συναγερμού (independent monitoring) και περιοδικούς ελέγχους εφεδρείας (fail-safe testing).

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- **IEC 61508 / IEC 61511:** *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*. Τεκμηριώνει την ανάγκη ύπαρξης ανεξάρτητων φυσικών δικλίδων ασφαλείας (Safety Instrumented Systems) που λειτουργούν αυτόνομα, ακόμη και αν το ψηφιακό σύστημα ελέγχου (PLC) παραβιαστεί.

- **ASHRAE Guideline 36 / Standard 135 (BACnet):** Οδηγίες για συστήματα αυτοματισμού κτιρίων και ψύξης (HVAC&R), συμπεριλαμβανομένων των διαδικασιών ασφαλούς λειτουργίας (fail-safe) και προστασίας των δικτύων ελέγχου.

---

4. Ανθρώπινος Παράγοντας & Εκπαίδευση

(Τεκμηριώνει: Ποσοστό Εκπαίδευσης Προσωπικού σε Phishing και USB)

- **ISO/IEC 27001:2022 (Control 6.3 – Information security awareness, education and training):** Επιβάλλει τη συνεχή εκπαίδευση του προσωπικού στην αναγνώριση απειλών κοινωνικής μηχανικής (phishing) και την ασφαλή χρήση αφαιρούμενων μέσων (USB).

- **NIST SP 800-50:** *Building an Information Technology Security Awareness and Training Program*. Παρέχει τη μεθοδολογία σχεδιασμού και μέτρησης της αποτελεσματικότητας των προγραμμάτων ευαισθητοποίησης εργαζομένων.

- **CIS Critical Security Controls (Version 8 – Control 14):** *Security Awareness and Skills Training*. Καθορίζει μετρήσιμους στόχους εκπαίδευσης προσωπικού για την αποτροπή αρχικής παραβίασης μέσω email ή φυσικών μέσων.

---

5. Κανονιστικό Πλαίσιο Ευρωπαϊκής Ένωσης & Ελλάδας

(Για ευρύτερη θεσμική τεκμηρίωση του πλαισίου KPIs)

- **Οδηγία (ΕΕ) 2022/2555 (NIS2) & Νόμος 5160/2024 (Ελλάδα):** Ενσωματώνει την ευρωπαϊκή οδηγία για υψηλό κοινό επίπεδο κυβερνοασφάλειας, καλύπτοντας ρητά τους τομείς **παραγωγής, μεταποίησης και διανομής τροφίμων** (ψυχρή αλυσίδα/σούπερ μάρκετ/logistics), απαιτώντας διαχείριση κινδύνων, ασφάλεια εφοδιαστικής αλυσίδας και μετρήσιμη αποτελεσματικότητα μέτρων (Άρθρο 21).

Βιβλιογραφική τεκμηρίωση ανά KPI με επίσημες αναφορές (τίτλους εγγράφων, ενότητες/άρθρα προτύπων και οργανισμούς έκδοσης) .

1. Ποσοστό Απομονωμένων Ελεγκτών Ψύξης (%) — *Διαχωρισμός IT / OT / POS*

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- **NIST SP 800-82 Rev. 3 (2023):** *Guide to Operational Technology (OT) Security*, National Institute of Standards and Technology — **Ενότητα 5: OT Network Architecture** (Τμηματοποίηση δικτύου, ζώνες ασφαλείας, απομόνωση ICS/PLCs από εταιρικά δίκτυα IT και τερματικά POS).

- **IEC 62443-3-3 (2013):** *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*, International Electrotechnical Commission — **SR 5.1: Network segmentation** (Διαχωρισμός κρίσιμων συστημάτων ελέγχου από μη-ελεγχόμενα δίκτυα).

2. Ποσοστό Εξάλειψης Εργοστασιακών Κωδικών (%) — *Default Credentials*

- **IEC 62443-4-2 (2019):** *Technical security requirements for IACS components* — **CR 1.1 & CR 1.5: Human user identification and authentication / Authenticator management** (Υποχρεωτική αλλαγή προεπιλεγμένων διαπιστευτηρίων κατά την εγκατάσταση).

- **ENISA (2019):** *Good Practices for Security of IoT in the context of Smart Manufacturing*, European Union Agency for Cybersecurity — **GP-TM-14 / Access Control** (Κατάργηση εργοστασιακών κωδικών πρόσβασης σε βιομηχανικούς ελεγκτές).

- **NISTIR 8259A (2020):** *IoT Device Cybersecurity Capability Core Baseline* — Ενότητα *Device Configuration* (Απαίτηση αλλαγής default passwords πριν τη θέση σε λειτουργία).

3. Κάλυψη Ανεξάρτητης Εποπτείας & Φυσικών Δικλίδων (%) — *Καταγραφέας SIM / Αναλογικός Θερμοστάτης*

- **IEC 61511-1 (2016):** *Functional safety – Safety instrumented systems for the process industry sector* — Αρχή της **Ανεξαρτησίας (Independence)** μεταξύ του Βασικού Συστήματος Ελέγχου (BPCS/PLC) και του Συστήματος Ασφαλείας (SIS), ώστε μια κυβερνοεπίθεση στο ψηφιακό δίκτυο να μην αχρηστεύει τη φυσική προστασία.

- **Κανονισμός (ΕΚ) 852/2004 & Πρότυπο ISO 22000:2018:** *Food safety management systems* — **Κεφάλαιο 8.5 (Hazard control / HACCP)** (Ανεξάρτητη παρακολούθηση Κρίσιμων Σημείων Ελέγχου - CCPs ψύξης).

4. Μέσος Χρόνος Εντοπισμού Ανωμαλίας (MTTD < 5 λεπτά)

- **ISO/IEC 27035-1:2023:** *Information technology — Information security incident management — Part 1: Principles and process* — Ορισμός μετρικών έγκαιρης ανίχνευσης (Detection metrics) και ειδοποίησης σε πραγματικό χρόνο.

- **NIST SP 800-61 Rev. 2:** *Computer Security Incident Handling Guide* — **Ενότητα 3.2: Detection and Analysis** (Σημασία αυτοματοποιημένων ειδοποιήσεων / SIEM / OT monitoring για τον άμεσο εντοπισμό ανωμαλιών).

- **MITRE ATT&CK® for ICS (v15):** Τακτική **Inhibit Response Function (TA0107)** & **Impair Process Control (TA0106)** — Τεκμηριώνει πώς οι επιτιθέμενοι αλλοιώνουν τις ενδείξεις θερμοκρασίας (Spoof Reporting Message) και γιατί απαιτείται εντοπισμός εντός λεπτών.

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

5. Μέσος Χρόνος Αποκατάστασης & Αντίδρασης (MTTR < 15–30 λεπτά)

- **NIST SP 800-82 Rev. 3 (2023): Ενότητα 6.2.12: Incident Response** (Διαδικασίες άμεσης απομόνωσης παραβιασμένου τμήματος OT χωρίς διακοπή της φυσικής ψύξης).
- **ASHRAE Guideline 36 (2021):** *High-Performance Sequences of Operation for HVAC Systems* — Προδιαγραφές χρονικών ορίων επαναφοράς ασφαλών συνθηκών λειτουργίας (Safe State Recovery) πριν επέλθει θερμική αλλοίωση φορτίου.

6. Ποσοστό Ελεγχόμενων Απομακρυσμένων Συνδέσεων (%) — *PAM / MFA με χρονικό περιορισμό*

- **NIST SP 800-82 Rev. 3 (2023): Ενότητα 6.2.2 (Access Control - AC-17 Remote Access)** & **IA-2 (Multi-Factor Authentication)** (Υποχρεωτική χρήση MFA και ελεγχόμενων πυλών/jump hosts για εξωτερικούς τεχνικούς συντήρησης).
- **IEC 62443-3-3 (2013): SR 1.13: Access via untrusted networks** (Έλεγχος, καταγραφή συνεδριών και χρονικός περιορισμός — Just-in-Time access — απομακρυσμένων συνδέσεων συντηρητών).
- **CIS Critical Security Controls v8 (2021): Control 6: Access Control Management (6.5 & 6.8)** (Διαχείριση προνομιούχων λογαριασμών - PAM και MFA).

7. Περιστατικά Μη Εξουσιοδοτημένων Συσκευών (USB) — *Στόχος: 0*

- **IEC 62443-3-3 (2013): SR 2.3: Use control for portable and mobile devices** (Αυστηρός έλεγχος ή φυσική/λογική απενεργοποίηση θυρών USB σε σταθμούς εργασίας HMI και PLCs).
- **NIST SP 800-82 Rev. 3 (2023): Έλεγχος MP-7 (Media Use)** (Περιορισμός χρήσης αφαιρούμενων μέσων αποθήκευσης σε περιβάλλοντα OT, βασικός φορέας κακόβουλου λογισμικού όπως το Stuxnet/Triton).

8. Ποσοστό Απωλειών Εμπορεύματος λόγω Κυβερνοσυμβάντων (%) —*Στόχος: 0%*

- **Οδηγία (ΕΕ) 2022/2555 (NIS2) & Ν. 5160/2024 (ΦΕΚ Α' 195): Άρθρο 21 (Μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας)** & **Παράρτημα ΙΙ (Τομέας: Παραγωγή, μεταποίηση και διανομή τροφίμων)** — Συνδέει άμεσα την κυβερνοασφάλεια με την επιχειρησιακή συνέχεια (Business Continuity) και την αποτροπή απώλειας κρίσιμων αποθεμάτων.
- **ISO 22301:2019:** *Security and resilience — Business continuity management systems* — Μετρικές οικονομικής και υλικής ζημιάς από διακοπή λειτουργίας κρίσιμων υποδομών.

9. Επιτυχία Δοκιμών Αυτόνομης Λειτουργίας (%) — *Fail-Safe / Manual Override*

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

- **NIST SP 800-82 Rev. 3 (2023): Έλεγχος CP-4 (Contingency Plan Testing)** (Περιοδικές δοκιμές μετάβασης σε χειροκίνητη ή αυτόνομη λειτουργία ασφαλείας σε περίπτωση απώλειας ψηφιακού ελέγχου).
- **IEC 61511-1 (2016): Κεφάλαιο 16: SIS Operation and Maintenance (Proof Testing)** (Υποχρεωτικές ετήσιες δοκιμές επιβεβαίωσης ότι οι φυσικές δικλίδες/manual overrides λειτουργούν σωστά).

10. Ποσοστό Εκπαίδευσης Προσωπικού (%) — *Phishing & Κακόβουλα USB (Στόχος > 90%)*

- **ISO/IEC 27001:2022: Παράρτημα Α, Έλεγχος 6.3 (Information security awareness, education and training)** (Τακτική εκπαίδευση προσωπικού για αναγνώριση κοινωνικής μηχανικής και φυσικών απειλών).
- **NIST SP 800-50 Rev. 1 (2024):** *Building a Cybersecurity and Privacy Learning Program* — Καθορισμός μετρήσιμων δεικτών συμμετοχής (Training Completion Rate >90%) σε προσομοιώσεις phishing και ασφαλή χρήση μέσων (USB).

*** <u>Σημείωση</u> : Πηγές Ορολογίας (για τους αστερίσκους [*] στο κείμενο)**

Για την τεκμηρίωση των ακρωνυμίων (*KPIs, PLCs, IT, POS, PAM, MFA, Phishing, USB*), η επίσημη αναφορά είναι:

- **NIST Computer Security Resource Center (CSRC) Glossary:** *Glossary of Key Information Security Terms* (NISTIR 7298 Rev. 3).

---

2. Βιβλιογραφία & Πρότυπα Αναφοράς :

Center for Internet Security. (2021). ***CIS Critical Security Controls (Version 8)*. CIS. cisecurity.org**

European Commission. (2013). ***Guidelines of 5 November 2013 on Good Distribution Practice of medicinal products for human use*** *(2013/C 343/01)*. Official Journal of the European Union.

European Parliament & Council of the European Union. (2004). ***Regulation (EC) No 852/2004 of the European Parliament and of the Council of 29 April 2004 on the hygiene of foodstuffs*.** Official Journal of the European Union.

European Parliament & Council of the European Union. (2022). ***Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)***. Official Journal of the European Union.

Αποποίηση ευθύνης :

Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

European Union Agency for Cybersecurity. (2019). ***Good practices for security of IoT in the context of smart manufacturing*. ENISA. doi.org**

ASHRAE. (2021). *ASHRAE Guideline 36-2021:* ***High-performance sequences of operation for HVAC systems*.** American Society of Heating, Refrigerating and Air-Conditioning Engineers.

International Electrotechnical Commission. (2013). *IEC 62443-3-3:* ***Industrial communication networks – Network and system security*** *– Part 3-3: System security requirements and security levels*. IEC.

International Electrotechnical Commission. (2016). *IEC 61511-1:* ***Functional safety – Safety instrumented systems for the process industry sector*** *– Part 1: Framework, definitions, system, hardware and application programming requirements*. IEC.

International Electrotechnical Commission**.** (2019). *IEC 62443-4-2:* ***Security for industrial automation and control systems*** *– Part 4-2: Technical security requirements for IACS components*. IEC.

International Organization for Standardization. (2018). *ISO 22000:2018 –* ***Food safety management systems – Requirements for any organization in the food chain*.** ISO.

International Organization for Standardization. (2019). *ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements*. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. ISO/IEC.

International Organization for Standardization & International Electrotechnical Commission. (2023). *ISO/IEC 27035-1:2023 –* ***Information technology – Information security incident management – Part 1: Principles and process*.** ISO/IEC.

National Institute of Standards and Technology. (2012). ***Computer security incident handling guide (NIST Special Publication 800-61 Rev****. 2)*. U.S. Department of Commerce. doi.org

National Institute of Standards and Technology**.** (2019). ***Glossary of key information security terms (NIST Interagency/Internal Report 7298 Rev.*** *3)*. U.S. Department of Commerce. doi.org

National Institute of Standards and Technology. (2020). ***IoT device cybersecurity capability core baseline (NIST Interagency/Internal Report 8259A****)*. U.S. Department of Commerce. doi.org

National Institute of Standards and Technology. (2023). ***Guide to operational technology (OT) security (NIST Special Publication 800-82 Rev.*** *3)*. U.S. Department of Commerce. doi.org

National Institute of Standards and Technology**.** (2024). ***Building a cybersecurity and privacy learning program (NIST Special Publication 800-50 Rev.*** *1)*. U.S. Department of Commerce. doi.org

---

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.

Ελληνική Δημοκρατία. (2024). ***Νόμος 5160/2024 (ΦΕΚ Α' 195/06.12.2024): Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 (NIS2) σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση***. Εθνικό Τυπογραφείο.

Δείκτες Απόδοσης Κυβερνοασφάλειας (KPIs*)

Για τη μέτρηση της αποτελεσματικότητας των μέτρων θωράκισης και της ταχύτητας αντίδρασης, παρακολουθούνται οι ακόλουθοι δείκτες:

• Ποσοστό Απομονωμένων Ελεγκτών Ψύξης (%): Ποσοστό ελεγκτών και PLCs* πλήρως διαχωρισμένων από το δίκτυο IT* / POS* (Στόχος: 100%).

• Ποσοστό Εξάλειψης Εργοστασιακών Κωδικών (%): Ποσοστό συσκευών στις οποίες έχουν αλλαχθεί οι προεπιλεγμένοι κωδικοί (Στόχος: 100%).

• Κάλυψη Ανεξάρτητης Εποπτείας & Φυσικών Δικλίδων (%): Ποσοστό θαλάμων με καταγραφέα SIM ή αναλογικό θερμοστάτη ασφαλείας (Στόχος: 100%).

• Μέσος Χρόνος Εντοπισμού Ανωμαλίας (MTTD): Χρόνος από την εμφάνιση ύποπτης μεταβολής έως τη λήψη ειδοποίησης (Στόχος: < 5 λεπτά).

• Μέσος Χρόνος Αποκατάστασης & Αντίδρασης (MTTR): Χρόνος απομόνωσης της απειλής και επαναφοράς ασφαλούς θερμοκρασίας (Στόχος: < 15–30 λεπτά).

• Ποσοστό Ελεγχόμενων Απομακρυσμένων Συνδέσεων (%): Παρεμβάσεις τεχνικών μέσω PAM*/MFA* με χρονικό περιορισμό (Στόχος: 100%).

• Περιστατικά Μη Εξουσιοδοτημένων Συσκευών (USB): Απόπειρες σύνδεσης άγνωστων συσκευών ανά μήνα (Στόχος: 0).

• Ποσοστό Απωλειών Εμπορεύματος λόγω Κυβερνοσυμβάντων (%): Κατεστραμμένα προϊόντα λόγω ψηφιακής επίθεσης (Στόχος: 0%).

• Επιτυχία Δοκιμών Αυτόνομης Λειτουργίας (%): Επιτυχής έκβαση ετήσιων δοκιμών fail-safe / manual override (Στόχος: 100%).

• Ποσοστό Εκπαίδευσης Προσωπικού (%): Εργαζόμενοι εκπαιδευμένοι στην αναγνώριση phishing* και κακόβουλων USB* (Στόχος: > 90%).

Για τη βιβλιογραφική τεκμηρίωση των παραπάνω δεικτών απόδοσης κυβερνοασφάλειας (KPIs) —οι οποίοι εστιάζουν στην προστασία συστημάτων Βιομηχανικού Ελέγχου (ICS / OT), PLCs, συστημάτων ψύξης (HVAC/Refrigeration) και εφοδιαστικής αλυσίδας τροφίμων/φαρμάκων (Cold Chain)— ***οι έγκυρες πηγές προέρχονται από διεθνή πρότυπα ασφάλειας, κανονισμούς και οδηγούς βέλτιστων πρακτικών.***

Αποποίηση ευθύνης :
Η εργασία αυτή αποτελεί προϊόν βιβλιογραφικής και διαδικτυακής διερεύνησης (AI)
με την οποία επιδιώκεται προσέγγιση της αρχιτεκτονικής & τεχνικής αντιμετωπισης του επίκαιρου ερώτηματος που αφορά στις **κυβερνοεπιθέσεις σε ψυγεία μονάδων επεξεργασίας κρέατος / super markets και κρεοπωλεία** . Η εργασία έχει ενημερωτικό χαρακτήρα και δεν αποτελεί πρόταση εφαρμογής καθώς ενδέχεται να περιέχει λάθη.