****

18/26/2025

Ιωάννης Α. Μπούχρας - IT Information Systems Security Manager - AI / ML Consultant

Κατάσταση Υποδομής Πληροφορικής

**Κίνδυνοι και Προτάσεις**

**2025-2026**

Περιεχόμενα

[1 Εισαγωγή 2](#_Toc201155567)

[2 Πρωτεύουσα Υποδομή 2](#_Toc201155568)

[3 Αντίγραφα Ασφαλείας 3](#_Toc201155569)

[4 Δευτερεύουσα Υποδομή 3](#_Toc201155570)

[5 Λογισμικό & Domain 4](#_Toc201155571)

[6 Mail Server 5](#_Toc201155572)

[7 Firewall 5](#_Toc201155573)

[7.1 Γιατί πρέπει να το διατηρήσουμε 6](#_Toc201155574)

[7.2 Συμπέρασμα & Σύσταση 6](#_Toc201155575)

[8 Web Υπηρεσίες 6](#_Toc201155576)

[9 Σταθμοί Εργασίας MICROSOFT WINDOWS 10 7](#_Toc201155577)

[10 Υποδομή Θεσσαλονίκης 8](#_Toc201155578)

[11 Backups Desktops χρηστών 8](#_Toc201155579)

[12 Εικονικά ετήσια αντίγραφα ασφαλείας χρηστών 9](#_Toc201155580)

[13 Πλατφόρμα UNIXFOR Cloud 10](#_Toc201155581)

[14 Indicators of Compromise - Case management & Monitoring 10](#_Toc201155582)

[15 Τηλεφωνικά κέντρα της εταιρίας 11](#_Toc201155583)

[16 Software τέλους ζωής 12](#_Toc201155584)

[17 Συμπέρασμα 12](#_Toc201155585)

# Εισαγωγή

Μετά από μια δύσκολη διετία κατά την οποία, λόγω οικονομικών πιέσεων και προτεραιοτήτων της εταιρίας, οι επενδύσεις στην υποδομή πληροφορικής ήταν περιορισμένες, το Τμήμα Πληροφορικής (NSS) θεωρεί καθήκον του να προχωρήσει σε μια ολοκληρωμένη ενημέρωση της παρούσης κατάστασης προς τη Διοίκηση.

Σκοπός της παρούσας αναφοράς είναι να αποτυπωθεί με σαφήνεια η πραγματική κατάσταση της υποδομής μας, οι **σοβαροί** κίνδυνοι που έχουν συσσωρευτεί λόγω της παλαιότητας του εξοπλισμού και της έλλειψης υποστήριξης (σημείωση: δεν αναφέρονται όλοι), καθώς και οι άμεσες ανάγκες που απαιτούνται ώστε να διασφαλίσουμε τη συνέχεια των επιχειρησιακών δραστηριοτήτων, τη συμμόρφωση με κανονισμούς και την προστασία της φήμης και της αξιοπιστίας της εταιρίας μας.

Η παρούσα ανάλυση δεν αποσκοπεί μόνο στην ανάδειξη των προβλημάτων, αλλά και στη διαμόρφωση ενός πλαισίου προτάσεων που θα επιτρέψει στην UNIXFOR να θωρακιστεί απέναντι σε σύγχρονες τεχνολογικές προκλήσεις, κινδύνους ασφάλειας και επιχειρησιακές διακοπές που θα μπορούσαν να έχουν καταστροφικές συνέπειες για την απρόσκοπτη λειτουργία και την ανταγωνιστικότητά της.

Αναλυτική κατάσταση της υποδομής μας βρίσκετε στο σύστημα του EN/ISO 27001 Παράρτημα Γ - Risk Assessment ISO27001\_2013.docx και Παράρτημα Γ - Risk Assessment - Unixfor Servers.docx

# Πρωτεύουσα Υποδομή

Η κύρια υποδομή πληροφορικής της εταιρίας στηρίζεται σε δύο εξυπηρετητές (Servers) Lenovo ThinkSystem SR650 και σε ένα σύστημα αποθήκευσης δεδομένων (Storage) IBM Storewize 5000e. Πρόκειται για την καρδιά της λειτουργίας μας, καθώς πάνω σε αυτά τα συστήματα «τρέχουν» όλα τα κρίσιμα παραγωγικά μηχανήματα της εταιρίας μέσω εικονικοποίησης (virtualization) με το λογισμικό VMware.

Στην υποδομή αυτή φιλοξενούνται όλες οι βασικές επιχειρησιακές εφαρμογές μας. Παρά το γεγονός ότι σε επίπεδο υλικού ο εξοπλισμός αυτός δεν έχει φτάσει ακόμη στο στάδιο του επίσημου τερματισμού ζωής (**end of life**), η απουσία ενεργών συμβολαίων υποστήριξης τόσο για το hardware όσο και για το λογισμικό τον καθιστά ουσιαστικά ευάλωτο σε κάθε ενδεχόμενο βλάβης. Οι άδειες χρήσης του VMware έχουν λήξει και δεν υφίσταται πλέον δυνατότητα πρόσβασης σε αναβαθμίσεις, ενημερώσεις ασφαλείας ή επίσημη τεχνική υποστήριξη, γεγονός που αυξάνει κατακόρυφα τον κίνδυνο για την εταιρία.

Η κατάσταση αυτή δημιουργεί έναν ιδιαίτερα υψηλό επιχειρησιακό κίνδυνο. Σε περίπτωση που προκύψει βλάβη σε έναν από τους δύο βασικούς servers, οι παραγωγικές υπηρεσίες που φιλοξενούνται σε αυτόν – δηλαδή οι εικονικές μηχανές που στηρίζουν την καθημερινή λειτουργία της εταιρίας ή πελατών – θα τεθούν εκτός λειτουργίας για μεγάλο χρονικό διάστημα. Η έλλειψη συμβολαίων υποστήριξης και η παλαιότητα του εξοπλισμού καθιστούν εξαιρετικά δύσκολη και χρονοβόρα τη διαδικασία εύρεσης ανταλλακτικών και αποκατάστασης της βλάβης. Ο εκτιμώμενος χρόνος αποκατάστασης μπορεί να ξεπεράσει ακόμη και τον ένα μήνα, γεγονός που θα έχει σοβαρές συνέπειες για τη λειτουργία της εταιρίας. Ακόμη πιο ανησυχητικό είναι το σενάριο βλάβης του κεντρικού συστήματος αποθήκευσης (Storage). Μια τέτοια βλάβη θα σημάνει την πλήρη παύση όλων των παραγωγικών υπηρεσιών της εταιρίας, με καταστροφικό αντίκτυπο στις επιχειρησιακές δραστηριότητες, τη φήμη και τις σχέσεις της εταιρίας με πελάτες, συνεργάτες, τράπεζες και ρυθμιστικές αρχές.

# Αντίγραφα Ασφαλείας

Το σύστημα αντιγράφων ασφαλείας της εταιρίας βασίζεται σε έναν εξυπηρετητή (Server) IBM 3650 M3, ο οποίος λειτουργεί με λογισμικό Symantec NetBackup. Πρόκειται για εξοπλισμό που έχει ξεπεράσει εδώ και καιρό το όριο ζωής του (end of life) και δεν καλύπτεται πλέον από καμία επίσημη τεχνική υποστήριξη (end of support). Παράλληλα, οι άδειες χρήσης του λογισμικού backup έχουν λήξει, με αποτέλεσμα η εταιρία να βρίσκεται σε καθεστώς παράνομης χρήσης, γεγονός που συνεπάγεται σοβαρό κίνδυνο επιβολής προστίμων σε περίπτωση ελέγχου ή audit από τη Symantec.

Η κατάσταση γίνεται ακόμη πιο κρίσιμη λόγω των τεχνικών περιορισμών του υπάρχοντος συστήματος. Ο χώρος αποθήκευσης για τα αντίγραφα ασφαλείας είναι σχεδόν πλήρης, καθώς απομένουν μόλις περίπου 400GB διαθέσιμα, κάτι που περιορίζει σημαντικά τη δυνατότητα λήψης νέων αντιγράφων και θέτει σε κίνδυνο την πληρότητα των backup. Για να καταλάβετε ο server μόνο του παραγωγικού μας TotalCare χρειάζεται τώρα που έχει 130+ kiosks 25GB το χρόνο από το backup.

Σε περίπτωση βλάβης του server backup, η εταιρία θα χάσει τη δυνατότητα επαναφοράς δεδομένων για μεγάλο χρονικό διάστημα, που μπορεί να ξεπεράσει ακόμη και τον ένα μήνα, καθώς δεν υπάρχει διαθέσιμος εξοπλισμός προς αντικατάσταση και δεν καλύπτεται από κάποιο συμβόλαιο τεχνικής υποστήριξης.

Αξίζει να σημειωθεί ότι σε περιπτώσεις κυβερνοεπιθέσεων, και ιδιαίτερα σε περιστατικά ransomware, το πρώτο που επιχειρούν οι επιτιθέμενοι μόλις καταφέρουν να εισέλθουν στο δίκτυο ενός οργανισμού είναι να εντοπίσουν και να κρυπτογραφήσουν ή να καταστρέψουν τα αντίγραφα ασφαλείας. Στόχος τους είναι να καταστήσουν αδύνατη την επαναφορά των δεδομένων και να μεγιστοποιήσουν την πίεση για καταβολή λύτρων. Η παρούσα αδυναμία του backup συστήματός μας, σε συνδυασμό με την έλλειψη σύγχρονων τεχνικών μέτρων προστασίας, καθιστά την εταιρία ιδιαίτερα ευάλωτη σε ένα τέτοιο σενάριο, με δυνητικά καταστροφικές συνέπειες.

# Δευτερεύουσα Υποδομή

Η δευτερεύουσα υποδομή της εταιρίας αποτελείται από δύο εξυπηρετητές (Servers) IBM 3650 M2 οι οποίοι είναι συνδεδεμένοι με σύστημα αποθήκευσης (Storage) IBM DS3524.

Η υποδομή αυτή φιλοξενεί μη παραγωγικά, αλλά εξαιρετικά σημαντικά περιβάλλοντα, όπως αυτά που αφορούν τις λειτουργίες του NSS, τα εργαλεία ασφάλειας της εταιρίας (Antivirus, EDR, Monitoring, IOCs (Indicators Of Compromise) Case Management κτλ.), καθώς και τις πλατφόρμες που χρησιμοποιούνται για δοκιμές, πειραματισμούς και την προσομοίωση αλλαγών πριν την εφαρμογή τους στα παραγωγικά συστήματα. Πρόκειται ουσιαστικά για το «εργαστήριο» και το προστατευτικό φίλτρο της υποδομής, μέσω του οποίου εξασφαλίζεται η σταθερότητα και η ασφάλεια πριν από κάθε νέα υλοποίηση ή παρέμβαση στα κρίσιμα παραγωγικά συστήματα.

Δυστυχώς, ο εξοπλισμός αυτός βρίσκεται πλέον σε κατάσταση end of life και end of support. Αυτό σημαίνει ότι δεν υπάρχει πλέον καμία επίσημη υποστήριξη από τον κατασκευαστή, δεν διατίθενται ανταλλακτικά στην αγορά από επίσημα κανάλια και δεν παρέχονται ενημερώσεις ή τεχνικές βελτιώσεις. Η παραμικρή βλάβη σε κάποιο από τα συστήματα αυτά, είτε αφορά στο hardware των servers είτε στο σύστημα αποθήκευσης, θα έχει ως αποτέλεσμα η εταιρία να χάσει τη δυνατότητα πρόσβασης σε αυτά τα περιβάλλοντα.

Η απώλεια των δοκιμαστικών και ασφαλείας περιβαλλόντων δεν επηρεάζει άμεσα την καθημερινή παραγωγή. Ωστόσο, καθιστά αδύνατη την ασφαλή ανάπτυξη νέων υπηρεσιών, την εφαρμογή ενημερώσεων ή αλλαγών στα παραγωγικά συστήματα και την υλοποίηση ελέγχων και δοκιμών ασφαλείας, εκθέτοντας έτσι την εταιρία σε σοβαρούς κινδύνους λειτουργικούς και κυβερνοασφάλειας. Επιπλέον, η απουσία τέτοιων περιβαλλόντων δυσχεραίνει την αντιμετώπιση κρίσεων και καθυστερεί την αποκατάσταση σε περιπτώσεις συμβάντων, καθώς δεν θα υπάρχει τρόπος να δοκιμάζονται λύσεις ή σενάρια αποκατάστασης προτού εφαρμοστούν στο «ζωντανό» παραγωγικό περιβάλλον.

# Λογισμικό & Domain

Η εταιρία βασίζεται σε υποδομή Windows domain – και Domain Controllers τεχνολογίας 2013 και σε servers που λειτουργούν με Windows Server 2012 R2 - αν και τα τελευταία χρόνια γίνετε προσπάθεια σε όσους νέους servers φτιάχνουμε να βρίσκονται στην έκδοση 2019-2022.

Η πλατφόρμα αυτή 2013, η οποία αποτελεί τον βασικό κορμό ταυτοποίησης, εξουσιοδότησης και ελέγχου πρόσβασης των χρηστών και των συστημάτων, βρίσκεται πλέον σε καθεστώς πλήρους λήξης υποστήριξης (end of support). Αυτό σημαίνει ότι η Microsoft δεν παρέχει πλέον καμία ενημέρωση ασφαλείας, αναβάθμιση ή τεχνική υποστήριξη για αυτά τα λειτουργικά συστήματα.

Η απουσία ενημερώσεων ασφαλείας έχει ως αποτέλεσμα οι servers αυτοί να διαθέτουν πλέον γνωστές ευπάθειες, οι οποίες είναι καταγεγραμμένες και εύκολα προσβάσιμες σε κακόβουλους παράγοντες. Ο κίνδυνος παραβίασης είναι υπαρκτός και σοβαρός, καθώς οι servers αυτοί αποτελούν το κεντρικό σημείο ελέγχου της υποδομής και οποιαδήποτε παραβίασή τους θα επέτρεπε σε επιτιθέμενους να αποκτήσουν προνομιακή πρόσβαση σε κρίσιμα συστήματα και δεδομένα.

Επιπλέον, τα λειτουργικά αυτά συστήματα δεν υποστηρίζουν πλέον σύγχρονο λογισμικό antivirus και άλλα εργαλεία προστασίας, με αποτέλεσμα η υποδομή να είναι πρακτικά ανοιχτή σε σύγχρονες κυβερνοαπειλές. Το γεγονός αυτό υπονομεύει άμεσα τη συμμόρφωση της εταιρίας με κανονιστικά πλαίσια όπως το GDPR και τα πρότυπα κυβερνοασφάλειας, ενώ ταυτόχρονα αυξάνει τον κίνδυνο σοβαρού περιστατικού ασφαλείας που θα μπορούσε να οδηγήσει σε απώλεια δεδομένων, διακοπή λειτουργίας και βλάβη της εταιρικής φήμης.

# Mail Server

Ο mail server της εταιρίας βασίζεται σε πλατφόρμα Microsoft Exchange 2013, η οποία έχει φτάσει στο τέλος ζωής της (end of life) και δεν υποστηρίζεται πλέον από τον κατασκευαστή (end of support). Αυτό σημαίνει ότι η υποδομή email μας λειτουργεί χωρίς καμία επίσημη τεχνική υποστήριξη, χωρίς ενημερώσεις ασφαλείας και χωρίς δυνατότητα πρόσβασης σε διορθωτικές αναβαθμίσεις ή patches για γνωστά προβλήματα.

Η παραμονή σε αυτή την πλατφόρμα συνεπάγεται σοβαρούς κινδύνους για τη λειτουργία και την ασφάλεια της εταιρίας. Σε περίπτωση που προκύψει οποιαδήποτε τεχνική βλάβη στον mail server, η εταιρία κινδυνεύει να μείνει χωρίς δυνατότητα αποστολής και λήψης email για μεγάλο χρονικό διάστημα, καθώς η αποκατάσταση θα απαιτήσει πολύπλοκες και χρονοβόρες διαδικασίες, χωρίς τη στήριξη της Microsoft. Μια τέτοια κατάσταση θα επηρεάσει άμεσα την επικοινωνία με πελάτες, συνεργάτες, τράπεζες και ρυθμιστικές αρχές, θέτοντας σε κίνδυνο τη λειτουργική συνέχεια και τη φήμη της εταιρίας.

Επιπρόσθετα, ο όγκος των δεδομένων που φιλοξενούνται στον υπάρχοντα mail server ξεπερνά το 1 terabyte καθώς έχει data από το 2004. Το μέγεθος αυτό καθιστά εξαιρετικά δύσκολη και χρονοβόρα οποιαδήποτε προσπάθεια μετεγκατάστασης των δεδομένων σε σύγχρονη πλατφόρμα, είτε σε νεότερη έκδοση Exchange είτε σε λύση cloud όπως το Microsoft 365. Ο μεγάλος αυτός όγκος δεδομένων, σε συνδυασμό με την παλαιότητα της υποδομής, αυξάνει σημαντικά το ρίσκο απώλειας δεδομένων ή διακοπής της λειτουργίας κατά τη διάρκεια της μετάβασης.

Τέλος, η χρήση ενός mail server εκτός υποστήριξης δημιουργεί σοβαρές ευπάθειες έναντι σύγχρονων κυβερνοαπειλών, καθώς δεν πληροί πλέον τα απαιτούμενα πρότυπα ασφαλείας για την προστασία από επιθέσεις όπως phishing, spoofing και παραβίαση δεδομένων.

# Firewall

Η εταιρία μας βασίζεται στο Check Point firewall, το οποίο έχει αποδειχθεί υψηλής αποτελεσματικότητας στην προστασία από σύγχρονες απειλές και ransomware. Σύμφωνα με το τελευταίο ανεξάρτητο benchmark της Miercom (2025), το Check Point Infinity Platform πέτυχε ασυναγώνιστο ποσοστό μπλοκαρίσματος, “zero-day” malware (99,9 %) και phishing (99,7 %).

Αυτά τα αποτελέσματα κατατάσσουν το Check Point ως την κορυφαία λύση σε διαθεσιμότητα και ασφάλεια, προστατεύοντας επιτυχώς τόσο on‑premises όσο και υποδομές cloud (hybrid mesh)

## Γιατί πρέπει να το διατηρήσουμε

* Βελτιστοποιημένη Απόδοση Ασφαλείας: Top score σε threat prevention (zero-day, phishing), χάρη στην εξελιγμένη τεχνολογία AI και real-time threat intelligence
* Υψηλότερη Αποδοτικότητα: Ενοποιημένη διαχείριση, αυτοματοποίηση, μείωση πολύπλοκων διαχειριστικών διεργασιών – 95% λιγότερος χρόνος διαχείρισης πολιτικών, 90% ταχύτερο patching .
* Κλιμακωτότητα & Ανθεκτικότητα: Από υποδομές περιφερειακής πρόσβασης έως μεγάλα data centers, το Check Point υποστηρίζει φόρτους έως 1 TBps και clustering μέχρι 3 Tbps χωρίς downtime
* Υποστήριξη Cloud & Hybrid Περιβάλλοντα: Το Check Point Infinity/CloudGuard παρέχει κυρίαρχη ασφάλεια σε cloud workloads, inline policies και ορατότητα σε σύνθετα υβριδικά δίκτυα

Αξιοπιστία στην Πρακτική: Περισσότεροι από 100.000 οργανισμοί εμπιστεύονται το Check Point. Ανεξάρτητοι testers (PeerSpot, eSecurityPlanet) το κατατάσσουν ως πρώτο στην ευκολία χρήσης, διαχείριση και ασφάλεια

## Συμπέρασμα & Σύσταση

Παρά το υψηλό κόστος συντήρησης, το Check Point αποδίδει άμεσα με κορυφαία αποτελέσματα ασφάλειας, μειωμένη πολυπλοκότητα και υψηλή αξιοπιστία.

**Σύμφωνα με την τελευταία ενημέρωση της Checkpoint τα firewalls τα οποία διαθέτουμε θα βγουν End of Support στο τέλος του 2025, και το κόστος αγοράς καινούριών είναι πολύ μεγάλο ~31.000 $ , για αυτόν τον λόγο προσπαθούμε να βρούμε χαμηλότερα μοντέλα για να μειώσουμε το κόστος αλλά να μην χάσουμε της υπηρεσίες ποιότητας, δηλαδή συνεχής προστασία απέναντι σε ransomware και άλλες απειλές, και τη συμμόρφωση με τα πλέον απαιτητικά πρότυπα ασφάλειας ISO και επιχειρησιακής συνέχειας.**

# Web Υπηρεσίες

Οι web υπηρεσίες της εταιρίας, όπως για παράδειγμα η πλατφόρμα TotalCare που προσφέρουμε σε πελάτες, φιλοξενούνται σήμερα εσωτερικά στους servers της δικής μας υποδομής. Η προσέγγιση αυτή, αν και λειτουργεί, ενέχει περιορισμούς που αφορούν τόσο στη διαθεσιμότητα όσο και στην ασφάλεια των υπηρεσιών μας. Η φιλοξενία σε τοπικούς servers περιορίζει τη δυνατότητα κλιμάκωσης των υπηρεσιών σε περιόδους αυξημένου φορτίου και μας καθιστά ευάλωτους σε περιστατικά όπως βλάβες hardware, διακοπές ρεύματος ή τοπικές κυβερνοεπιθέσεις.

Η μεταφορά των web υπηρεσιών μας σε υποδομή cloud, σε αξιόπιστες πλατφόρμες όπως το Microsoft Azure ή το AWS, θα ενισχύσει καθοριστικά τη διαθεσιμότητα των συστημάτων, διασφαλίζοντας ότι οι υπηρεσίες μας θα παραμένουν προσβάσιμες και λειτουργικές ανεξαρτήτως τοπικών συνθηκών ή αστοχιών υλικού. Επιπλέον, οι cloud πλατφόρμες ενσωματώνουν εξελιγμένα μέτρα κυβερνοασφάλειας, όπως προηγμένα firewalls, DDoS protection, μηχανισμούς identity & access management και real-time παρακολούθηση για ύποπτη δραστηριότητα, παρέχοντας έτσι ένα επίπεδο προστασίας που είναι πολύ δύσκολο να επιτευχθεί σε τοπικό επίπεδο με το υφιστάμενο προσωπικό και εξοπλισμό.

Η μετάβαση αυτή θα προσφέρει στη UNIXFOR μεγαλύτερη ευελιξία, καθώς οι πόροι μπορούν να αυξομειώνονται δυναμικά ανάλογα με τις ανάγκες, χωρίς να απαιτούνται δαπανηρές επενδύσεις σε φυσικό εξοπλισμό. Επιπλέον, θα μειώσει το λειτουργικό φορτίο της εσωτερικής υποδομής, απελευθερώνοντας πόρους και δυνατότητες του IT τμήματος ώστε να επικεντρωθεί σε κρίσιμες λειτουργίες και στρατηγικές πρωτοβουλίες.

Με βάση τα παραπάνω, το Τμήμα Πληροφορικής εισηγείται τη σταδιακή μετάβαση των web υπηρεσιών σε σύγχρονη cloud υποδομή, συνοδευόμενη από κατάλληλα Service Level Agreements (SLA), ώστε να διασφαλίσουμε υψηλή διαθεσιμότητα, ανθεκτικότητα σε κυβερνοαπειλές και απρόσκοπτη εμπειρία χρήσης για τους πελάτες και συνεργάτες μας.

# Σταθμοί Εργασίας MICROSOFT WINDOWS 10

Από τις **14 Οκτωβρίου 2025**, η Microsoft θα τερματίσει οριστικά την υποστήριξη για τα Windows 10 (Home & Pro & Enterprise), γεγονός που σημαίνει ότι δεν θα παρέχονται πλέον **τεχνική βοήθεια**, **software updates** ή σημαντικές **επικαιροποιήσεις ασφαλείας**. Αν και το λειτουργικό σύστημα θα συνεχίσει να λειτουργεί, η απουσία νέων επιδιορθώσεων θα το καθιστά όλο και πιο ευάλωτο σε επιθέσεις (π.χ. malware, ransomware), καθώς εκμεταλλεύονται γνωστές ευπάθειες που δεν θα έχουν διορθωθεί.

Η μοναδική βιώσιμη εναλλακτική για διασφάλιση της ασφάλειας και της συμμόρφωσης είναι η μετάβαση στα **Windows 11**, το οποία ενσωματώνει αυξημένα χαρακτηριστικά προστασίας. Βασική προϋπόθεση λειτουργίας αποτελεί η ύπαρξη **TPM 2.0 (ένα chip πάνω στην motherboard)**, καθώς η Microsoft το χαρακτηρίζει «μη διαπραγματεύσιμο» στοιχείο προηγμένης ασφάλειας. Το TPM 2.0 λειτουργεί ως hardware-based root of trust και υποστηρίζει χαρακτηριστικά όπως BitLocker, Windows Hello και προστασία από firmware επιθέσεις.

Ωστόσο, **η πλειονότητα των υπαρχόντων εταιρικών υπολογιστών δεν διαθέτει TPM 2.0**. Παρά το γεγονός ότι σε ορισμένες μητρικές πλακέτες υπάρχει δυνατότητα ενεργοποίησης TPM μέσω BIOS/UEFI, τα εργαλεία και οι γνώσεις που απαιτούνται για τη διάγνωση και ενεργοποίηση του TPM σε μεγάλη κλίμακα ενδέχεται να αποτελέσουν σημαντική πρόκληση.

Συνεπώς, για να διασφαλιστεί η **συνέχεια των ενημέρωσεων** ασφαλείας μετά την ημερομηνία λήξης υποστήριξης των Windows 10, απαιτείται η **αναβάθμιση ή αντικατάσταση** των υπολογιστών που δεν πληρούν τις ελάχιστες προϋποθέσεις του Windows 11 έτσι η εταιρία εξασφαλίζει ότι η εταιρική πλατφόρμα υπολογιστών θα παραμένει ασφαλής, ενημερωμένη και συμμορφωμένη με τα πιο αυστηρά πρότυπα κυβερνοασφάλειας.

# Υποδομή Θεσσαλονίκης

Ο εξοπλισμός του παραρτήματος της Θεσσαλονίκης αποτελείται από servers και υποστηρικτικά συστήματα που βρίσκονται πλέον σε προχωρημένο στάδιο παλαιότητας και έχουν καταστεί τεχνολογικά ξεπερασμένα. Ο εξοπλισμός αυτός είναι **end of life** και **end of support**, γεγονός που σημαίνει πως δεν υποστηρίζεται πλέον από τον κατασκευαστή και δεν υπάρχουν διαθέσιμα επίσημα ανταλλακτικά για την αποκατάσταση οποιασδήποτε βλάβης.

Η παραμονή σε αυτή την κατάσταση συνεπάγεται σοβαρό επιχειρησιακό ρίσκο. Ακόμη και μία απλή βλάβη σε κάποιο κρίσιμο εξάρτημα του hardware μπορεί να οδηγήσει σε **ολική αδυναμία λειτουργίας του παραρτήματος**, με άμεσο αντίκτυπο στην παροχή υπηρεσιών προς πελάτες και συνεργάτες της περιοχής. Η απουσία ανταλλακτικών σημαίνει ότι η αποκατάσταση μιας βλάβης θα είναι είτε αδύνατη είτε εξαιρετικά χρονοβόρα και δαπανηρή, καθώς θα απαιτείται η αναζήτηση μεταχειρισμένων ή μη πιστοποιημένων εξαρτημάτων, χωρίς καμία εγγύηση αξιοπιστίας.

Επιπλέον, η χρήση παρωχημένου εξοπλισμού περιορίζει τις δυνατότητες της υποδομής για υποστήριξη σύγχρονων τεχνολογικών απαιτήσεων, αυξάνει την πιθανότητα τεχνικών προβλημάτων και ενισχύει τις ευπάθειες έναντι κυβερνοαπειλών. Έτσι θεωρείται επιβεβλημένη η **ολική αντικατάσταση του εξοπλισμού του παραρτήματος Θεσσαλονίκης**, με λύσεις σύγχρονες και υποστηριζόμενες, ώστε να εξασφαλιστεί η απρόσκοπτη λειτουργία, η διαθεσιμότητα των υπηρεσιών και η συμμόρφωση με τα σύγχρονα πρότυπα ασφαλείας και αξιοπιστίας.

# Backups Desktops χρηστών

Η διαδικασία λήψης αντιγράφων ασφαλείας των desktop υπολογιστών των χρηστών βασίζεται σήμερα στη χρήση του λογισμικού **Symantec SLO (Desktop Laptop Option)**. Μέσω της λύσης αυτής, λαμβάνονται αντίγραφα ασφαλείας μόνο για συγκεκριμένους καταλόγους, όπως το **Desktop** και τα **My Documents**, με στόχο την προστασία των βασικών προσωπικών αρχείων εργασίας των χρηστών.

Ωστόσο, το συγκεκριμένο λογισμικό αλλά και ο server βρίσκεται πλέον σε καθεστώς **end of life** και **end of support**. Αυτό σημαίνει ότι η Symantec δεν παρέχει πλέον ενημερώσεις, patches ασφαλείας ή τεχνική υποστήριξη για το προϊόν αυτό, και δεν έχουμε ανανεώσει της άδειες χρήσης. Η συνέχιση της χρήσης του θέτει την εταιρία σε άμεσο κίνδυνο, τόσο από την άποψη της ασφάλειας των δεδομένων όσο και από πλευράς συμμόρφωσης με κανονιστικά πλαίσια (GDPR, πολιτικές εταιρικής ασφάλειας).

Η απουσία υποστήριξης συνεπάγεται πως σε περίπτωση που προκύψει τεχνικό πρόβλημα, δυσλειτουργία ή αστοχία του λογισμικού, δεν θα υπάρχει τρόπος άμεσης αποκατάστασης ή διόρθωσης. Παράλληλα, οι δυνατότητες του DLO v1.0 είναι πλέον ξεπερασμένες σε σχέση με τις σύγχρονες ανάγκες ενός οργανισμού για πλήρη, αυτοματοποιημένη, ασφαλή και κεντρικά διαχειριζόμενη λήψη αντιγράφων ασφαλείας των endpoint συσκευών.

Η επένδυση στην αναβάθμιση των licenses αλλά και του software θα διασφαλίσει την προστασία των προσωπικών αρχείων των χρηστών, θα μειώσει τον επιχειρησιακό κίνδυνο και θα ενισχύσει τη συνολική στρατηγική ασφάλειας των δεδομένων της εταιρίας.

# Εικονικά ετήσια αντίγραφα ασφαλείας χρηστών

Στο πλαίσιο της στρατηγικής ασφάλειας δεδομένων, η εταιρία μας ακολουθούσε επί σειρά ετών τη διαδικασία λήψης **ετήσιων εικονικών αντιγράφων ασφαλείας (images)** των desktop υπολογιστών των χρηστών. Συγκεκριμένα, πραγματοποιούνταν **μία φορά τον χρόνο**, συνήθως κατά τον μήνα Αύγουστο, ώστε να δημιουργείται πλήρες image του κάθε υπολογιστή. Η διαδικασία αυτή πραγματοποιούνταν με χρήση του λογισμικού **EaseUS**, με σκοπό τη διασφάλιση της δυνατότητας πλήρους επαναφοράς του συστήματος σε περίπτωση σοβαρής βλάβης, χωρίς την ανάγκη επαναγκατάστασης από την αρχή.

Η διαδικασία λήψης του ετήσιου image ήταν χρονοβόρα, καθώς η δυναμικότητα υλοποίησης ήταν περίπου **1 υπολογιστής την ημέρα**, λόγω του όγκου των δεδομένων και του τρόπου οργάνωσης της εργασίας. Στο παρελθόν, η συγκεκριμένη διαδικασία υλοποιούνταν με ευθύνη και επίβλεψη του προσωπικού του τμήματος **NSS (προσωπικό ασφαλείας τον Αύγουστο )**.

Δυστυχώς, εδώ και δύο χρόνια, λόγω έλλειψης προσωπικού στο τμήμα, η διαδικασία αυτή **δεν τηρείται πλέον**. Το αποτέλεσμα είναι ότι σήμερα η πλειονότητα των υπολογιστών δεν διαθέτει πρόσφατο πλήρες image, κάτι που αυξάνει σημαντικά τον χρόνο και την πολυπλοκότητα αποκατάστασης σε περίπτωση βλάβης. Εκτιμάται ότι σε περίπτωση αστοχίας hardware ή σοβαρού προβλήματος λειτουργικού συστήματος, η πλήρης αποκατάσταση ενός υπολογιστή χρήστη μπορεί να απαιτήσει **έως και τέσσερις εργάσιμες ημέρες**, ενώ με πρόσφατο image ο χρόνος αυτός θα μπορούσε να περιοριστεί σε **λιγότερο από μία ημέρα**.

Η απουσία της διαδικασίας αυτής δημιουργεί αυξημένο επιχειρησιακό ρίσκο και μειώνει τη διαθεσιμότητα του ανθρώπινου δυναμικού, καθώς οι χρήστες παραμένουν χωρίς λειτουργικό υπολογιστή για σημαντικό χρονικό διάστημα. Το Τμήμα Πληροφορικής θεωρεί αναγκαία την **επανενεργοποίηση και αναβάθμιση της διαδικασίας λήψης πλήρων εικονικών αντιγράφων ασφαλείας**, με στόχο να διασφαλιστεί η ταχεία επαναφορά σε περιπτώσεις βλάβης και να ενισχυθεί η συνολική επιχειρησιακή συνέχεια της εταιρίας.

# Πλατφόρμα UNIXFOR Cloud

Η πλατφόρμα **UNIXFOR Cloud**, που βασίζεται στη λύση **OwnCloud**, αποτελεί το βασικό μας εσωτερικό σύστημα για την ασφαλή διαμοίραση αρχείων και την απομακρυσμένη πρόσβαση σε έγγραφα και δεδομένα. Παρά τη σημαντική της συμβολή στη διευκόλυνση της καθημερινής εργασίας και της συνεργασίας μεταξύ των χρηστών/πελατων/συνεργατών, η πλατφόρμα λειτουργεί πλέον σε **παλαιότερη έκδοση** που χρήζει άμεσης αναβάθμισης. Η υφιστάμενη έκδοση του OwnCloud δεν διαθέτει τις τελευταίες βελτιώσεις ασφαλείας και λειτουργικότητας, ενώ η έλλειψη αναβαθμίσεων αυξάνει τον κίνδυνο εμφάνισης ευπαθειών και τεχνικών προβλημάτων που θα μπορούσαν να θέσουν σε κίνδυνο τα εταιρικά δεδομένα.

Πέρα από την ανάγκη αναβάθμισης της πλατφόρμας, έχει προκύψει και ζήτημα επάρκειας αποθηκευτικού χώρου. Η συνεχής αύξηση του όγκου των δεδομένων και των αρχείων που διακινούνται μέσω του OwnCloud έχει οδηγήσει τα διαθέσιμα αποθηκευτικά μέσα στα όρια τους >100GB , με αποτέλεσμα να δημιουργείται πλέον **άμεση ανάγκη επέκτασης των χώρων** για την κάλυψη των τρεχουσών και μελλοντικών αναγκών των χρηστών και των έργων της εταιρίας.

Το Τμήμα Πληροφορικής εισηγείται την υλοποίηση ενός **σχεδίου αναβάθμισης της πλατφόρμας OwnCloud στην τελευταία έκδοση**, καθώς και την ενίσχυση της υποδομής αποθήκευσης, ώστε να διασφαλιστεί η ασφάλεια, η επεκτασιμότητα και η απρόσκοπτη λειτουργία του UNIXFOR Cloud στο πλαίσιο των σύγχρονων επιχειρησιακών αναγκών.

# Indicators of Compromise - Case management & Monitoring

Στο πλαίσιο της πολιτικής κυβερνοασφάλειας της εταιρίας, η παρακολούθηση **Indicators of Compromise (IoC)** και η διαχείριση περιστατικών μέσω συστημάτων **case management** αποτελούν κρίσιμα στοιχεία για την έγκαιρη ανίχνευση και απόκριση σε κυβερνοαπειλές. Η διαδικασία αυτή, όταν εκτελείται σωστά, επιτρέπει την άμεση αναγνώριση ύποπτων συμπεριφορών, την αποτροπή εξάπλωσης περιστατικών ασφαλείας και την τεκμηριωμένη διαχείριση κάθε συμβάντος έως την πλήρη επίλυσή του.

Δυστυχώς, λόγω της **έλλειψης προσωπικού στο τμήμα NSS**  τα τελευταία χρόνια, οι διαδικασίες αυτές **δεν εκτελούνται πλέον με τον απαιτούμενο βαθμό πληρότητας και συστηματικότητας**. Δεν γίνεται επαρκής ανάλυση των logs, των alerts και των indicators που καταγράφονται από τα συστήματα ασφάλειας (firewall, endpoint protection, EDR/XDR monitoring tools), με αποτέλεσμα κρίσιμα σημάδια παραβίασης ή κακόβουλης δραστηριότητας να είναι πιθανό να περάσουν απαρατήρητα.

Επιπλέον, η διαδικασία **case management monitoring** —δηλαδή η τεκμηριωμένη καταγραφή, παρακολούθηση και διαχείριση των περιστατικών ασφάλειας— δεν τηρείται με συνέπεια. Αυτό έχει ως συνέπεια:

* να καθυστερεί η απόκριση σε συμβάντα,
* να μειώνεται η ικανότητα της εταιρίας να αποδείξει συμμόρφωση σε ελέγχους ή audits,
* και να υπονομεύεται η συνολική στρατηγική ασφάλειας.

Η κατάσταση αυτή αυξάνει σημαντικά το **ρίσκο παραβίασης της υποδομής μας**, καθώς και τις πιθανότητες να αντιμετωπίσουμε μελλοντικά περιστατικά ασφαλείας με ανεπαρκή τεκμηρίωση, περιορισμένη δυνατότητα ανάλυσης αιτιών και μεγαλύτερη δυσκολία στην αποκατάσταση.

Το Τμήμα Πληροφορικής θεωρεί επιτακτική ανάγκη την **ενίσχυση του ανθρώπινου δυναμικού ή την αξιοποίηση managed security υπηρεσιών (SOC, MDR)** ώστε να αποκατασταθεί το monitoring των IoC και η ορθή διαχείριση των περιστατικών με σύγχρονα εργαλεία και τεκμηριωμένες διαδικασίες. Μόνο έτσι θα εξασφαλιστεί η πραγματική προστασία της υποδομής και η συμμόρφωση της εταιρίας με τα διεθνή πρότυπα και τις ρυθμιστικές απαιτήσεις.

# Τηλεφωνικά κέντρα της εταιρίας

Σήμερα, τα τηλεφωνικά κέντρα της εταιρίας τόσο στην Αθήνα όσο και στο παράρτημα της Θεσσαλονίκης βασίζονται σε **on-premise υποδομή**, η οποία λειτουργεί με λογισμικό **Asterisk** και φιλοξενείται σε τοπικούς servers. Αν και η λύση αυτή υποστήριξε επαρκώς την επικοινωνία της εταιρίας κατά το παρελθόν και μέχρι σήμερα, παρουσιάζει πλέον σοβαρούς περιορισμούς και αυξημένους κινδύνους για τη λειτουργική συνέχεια και την ποιότητα των υπηρεσιών προς τους πελάτες.

Η λειτουργία των τηλεφωνικών κέντρων πραγματοποιείται **χωρίς εξωτερική υποστήριξη**, ενώ οι servers στους οποίους φιλοξενούνται δεν καλύπτονται από ενεργά συμβόλαια τεχνικής υποστήριξης. Αυτό σημαίνει ότι σε περίπτωση **βλάβης hardware ή προβλήματος στο λογισμικό**, η εταιρία θα αντιμετωπίσει σημαντικές δυσκολίες στην άμεση αποκατάσταση της λειτουργίας του τηλεφωνικού κέντρου. Το ενδεχόμενο αυτό θα έχει άμεσο αντίκτυπο στην **επικοινωνία με πελάτες, συνεργάτες και κρίσιμες υπηρεσίες**, καθώς θα διακοπεί η δυνατότητα εξυπηρέτησης εισερχόμενων και εξερχόμενων κλήσεων για αβέβαιο χρονικό διάστημα.

Η παραμονή σε αυτό το καθεστώς δημιουργεί σοβαρό επιχειρησιακό ρίσκο, καθώς η επικοινωνία με τους πελάτες αποτελεί βασικό πυλώνα της αξιοπιστίας και της εμπορικής λειτουργίας της εταιρίας.

Το Τμήμα Πληροφορικής προτείνει ως **στρατηγική λύση** τη μετάβαση των τηλεφωνικών κέντρων σε **cloud PBX υποδομή με εξωτερική τεχνική υποστήριξη**, η οποία θα προσφέρει:

* υψηλή διαθεσιμότητα και ανθεκτικότητα μέσω γεωγραφικά κατανεμημένων data centers,
* ευελιξία στην επεκτασιμότητα (π.χ. εύκολη προσθήκη νέων γραμμών/χρηστών),
* προηγμένα εργαλεία παρακολούθησης και διαχείρισης κλήσεων,
* συμβατότητα με σύγχρονα συστήματα CRM και πλατφόρμες επικοινωνίας,
* και πάνω απ’ όλα **εγγυημένη τεχνική υποστήριξη** από εξειδικευμένους παρόχους.

Με αυτόν τον τρόπο η εταιρία θα εξασφαλίσει την **αδιάλειπτη λειτουργία της επικοινωνίας της με τους πελάτες**, θα μειώσει το ρίσκο διακοπής της επιχειρησιακής συνέχειας και θα ευθυγραμμιστεί με τα πρότυπα των σύγχρονων οργανισμών.

# Software τέλους ζωής

Η υποδομή της εταιρίας εξακολουθεί να βασίζεται σε ορισμένα κομβικά λογισμικά και εφαρμογές, τα οποία βρίσκονται σε κατάσταση **τέλους ζωής (end of life)** και δεν υποστηρίζονται πλέον επίσημα από τους κατασκευαστές τους. Χαρακτηριστικά παραδείγματα αποτελούν οι εφαρμογές ERP που έχουν αναπτυχθεί ή βασίζονται σε **Oracle Forms 4.5, 8 και 9**, καθώς και άλλες αντίστοιχες πλατφόρμες παλαιάς τεχνολογίας.

Η χρήση παρωχημένων λογισμικών εγκυμονεί πολλαπλούς κινδύνους για την εταιρία. Αφενός, τα συστήματα αυτά δεν λαμβάνουν ενημερώσεις ασφαλείας ή διορθωτικά patches, με αποτέλεσμα να περιέχουν γνωστές ευπάθειες που μπορούν να αξιοποιηθούν από κακόβουλους παράγοντες. Αφετέρου, η έλλειψη τεχνικής υποστήριξης καθιστά ιδιαίτερα δύσκολη και χρονοβόρα την αποκατάσταση βλαβών ή την αντιμετώπιση λειτουργικών προβλημάτων, ενώ η εξεύρεση εξειδικευμένων συνεργατών για τη συντήρηση ή αναβάθμισή τους είναι πλέον περιορισμένη και κοστοβόρα.

Επιπλέον, η παραμονή σε τέτοιες πλατφόρμες περιορίζει σημαντικά τη δυνατότητα ενσωμάτωσης σύγχρονων τεχνολογιών, την αυτοματοποίηση διαδικασιών και την υλοποίηση ψηφιακών έργων που θα μπορούσαν να βελτιώσουν την αποτελεσματικότητα και την ανταγωνιστικότητα της εταιρίας. Το Τμήμα Πληροφορικής θεωρεί αναγκαία τη χάραξη **σχεδίου σταδιακής απεξάρτησης από το παρωχημένο λογισμικό και μετάβασης σε σύγχρονες λύσεις**, που θα προσφέρουν ασφάλεια, επεκτασιμότητα και μακροχρόνια υποστήριξη.

# Συμπέρασμα

Σκοπός του παρόντος εγγράφου είναι να παρέχει στη Διοίκηση της UNIXFOR μια ολοκληρωμένη, αντικειμενική, σφαιρική και σαφή εικόνα της υφιστάμενης κατάστασης της υποδομής πληροφορικής της εταιρίας, όπως αυτή έχει διαμορφωθεί μετά από μια παρατεταμένη περίοδο περιορισμένων επενδύσεων και στελέχωσης. Μέσα από την ανάλυση μόνο των βασικών στοιχείων και προκλήσεων που αντιμετωπίζουμε σήμερα, το έγγραφο αυτό επιδιώκει να καταγράψει με υπευθυνότητα τα κρίσιμα θέματα που απαιτούν την προσοχή και στήριξη της Διοίκησης, ώστε να υπάρχει σφαιρική κατανόηση των κινδύνων και να τεθούν οι βάσεις για τη λήψη αποφάσεων που θα διασφαλίσουν τη λειτουργική συνέχεια, την ασφάλεια και την ανάπτυξη της εταιρίας στο μέλλον.

Η παρούσα ενημέρωση δεν αποσκοπεί μόνο στην ανάδειξη των προβλημάτων, αλλά και στο να συμβάλει στη χάραξη μιας στρατηγικής αναβάθμισης και ενίσχυσης της υποδομής, με τρόπο που θα ανταποκρίνεται στις ανάγκες και στις προκλήσεις του σύγχρονου τεχνολογικού περιβάλλοντος.