# Νομικό και κανονιστικό τοπίο κυβερνοασφάλειας

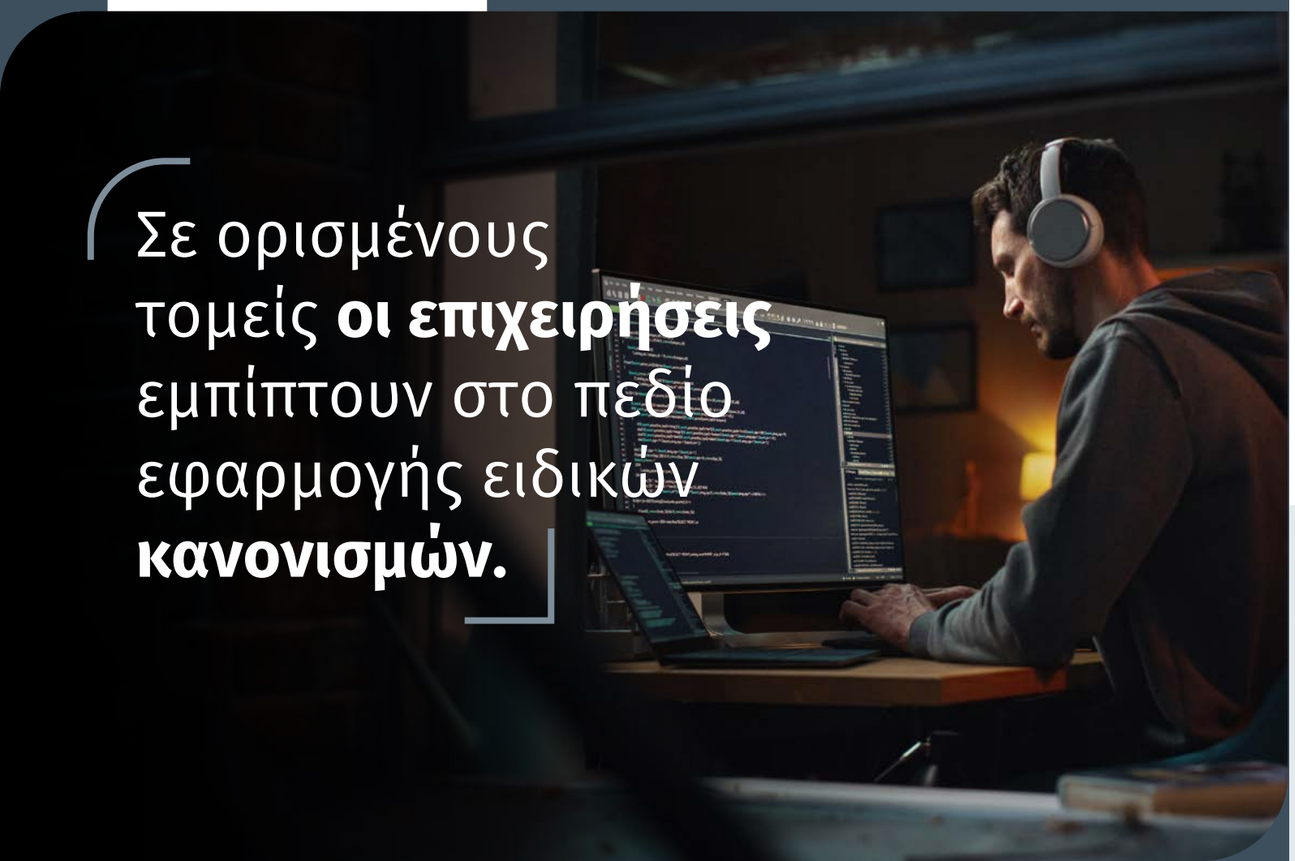
## Προκλήσεις & ευκαιρίες

Building a better working world

Microsoft


# Περιεχόμενα

# 1 Εισαγωγή



Σε ορισμένους τομείς **οι επιχειρήσεις** εμπίπτουν στο πεδίο εφαρμογής ειδικών **κανονισμών.**

## 1.1 Σκοπός της έκθεσης

Οι σημαντικές προκλήσεις που προκύπτουν από την ψηφιοποίηση του περιβάλλοντος λειτουργίας των επιχειρήσεων, καθώς και από μια σειρά νέων αναδυόμενων τεχνολογιών, έχουν διαμορφώσει ένα δυναμικό και πολύπλοκο κανονιστικό περιβάλλον όπου οι επιχειρήσεις υποχρεούνται να τηρούν πολλαπλές απαιτήσεις συμμόρφωσης σε εθνικό και περιφερειακό επίπεδο. Επιπλέον, σε ορισμένους τομείς, οι επιχειρήσεις εμπίπτουν στο πεδίο εφαρμογής ειδικών κανονισμών. Οι κανονιστικές αλλαγές, σε συνδυασμό με ένα διαρκώς μεταβαλλόμενο τοπίο όσον αφορά τους κινδύνους, τις απειλές και τους σχετικούς παράγοντες (threat actors) αυτών στον κυβερνοχώρο, αυξάνουν την πολυπλοκότητα της διαχείρισης τόσο για τις επιχειρήσεις όσο και για τις ομάδες κυβερνοασφάλειας, καθώς πρέπει να εντοπιστούν περιοχές με συγκλίνοντες ή επικαλυπτόμενους κανονισμούς. Ωστόσο, ταυτόχρονα, αυτό μπορεί να δημιουργήσει ευκαιρίες βελτίωσης για νέους τομείς ανάπτυξης.

Στο πλαίσιο αυτό, η παρούσα έκθεση στοχεύει στα εξής:

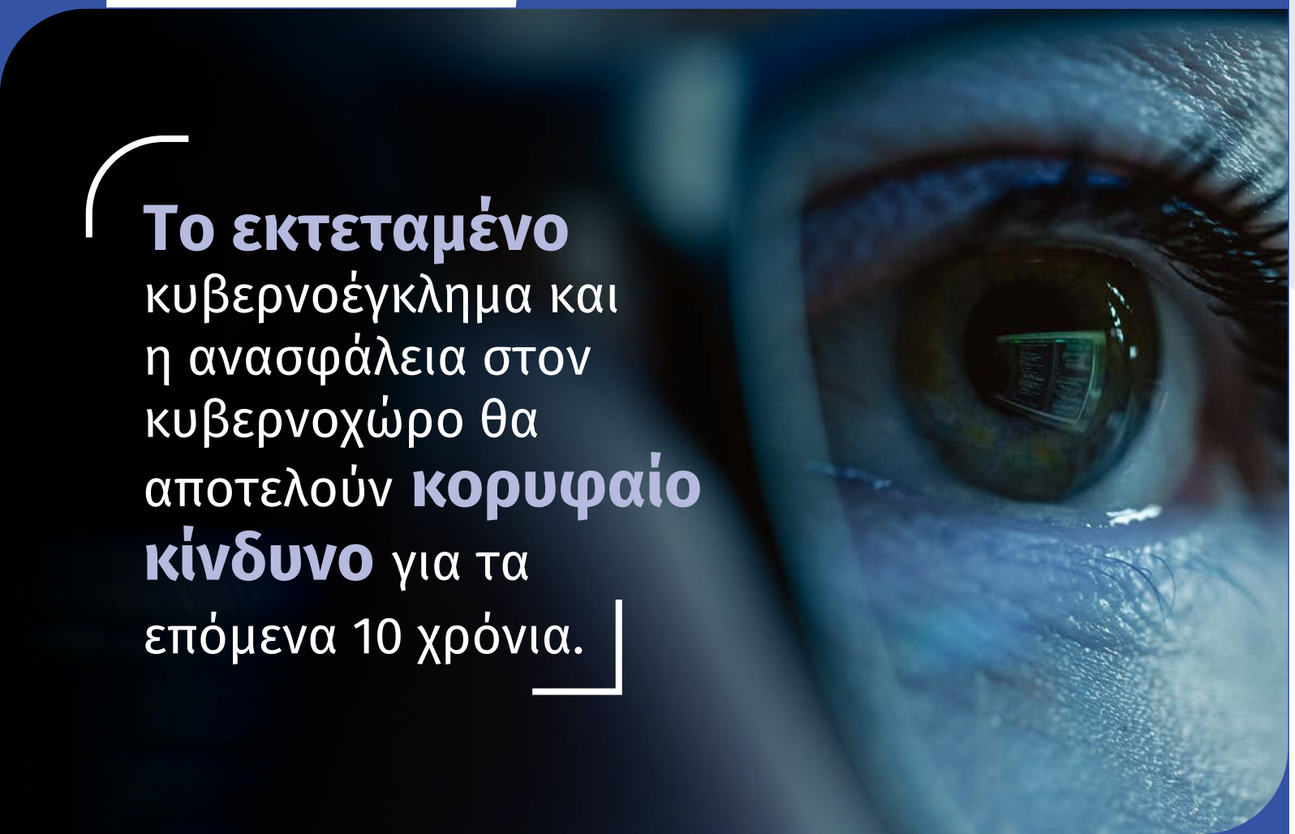
- Παροχή μιας σφαιρικής ανάλυσης του ισχύοντος νομοθετικού και κανονιστικού τοπίου της κυβερνοασφάλειας στην ελληνική αγορά και στην αγορά της ΕΕ
- Προσδιορισμός των προκλήσεων που αντιμετωπίζουν οι επιχειρήσεις στην προσπάθειά τους να διασφαλίσουν τη συμμόρφωση με την πληθώρα των απαιτήσεων
- Επισήμανση του τρόπου με τον οποίο η Microsoft μπορεί να υποστηρίξει την αντιμετώπιση αυτών των προκλήσεων και να επιτρέψει στις επιχειρήσεις να αποκτήσουν ανταγωνιστικό πλεονέκτημα και να επιτύχουν την επιχειρησιακή αριστεία

## 1.2 Αντικείμενο της έκθεσης

Το αντικείμενο της παρούσας έκθεσης σχετίζεται με τους νόμους και τους κανονισμούς για την κυβερνοασφάλεια που ισχύουν σήμερα για τις επιχειρήσεις που έχουν συσταθεί στην Ελλάδα, καθώς και για τις επιχειρήσεις που λειτουργούν σε περιφερειακή ή παγκόσμια κλίμακα, δηλαδή τους νόμους που εφαρμόζονται από τις ελληνικές αρχές, όπως το Υπουργείο Ψηφιακής Διακυβέρνησης, την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, και την Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθώς και από την Ευρωπαϊκή Ένωση.

Επιπλέον, προκειμένου να διευρυνθεί περαιτέρω το θέμα και να αναλυθούν εις βάθος οι προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις στην Ελλάδα, διεξήχθη μια έρευνα που περιλάμβανε διάφορες πτυχές του εν λόγω ζητήματος. Στην έρευνα αυτή συμμετείχαν επαγγελματίες που ασχολούνται με θέματα κυβερνοασφάλειας και προστασίας του απορρήτου (π.χ. Επικεφαλής Προστασίας Πληροφοριών (CISO), Διευθυντές Ασφάλειας Πληροφοριών και Υπεύθυνοι Προστασίας Δεδομένων) και εργάζονται σε επιχειρήσεις που δραστηριοποιούνται στην Ελλάδα σε διάφορους κλάδους, όπως ο χρηματοπιστωτικός κλάδος, οι κλάδοι της ενέργειας και των τηλεπικοινωνιών, και ο δημόσιος τομέας.

# 2 Υπόβαθρο της έκθεσης

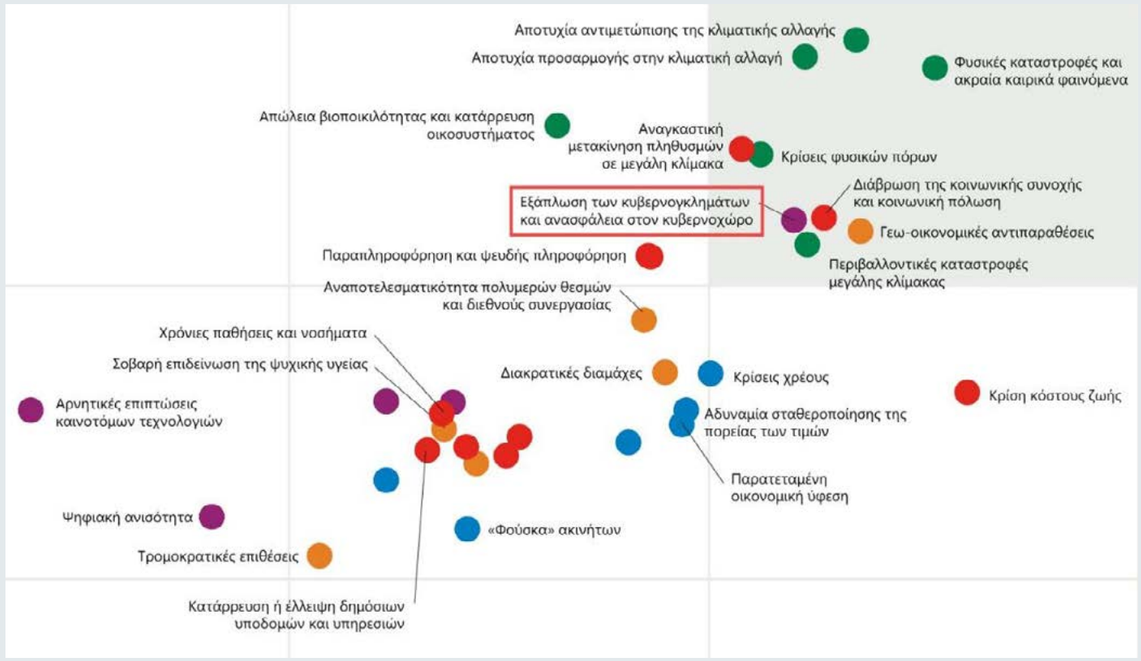


**Το εκτεταμένο** κυβερνοέγκλημα και η ανασφάλεια στον κυβερνοχώρο θα αποτελούν **κορυφαίο κίνδυνο** για τα επόμενα 10 χρόνια.

## 2.1 Επισκόπηση του τοπίου των κυβερνοαπειλών

Ο ανεξέλεγκτος ρυθμός ψηφιοποίησης, σε συνδυασμό με την ταχεία υιοθέτηση νέων τεχνολογιών, οδηγεί σε ευπάθειες τις οποίες μπορούν να εκμεταλλευτούν διάφοροι παράγοντες, όπως κυβερνοεγκληματίες, εθνικά κράτη ή ακόμη και εσωτερικοί κακόβουλοι χρήστες (insiders), για προσωπικό, ιδεολογικό, οικονομικό ή γεωπολιτικό όφελος. Ιστορικά, οι κυβερνοαπειλές εξελίσσονται παράλληλα με τις σχετικές τεχνολογικές εξελίξεις.

Οι πρώιμες περιπτώσεις των «script kiddies», που ξεκινούσαν επιθέσεις για να διασκεδάσουν, να πειραματιστούν ή να αποκτήσουν φήμη, έδωσαν σταδιακά τη θέση τους σε πιο εξελιγμένους επιτιθέμενους, όπως insiders, εγκληματικά δίκτυα και threat actors που χρηματοδοτούνται από κρατικούς φορείς, καθώς και, πιο πρόσφατα, σε ρομποτικές επιθέσεις με τη βοήθεια της τεχνητής νοημοσύνης και της μηχανικής μάθησης.



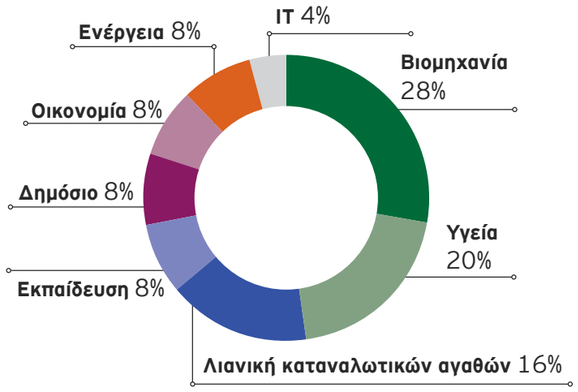

Είναι προφανές ότι η κυβερνοασφάλεια αποτελεί πλέον κύριο μέλημα και είναι συνεχώς παρούσα στις ημερήσιες διατάξεις των Διοικητικών Συμβουλίων, καθώς αρχίζει να γίνεται εμφανές ότι κάθε επιχείρηση βρίσκεται σε κίνδυνο και ότι η απειλή μιας κυβερνοεπίθεσης είναι πιο πιθανή και πιο τρομακτική από ποτέ. Για την ακρίβεια, σύμφωνα με την έκθεση Global Risk Report 2023 του Παγκόσμιου Οικονομικού Φόρουμ[1], οι κυβερνοεπιθέσεις σε υποδομές ζωτικής σημασίας αποτελούν έναν από τους πέντε κορυφαίους κινδύνους για το 2023 με τις μεγαλύτερες δυνητικές επιπτώσεις σε παγκόσμια κλίμακα, ενώ το εκτεταμένο κυβερνοέγκλημα και η ανασφάλεια στον κυβερνοχώρο θα αποτελούν κορυφαίο κίνδυνο για τα επόμενα 10 χρόνια, τον οποίο υπερβαίνουν μόνο οι περιβαλλοντικοί και κοινωνικοί κίνδυνοι (Εικόνα 1).

[1] *https://www.weforum.org/reports/global-risks-report-2023/*

Τα τελευταία χρόνια οι κυβερνοεπιθέσεις έχουν αυξηθεί εκθετικά, κάτι που ισχύει και για την περίοδο 2021-2022, τόσο από άποψη αριθμού όσο και από άποψη σοβαρότητας, σύμφωνα με την τελευταία έκθεση Threat Landscape[2] του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA). Ενδεικτικά, η συχνότητα συγκεκριμένων επιθέσεων, όπως οι επιθέσεις ransomware και το ηλεκτρονικό ψάρεμα (phishing), έχει αυξηθεί σημαντικά, ιδίως ως αποτέλεσμα της στροφής προς την τηλεργασία, η οποία θεωρήθηκε ως εξαιρετικά σημαντική ευκαιρία από τους επιτιθέμενους που επιδιώκουν να επωφεληθούν από το μεταβαλλόμενο εργασιακό περιβάλλον.

Πιο συγκεκριμένα, σύμφωνα με την έκθεση Cost of a Data Breach 2022[3] της IBM, την περασμένη χρονιά καταγράφηκε σημαντική αύξηση των παραβιάσεων που προκλήθηκαν από επιθέσεις ransomware, η οποία φτάνει το 41% σε σχέση με το 2021. Οι παραβιάσεις που προκλήθηκαν από εκστρατείες ηλεκτρονικού ψαρέματος (phishing campaigns) αυξήθηκαν επίσης κατά 48%, αποτελώντας τον πιο συνηθισμένο φορέα αρχικής πρόσβασης σύμφωνα με την τελευταία έκθεση Threat Landscape του ENISA, ενώ σημειώνεται ότι το 40% όλων των κυβερνοαπειλών πραγματοποιείται πλέον απευθείας μέσω της εφοδιαστικής αλυσίδας.

Επιπλέον, σύμφωνα με την έκθεση Digital Defense Report 2022[4] της Microsoft, περίπου 710 εκατομμύρια μηνύματα ηλεκτρονικού ψαρέματος μπλοκάρονται εβδομαδιαίως από τις σχετικές λύσεις ασφάλειας της Microsoft, ενώ από το 2019 παρατηρείται σταθερή αύξηση των επιθέσεων ransomware. Τα τελευταία ευρήματα (Εικόνα 2) δείχνουν ότι οι κλάδοι που στοχοποιούνται περισσότερο είναι η βιομηχανία (28%) και η υγεία (20%), ακολουθούμενοι από τη λιανική πώληση καταναλωτικών αγαθών (16%).



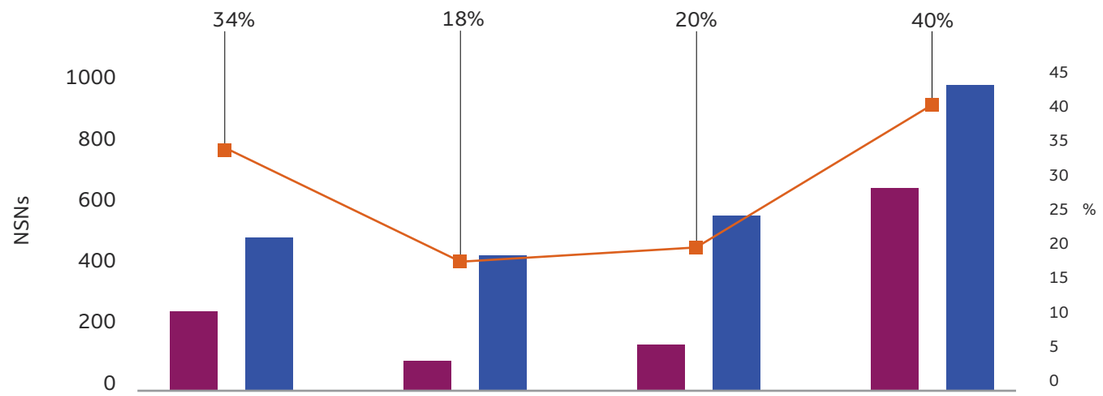

*Εικόνα 2: Περιστατικά και αντιμετώπιση επιθέσεων ransomware*

[2] *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022*
[3] *https://www.ibm.com/reports/data-breach*
[4] *https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022*



Επιπλέον, μετά την εισβολή της Ρωσίας στην Ουκρανία, ο αριθμός των κυβερνοεπιθέσεων που προέρχονται από ομάδες εθνικών κρατών εναντίον κρίσιμων και μη κρίσιμων υποδομών αυξήθηκε σημαντικά. Σύμφωνα με την έκθεση «Threat Intelligence: A year of Russian hybrid warfare in Ukraine» της Microsoft[5], οι κύριες τάσεις που μπορούν να εντοπιστούν μετά την εισβολή της Ρωσίας περιλαμβάνουν την αύξηση χρήσης του ransomware ως αδιαμφισβήτητου καταστροφικού όπλου, τη χρήση διαφορετικών εργαλείων για την απόκτηση αρχικής πρόσβασης σε στόχους και την αυξημένη χρήση των χακτιβιστών (hacktivists) για την προβολή ισχύος. Γενικότερα, σύμφωνα με την ανωτέρω έκθεση Digital Defense, το 40% των ειδοποιήσεων NSN (Nation State Notifications)[6] αφορούσε κρίσιμες υποδομές, με τους παράγοντες απειλών να επικεντρώνονται σε εταιρείες του τομέα της πληροφορικής, χρηματοπιστωτικές υπηρεσίες, συστήματα μεταφορών και υποδομές επικοινωνιών.

**Τάσεις κυβερνοεπιθέσεων από εθνικά κράτη**




Τέλος, όπως επιβεβαιώνεται από την ίδια έκθεση, η έννοια του Cybercrime as a Service (CaaS) αποτελεί μια αυξανόμενη και εξελισσόμενη απειλή παγκοσμίως, με το Phishing as a Service (PhaaS) να αποτελεί ένα χαρακτηριστικό παράδειγμα ολοκληρωμένης υπηρεσίας κυβερνοεγκλήματος που προσφέρεται από κυβερνοεγκληματίες σε συνδρομητική βάση. Η κύρια απειλή που θέτει το PhaaS σχετίζεται με την προσβασιμότητά του, καθώς μπορεί, θεωρητικά, να χρησιμοποιηθεί από κάθε ενδιαφερόμενο επιλέγοντας ένα πρότυπο ή ένα σχέδιο ιστότοπου phishing ανάμεσα στα εκατοντάδες που προσφέρονται, παρέχοντας μια διεύθυνση e-mail για τη λήψη των διαπιστευτηρίων που θα υποκλέπτονται από τα θύματα του ηλεκτρονικού ψαρέματος και, τέλος, πληρώνοντας τον έμπορο του PhaaS σε κρυπτονόμισμα.

[5] *https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf*
[6] *Τα Nation State Notifications (NSN) είναι ειδοποιήσεις που αποστέλλει η Microsoft απευθείας στους πελάτες της, σε περίπτωση που εντοπιστούν παράγοντες εθνικών κρατών που στοχεύουν ή θέτουν σε κίνδυνο τουλάχιστον έναν λογαριασμό στον οργανισμό του πελάτη, και περιλαμβάνουν τις πληροφορίες που χρειάζονται για τη διερεύνηση της δραστηριότητας.*

## 2.2 Οι ταχείες τεχνολογικές εξελίξεις ως βασικός παράγοντας του εξελισσόμενου τοπίου κυβερνοαπειλών

Οι τελευταίες κύριες τεχνολογικές εξελίξεις, ως αποτέλεσμα της προαναφερθείσας ραγδαίας ψηφιοποίησης, μπορούν να εντοπιστούν στους εξής τομείς: Cloud Computing, OT-IoT, Blockchain, Τεχνητή Νοημοσύνη και Μηχανική Μάθηση.

### Cloud Computing

Η επιταχυνόμενη εφαρμογή και ανάπτυξη λύσεων cloud computing αποτελεί σημαντικό παράγοντα για τη συνολική ψηφιοποίηση όλων των κλάδων, ιδίως όπως έχουν διαμορφωθεί οι συνθήκες μετά την πανδημία, όπου το μοντέλο εργασίας από το σπίτι υιοθετείται όλο και περισσότερο από επιχειρήσεις σε όλους τους κλάδους. Η μετάβαση σε τέτοιου είδους λύσεις είναι καθοριστικής σημασίας για την υποστήριξη των όλο και πιο σύνθετων οργανωτικών απαιτήσεων και στόχων, καθώς ενισχύουν την ταχύτητα διάθεσης των προϊόντων στην αγορά και την ευελιξία και τη συνολική αποκρισιμότητα των επιχειρήσεων. Ωστόσο, η μετάβαση σε λύσεις cloud απαιτεί αλλαγή του συνολικού προτύπου ασφάλειας, καθώς οι επιχειρήσεις πρέπει να εξετάσουν στρατηγικές για το cloud που μπορούν να τους προσφέρουν την κατάλληλη υποστήριξη και, ταυτόχρονα, να δώσουν λύσεις στις σχετικές ανησυχίες για την ασφάλεια.

Κατά συνέπεια, η κύρια πρόκληση που αντιμετωπίζουν οι επιχειρήσεις είναι να αποκτήσουν μια σαφέστερη εικόνα και συνολική κατανόηση των λειτουργιών cloud, των διαθέσιμων μοντέλων υπηρεσιών (SaaS, PaaS και IaaS), καθώς και των απαιτήσεων που συνεπάγονται σε επίπεδο ασφάλειας. Για παράδειγμα, η εισαγωγή του μοντέλου επιμερισμένης ευθύνης (shared responsibility model), μέσω του οποίου οι πάροχοι πρέπει να διασφαλίζουν ότι η υποδομή τους και τα δεδομένα των πελατών τους είναι επαρκώς ασφαλισμένα, ενώ οι ίδιοι οι πελάτες πρέπει με τη σειρά τους να διασφαλίζουν ότι εφαρμόζονται ισχυροί έλεγχοι πρόσβασης και ταυτοποίησης, απαιτεί από τους οργανισμούς να καθορίσουν, να εφαρμόσουν και να προσαρμόσουν αναλόγως τις στρατηγικές τους για το cloud, γεγονός που, όπως αναφέρθηκε, απαιτεί βαθύτερη κατανόηση των σχετικών απαιτήσεων ασφάλειας.



### OT / IoT

Η επιχειρησιακή τεχνολογία (OT) αναφέρεται στην παρακολούθηση και λειτουργία των βιομηχανικών συστημάτων και διεργασιών, και της συνολικής υποδομής, μέσω της χρήσης των σχετικών πόρων υλικού και λογισμικού. Οι τεχνολογίες OT και IT συγκλίνουν ταχύτατα, διεκπεραιώνοντας λειτουργίες εξ αποστάσεως και λειτουργίες ανάκτησης δεδομένων, και οδηγώντας έτσι σε νέους φορείς επίθεσης και σε μια συνολικά διευρυμένη επιφάνεια επίθεσης. Επιπλέον, και λόγω της εστίασής τους στα Βιομηχανικά Συστήματα Ελέγχου (ICS), οι επιθέσεις σε υποδομές OT διαφέρουν από τις παραδοσιακές επιθέσεις εναντίον περιβαλλόντων IT, έχοντας δυνητικά απτές συνέπειες στον πραγματικό κόσμο και οδηγώντας ακόμη και σε πραγματική απειλή σοβαρού τραυματισμού ή απώλειας ζωής, ως αποτέλεσμα της διακοπής λειτουργίας των εξαρτημάτων.

Ταυτόχρονα, οι συσκευές Internet of Things (IoT), οι οποίες περιλαμβάνουν εκτυπωτές, κάμερες ασφαλείας και συστήματα ελέγχου φυσικής πρόσβασης, υιοθετούνται με ταχείς ρυθμούς από επιχειρήσεις στον βιομηχανικό κλάδο, αλλά και σε άλλους κλάδους, καθώς είναι ζωτικής σημασίας για την αποτελεσματικότερη υποστήριξη των καθημερινών λειτουργιών. Ομοίως με το OT, οι συσκευές IoT μπορούν να λειτουργήσουν ως πρόσθετα μέσα επιθέσεων, διευρύνοντας σημαντικά την επιφάνεια επίθεσης των επιχειρήσεων, ιδίως μέσω της εκμετάλλευσης μη διαχειριζόμενων συσκευών, και οδηγώντας δυνητικά σε σοβαρή απώλεια δεδομένων. Πιο συγκεκριμένα, οι εκτεθειμένες συσκευές IoT είναι ιδιαίτερα ευάλωτες σε επιθέσεις κακόβουλου λογισμικού (π.χ. μέσω Mirai), μεταξύ άλλων από επιτιθέμενους που χρησιμοποιούν λειτουργίες κακόβουλου λογισμικού με τη μορφή υπηρεσιών (malware as a service), καθώς και σε μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση μέσω μη ασφαλών θυρών που μπορούν να εντοπιστούν μέσω του διαδικτύου, εκμετάλλευσης ευπαθειών και διαδικτυακών εκμεταλλεύσεων μέσω HTTP.

Έτσι, προκειμένου να εξασφαλίσουν επαρκή ασφάλεια για τα οικοσυστήματα OT και IoT, οι επιχειρήσεις πρέπει να καθορίσουν και να εφαρμόσουν ένα κατάλληλο σχέδιο δράσης, το οποίο προϋποθέτει την ταυτοποίηση των σχετικών πόρων, τη βαθύτερη κατανόηση του οικοσυστήματος ευπαθειών, την αξιοποίηση των υφιστάμενων μηχανισμών ασφαλείας, τον καθορισμό ενός συστήματος διακυβέρνησης OT και IoT, και την εφαρμογή των κατάλληλων μηχανισμών ασφαλείας σύμφωνα με τις σχετικές απαιτήσεις.

### Blockchain

Το Blockchain είναι μια αναδυόμενη τεχνολογία με ανερχόμενες εφαρμογές σε κλάδους όπως οι επιχειρήσεις κοινής ωφέλειας και ο τομέας της ενέργειας, καθώς και ο τομέας της τεχνολογίας γενικότερα, καθώς επιλύει μια σειρά από ζητήματα που σχετίζονται με την ιδιοκτησία. Οι τεχνολογίες Blockchain βρίσκονται ακόμη σε πρώιμο στάδιο και έχουν επιφέρει νέες προκλήσεις ασφάλειας που πρέπει να αντιμετωπιστούν. Παρά το γεγονός ότι οι τεχνολογίες Blockchain έχουν συγκεκριμένα χαρακτηριστικά ασφάλειας, καθώς βασίζονται εγγενώς στις αρχές της κρυπτογραφίας, της αποκέντρωσης και της συναίνεσης, ανάλογα και με την εφαρμογή αυτών των τεχνολογιών (με άδεια/ιδιωτική ή χωρίς άδεια/δημόσια), οι γνωστές ευπάθειες των υποδομών μπορούν να χειραγωγηθούν και να αξιοποιηθούν από κακόβουλους παράγοντες. Πιο συγκεκριμένα, οι τεχνολογίες Blockchain είναι ευάλωτες σε διαδεδομένους τύπους επιθέσεων, όπως το phishing, καθώς και σε πιο εξελιγμένους τύπους επιθέσεων, όπως οι επιθέσεις δρομολόγησης (routing) και Sybil[7], απαιτώντας έτσι αποτελεσματική διαχείριση των πορτοφολιών/κλειδιών, διαχείριση ευπαθειών έξυπνων συμβολαίων (smart contracts) και κατάλληλες μεθόδους αντιμετώπισης επιθέσεων phishing.

### Τεχνητή Νοημοσύνη / Μηχανική Μάθηση

Τέλος, οι δυνατότητες και οι λύσεις Τεχνητής Νοημοσύνης (Artificial Intelligence - AI) και Μηχανικής Μάθησης (Machine Learning - ML) χρησιμοποιούνται όλο και περισσότερο σε ποικίλες εφαρμογές, συμπεριλαμβανομένης της αξιοποίησής τους σε εργαλεία βασισμένα στην AI για την ανίχνευση απειλών, τη διαχείριση ευπαθειών, τη συνολική παρακολούθηση και, τελικά, την αντιμετώπιση τυχόν περιστατικών. Ωστόσο, οι λύσεις αυτές είναι επίσης δυνητικά ευάλωτες σε επιθέσεις άμεσης χειραγώγησης δεδομένων που εκμεταλλεύονται τους αλγορίθμους που έχουν υλοποιηθεί και μεταβάλλουν τη λειτουργικότητά τους. Κυριότερα, όμως, οι δυνατότητες AI και ML χρησιμοποιούνται και σε κυβερνοεπιθέσεις, καθώς αυτές γίνονται πιο εξελιγμένες και πολύπλοκες, για την αποτελεσματικότερη πλοήγηση, τον εντοπισμό και την εκμετάλλευση πιθανών ευπαθειών[8].

*[7] Οι επιθέσεις δρομολόγησης είναι κυβερνοεπιθέσεις που στρέφονται εναντίον παρόχων υπηρεσιών διαδικτύου (ISP), με στόχο τη μείωση του χρόνου διαθεσιμότητας και, ως εκ τούτου, την παρεμπόδιση της πρόσβασης των χρηστών στο blockchain. Οι επιθέσεις Sybil είναι κυβερνοεπιθέσεις κατά τις οποίες δημιουργείται ένας μεγάλος αριθμός ψευδώνυμων ταυτοτήτων σε μια υπηρεσία με σκοπό την υπονόμευση του συστήματος φήμης της.*

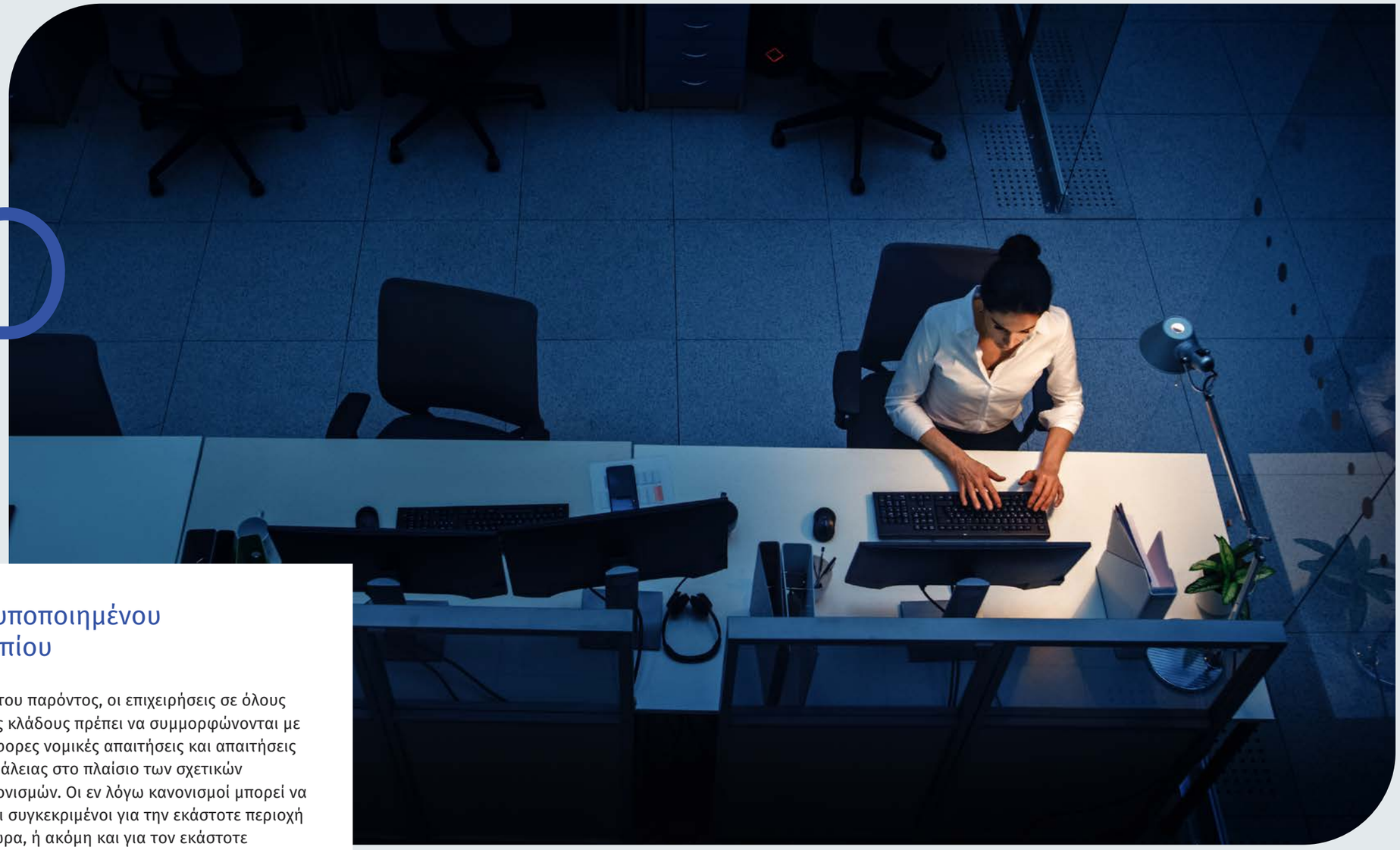
*[8] Οι δυνατότητες AI και ML χρησιμοποιούνται πλέον σε προηγμένες μόνιμες απειλές (APT), επιθέσεις ηλεκτρονικού ψαρέματος και κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS).*

## 2.3 Η ανάγκη δημιουργίας ενός τυποποιημένου νομοθετικού και κανονιστικού τοπίου

Οι ανωτέρω τεχνολογικές εξελίξεις υπαγόρευσαν την ανάγκη για κατάλληλους κανονιστικούς και νομοθετικούς ελέγχους. Ωστόσο, αυτό έχει οδηγήσει σε ραγδαία αύξηση του αριθμού των σχετικών απαιτήσεων, κατακερματίζοντας περαιτέρω το νομοθετικό και κανονιστικό τοπίο στο σύνολό του.

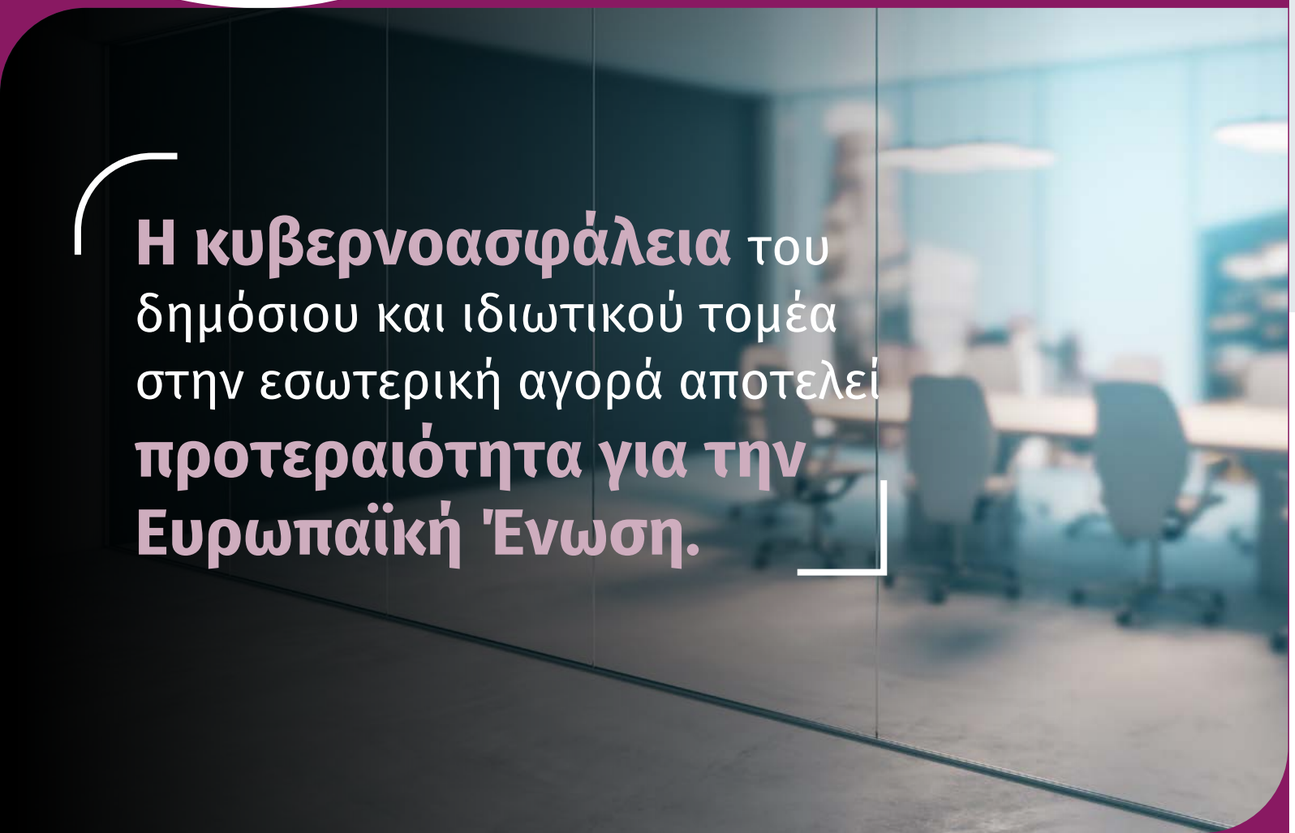
Αυτός ο υψηλός βαθμός κατακερματισμού αποτελεί επίσης σημαντική πρόκληση για την ασφάλεια στον κυβερνοχώρο, καθώς το τοπίο αναμένεται να γίνει ακόμη πιο κατακερματισμένο στο μέλλον και, ως εκ τούτου, η διαχείρισή του θα είναι πιο χρονοβόρα τόσο για τις εταιρείες όσο και για τους ενδιαφερόμενους φορείς.

Επί του παρόντος, οι επιχειρήσεις σε όλους τους κλάδους πρέπει να συμμορφώνονται με διάφορες νομικές απαιτήσεις και απαιτήσεις ασφάλειας στο πλαίσιο των σχετικών κανονισμών. Οι εν λόγω κανονισμοί μπορεί να είναι συγκεκριμένοι για την εκάστοτε περιοχή ή χώρα, ή ακόμη και για τον εκάστοτε κλάδο, και είναι εξαιρετικά δύσκολο να χαρτογραφηθούν σωστά και αποτελεσματικά. Για τον σκοπό αυτό, και συγκεκριμένα σε νομοθετικό-κανονιστικό επίπεδο, θα πρέπει να γίνει προσπάθεια για τη μέγιστη δυνατή τυποποίηση του συνολικού τοπίου, διασφαλίζοντας παράλληλα την παροχή της κατάλληλης καθοδήγησης στις επηρεαζόμενες επιχειρήσεις, ώστε να έχουν μεγαλύτερη επίγνωση των υποχρεώσεών τους και των σχετικών απαιτήσεων που πρέπει να τηρούν.



> Οι κανονισμοί μπορεί να είναι συγκεκριμένοι για την εκάστοτε **περιοχή ή χώρα, ή ακόμη και για τον εκάστοτε κλάδο,** και είναι εξαιρετικά δύσκολο να χαρτογραφηθούν σωστά & αποτελεσματικά.

# 3 Τρέχουσα κατάσταση



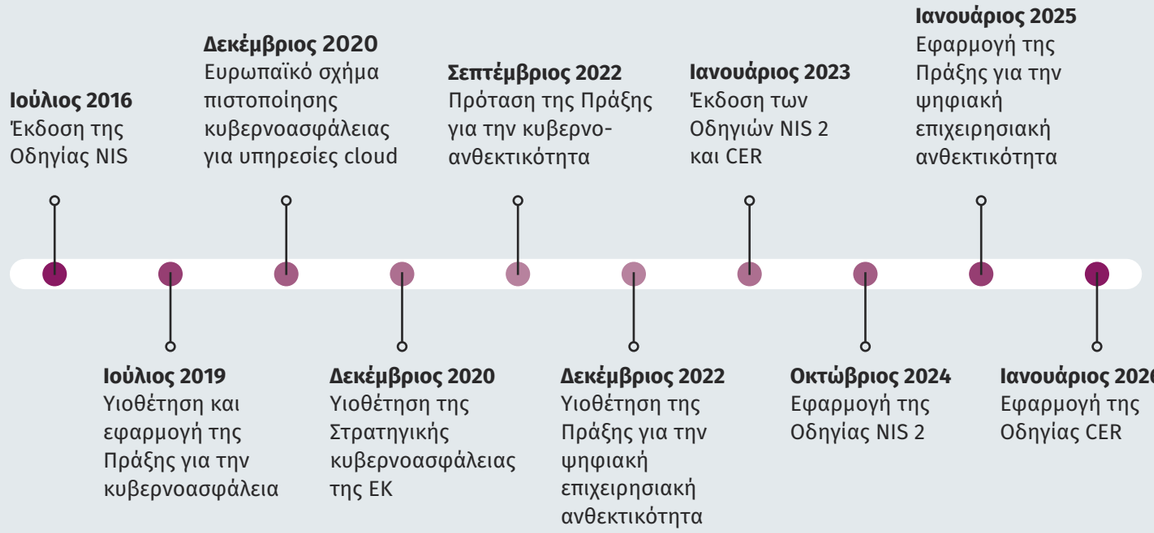
**Η κυβερνοασφάλεια** του δημόσιου και ιδιωτικού τομέα στην εσωτερική αγορά αποτελεί **προτεραιότητα για την Ευρωπαϊκή Ένωση.**

## 3.1 Συνοπτική παρουσίαση

Η κυβερνοασφάλεια του δημόσιου και ιδιωτικού τομέα στην εσωτερική αγορά αποτελεί προτεραιότητα για την Ευρωπαϊκή Ένωση στο πλαίσιο του στρατηγικού της στόχου να καταστεί παγκόσμιος ηγέτης στην ψηφιακή εποχή.

Στο πλαίσιο αυτό, τα θεσμικά όργανα της ΕΕ έχουν υιοθετήσει διάφορες πρωτοβουλίες σε επίπεδο πολιτικών και νομοθετικών πράξεων. Το χρονοδιάγραμμα της εξέλιξης των κανονισμών της ΕΕ για την ασφάλεια στον κυβερνοχώρο έχει ως εξής:

**Χρονοδιάγραμμα κανονισμών της ΕΕ για την κυβερνοασφάλεια**




*Εικόνα 4: Χρονοδιάγραμμα κανονισμών της ΕΕ για την κυβερνοασφάλεια*

Ακολουθώντας τις εξελίξεις στην Ευρωπαϊκή Ένωση, η Ελλάδα έχει υιοθετήσει την Εθνική Στρατηγική Κυβερνοασφάλειας 2020 - 2025 και έχει λάβει ενεργά μέτρα για την αναβάθμιση του επιπέδου ασφάλειας των πληροφοριών στη χώρα.

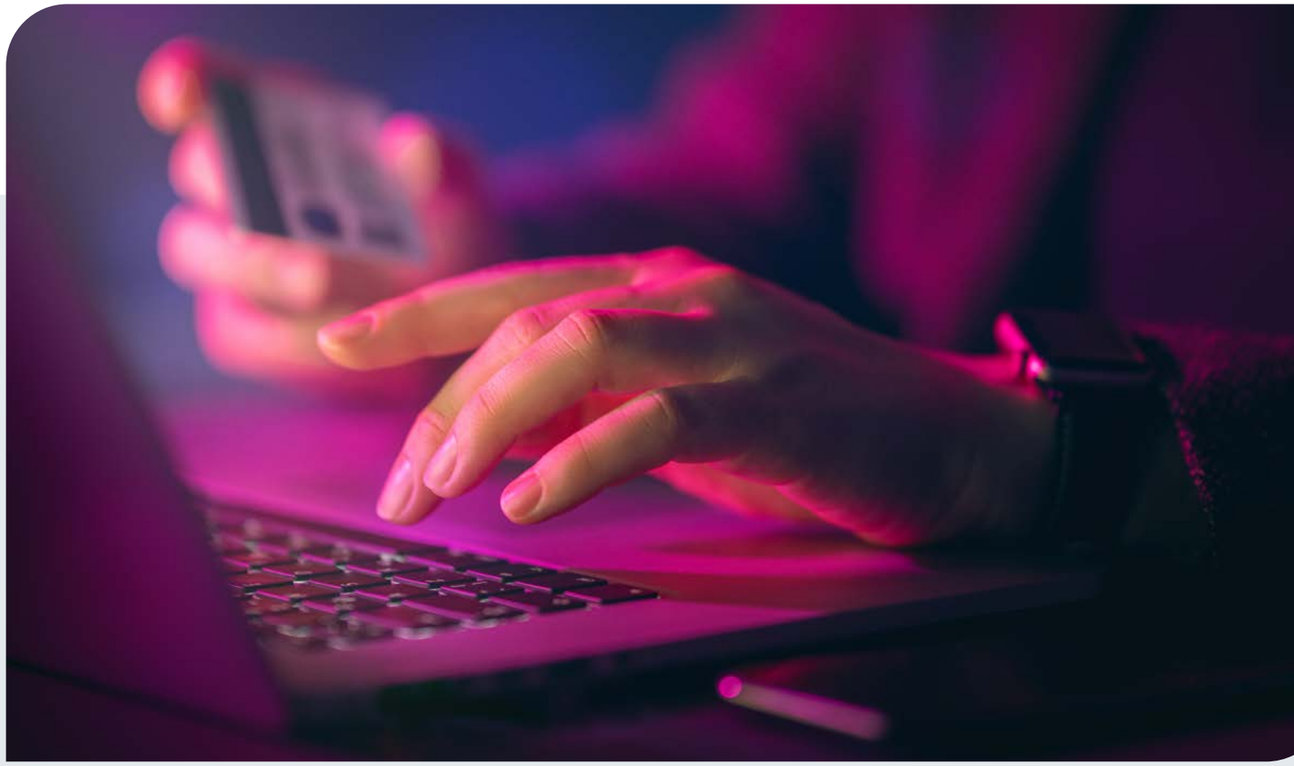
**Οι κυριότερες νομοθετικές πράξεις για την κυβερνοασφάλεια στην Ελλάδα είναι οι ακόλουθες:**

| Πράξη / Νόμος | Περιγραφή | Πεδίο εφαρμογής | Επόμενα βήματα |
|---|---|---|---|
| Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα («DORA») | Εισαγωγή ενός προηγμένου συνόλου υποχρεώσεων κυβερνοασφάλειας για τις χρηματοπιστωτικές οντότητες | • Πιστωτικά και χρηματοπιστωτικά ιδρύματα<br>• Πάροχοι υπηρεσιών κρυπτοστοιχείων<br>• Τρίτοι πάροχοι υπηρεσιών ΤΠΕ | • Έναρξη ισχύος στις 27 Δεκεμβρίου 2022<br>• Εφαρμογή από 17 Ιανουαρίου 2025 |
| Ελληνικός νόμος-πλαίσιο 4577/2018 για την κυβερνοασφάλεια και Υπουργική Απόφαση 1027/2019 | Ενσωμάτωση στην ελληνική νομοθεσία της οδηγίας NIS, η οποία θεσπίζει μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των δικτύων και των συστημάτων πληροφοριών για τις εθνικές υποδομές ζωτικής σημασίας των κρατών μελών σε ολόκληρη την ΕΕ | • Φορείς παροχής βασικών υπηρεσιών<br>• Πάροχοι ψηφιακών υπηρεσιών | Δημοσίευση του εθνικού καταλόγου υπόχρεων οντοτήτων |
| Άρθρα 109-223 του Νόμου 4727/2020 για τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών | Εισαγωγή μέτρων ασφάλειας πληροφοριών, όπως αυτά εξειδικεύονται περαιτέρω από τις αποφάσεις της ελληνικής Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών | Πάροχοι δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών | Πρωτοβουλίες για την ασφαλή ανάπτυξη δικτύων 5G σύμφωνα με τις απαιτήσεις της εργαλειοθήκης της ΕΕ για το 5G |
| Άρθρα 32-42 του Νόμου 4961/2022 | Υιοθέτηση μέτρων που διασφαλίζουν το κατάλληλο επίπεδο κυβερνοασφάλειας στις συσκευές IOT και ορισμός υπευθύνων για την ασφάλεια του IoT | Κατασκευαστές, εισαγωγείς, διανομείς και φορείς εκμετάλλευσης συσκευών IoT | Έκδοση Υπουργικών Αποφάσεων σχετικά με τις τεχνικές προδιαγραφές και τα μέτρα ασφαλείας των συσκευών τεχνολογίας IoT |

Τα τελευταία δύο χρόνια έχουν σημειωθεί σημαντικές εξελίξεις σε επίπεδο ΕΕ όσον αφορά τη νομοθεσία για την κυβερνοασφάλεια. Σύμφωνα με τη Στρατηγική Κυβερνοασφάλειας της ΕΚ, η ΕΕ εξέδωσε τις οδηγίες NIS2 και CER, και η Ευρωπαϊκή Επιτροπή πρότεινε την Πράξη για την κυβερνοανθεκτικότητα. Η μεταφορά της ανωτέρω Οδηγίας στην ελληνική νομοθεσία και η υιοθέτηση της Πράξης θα αλλάξουν σημαντικά το κανονιστικό τοπίο για την κυβερνοασφάλεια στη χώρα. Τα κύρια σημεία των επικείμενων εξελίξεων σχετικά με τη νομοθεσία για την κυβερνοασφάλεια είναι τα εξής:

## Κύρια σημεία της Πράξης για την κυβερνοανθεκτικότητα, της Οδηγίας NIS II και της Οδηγίας CERD

| Πράξη / Νόμος | Περιγραφή | Πεδίο εφαρμογής | Επόμενα βήματα |
|---|---|---|---|
| Πράξη για την κυβερνο-ανθεκτικότητα | Θέσπιση οριζόντιων απαιτήσεων κυβερνοασφάλειας για προϊόντα υλικού και λογισμικού με ψηφιακά στοιχεία | • Κατασκευαστές<br>• Εξουσιοδοτημένοι αντιπρόσωποι<br>• Εισαγωγείς<br>• Διανομείς προϊόντων με ψηφιακά στοιχεία | Οι οικονομικοί φορείς θα έχουν προθεσμία δύο ετών για να προσαρμοστούν στις απαιτήσεις της Πράξης. |
| Ευρωπαϊκό σχήμα πιστοποίησης κυβερνοασφάλειας για υπηρεσίες cloud | Πιστοποίηση της κυβερνοασφάλειας των υπηρεσιών cloud βάσει της Πράξης για την κυβερνοασφάλεια | Πάροχοι υπηρεσιών cloud (CSP) | • Δεκέμβριος 2020: Δημόσια διαβούλευση του ENISA<br>• Ιούλιος - Οκτώβριος 2023: Εκτιμώμενη έναρξη ενεργειών συντονισμού και υποστήριξης, επιτροπολογία EUCS (η επιτροπολογία είναι μια διαδικασία που ακολουθείται από τις επιτροπές της Ευρωπαϊκής Επιτροπής προκειμένου να διαμορφωθεί μια νομοθεσία)<br>• Τελευταίο τρίμηνο του 2023: Έκδοση από τον ENISA<br>• Αρχές του 2024: Έγκριση από την Ευρωπαϊκή Επιτροπή |



| Πράξη / Νόμος | Περιγραφή | Πεδίο εφαρμογής | Επόμενα βήματα |
|---|---|---|---|
| Οδηγία NIS II | Επέκταση του ουσιαστικού πεδίου εφαρμογής των υποχρεώσεων κυβερνοασφάλειας σε νέες κατηγορίες οντοτήτων | • Οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας CERD<br>• Πάροχοι δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών<br>• Πάροχοι υπηρεσιών εμπιστοσύνης<br>• Μητρώα ονομάτων τομέων ανώτατου επιπέδου και πάροχοι υπηρεσιών συστημάτων ονομάτων τομέων<br>• Δημόσιοι φορείς | • Έναρξη ισχύος στις 16 Ιανουαρίου 2023<br>• Προθεσμία μεταφοράς έως τις 17 Οκτωβρίου 2024<br>• Κατάρτιση καταλόγου υπόχρεων οντοτήτων έως τις 17 Απριλίου 2025 |
| Οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων (CERD) | Θέσπιση υποχρεώσεων για κρίσιμες οντότητες για την πρόληψη, την προστασία, την αντίσταση, τον μετριασμό και την ανάκαμψη από περιστατικά που έχουν τη δυνατότητα να διαταράξουν την παροχή βασικών υπηρεσιών | Φορείς παροχής βασικών υπηρεσιών σε τομείς όπως η ενέργεια, οι μεταφορές, οι τράπεζες, οι υποδομές χρηματοπιστωτικών αγορών, η υγεία και το πόσιμο νερό | • Έναρξη ισχύος στις 16 Ιανουαρίου 2023<br>• Προθεσμία μεταφοράς έως τις 17 Ιανουαρίου 2026<br>• Κατάρτιση εθνικών καταλόγων κρίσιμων οντοτήτων έως τις 17 Ιουλίου 2026 |

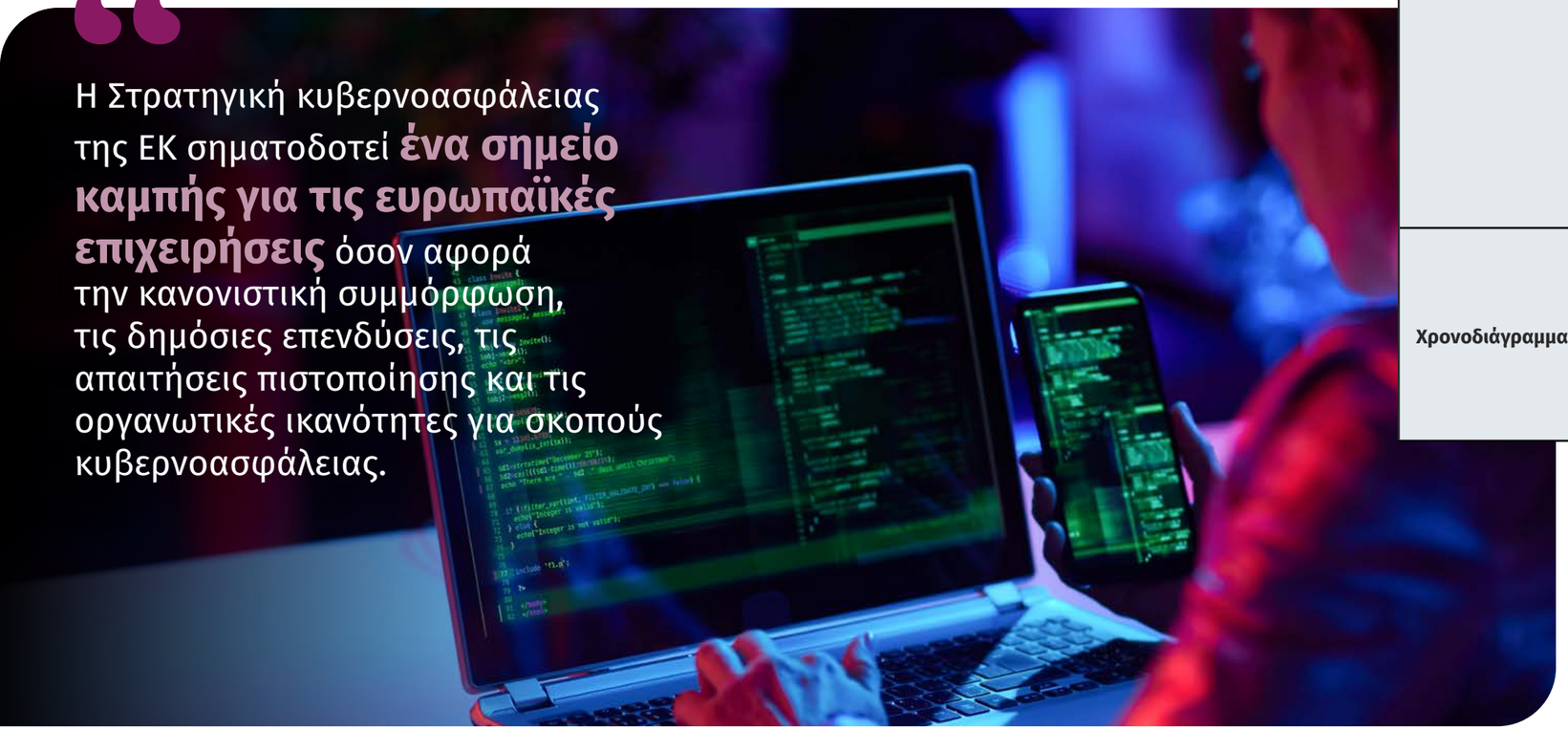
Λαμβάνοντας υπόψη τις σημαντικές εξελίξεις στη ρύθμιση των απαιτήσεων κυβερνοασφάλειας σε ενωσιακό και εθνικό επίπεδο, οι ελληνικές επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής των σχετικών υποχρεώσεων θα πρέπει να δημιουργήσουν επαρκή πλαίσια ασφάλειας πληροφοριών και να εκτελέσουν αντίστοιχες ασκήσεις συμμόρφωσης, ώστε να είναι σύμφωνες με τον νόμο.

## 3.2 Πολιτικές

Σε επίπεδο χάραξης πολιτικής, η Ευρωπαϊκή Ένωση έχει λάβει σημαντικά μέτρα για την προώθηση της κυβερνοασφάλειας ως στρατηγικό στοιχείο του σχεδίου της για τον ψηφιακό μετασχηματισμό των επιχειρήσεων και τη διασφάλιση μιας δίκαιης και ανταγωνιστικής ψηφιακής οικονομίας στην Ευρώπη.

Ήδη από το 2019, η νεοδιορισθείσα τότε Ευρωπαϊκή Επιτροπή της Ursula von Der Leyen όρισε την κυβερνοασφάλεια ως τομέα προτεραιότητας στο πλαίσιο της νέας ψηφιακής στρατηγικής της για μια Ευρώπη κατάλληλη για την ψηφιακή εποχή.

Με τη Στρατηγική κυβερνοασφάλειας[9], η οποία υιοθετήθηκε στις 16 Δεκεμβρίου 2020, η Ευρωπαϊκή Επιτροπή στοχεύει να ενισχύσει τη συλλογική ανθεκτικότητα της Ένωσης στις κυβερνοαπειλές και να διασφαλίσει ότι οι πολίτες και οι επιχειρήσεις επωφελούνται από αξιόπιστες ψηφιακές τεχνολογίες, αναπτύσσοντας κανονιστικά, επενδυτικά και πολιτικά όργανα σε τρεις τομείς δράσης, ήτοι (1) ανθεκτικότητα, τεχνολογική κυριαρχία και ηγεσία, (2) δημιουργία επιχειρησιακής ικανότητας για πρόληψη, αποτροπή και άμυνα, και (3) προώθηση ενός παγκόσμιου και ανοικτού κυβερνοχώρου.




| Τομέας εστίασης | Στρατηγική Κυβερνοασφάλειας της ΕΕ |
|---|---|
| **Σκοπός** | • Ανθεκτικότητα, τεχνολογική κυριαρχία και ηγεσία<br>• ο Ανάπτυξη επιχειρησιακής ικανότητας για πρόληψη, αποτροπή και άμυνα<br>• ο Προώθηση ενός παγκόσμιου και ανοικτού κυβερνοχώρου μέσω αυξημένης συνεργασίας |
| **Κύριες ενέργειες** | **Κανονιστικές ενέργειες:**<br>• Οδηγία NIS 2<br>• Πράξη για την κυβερνοανθεκτικότητα για ένα διαδίκτυο ασφαλών πραγμάτων<br>• Οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων (CER)<br><br>**Επενδυτικές ενέργειες:**<br>• Ευρωπαϊκή κυβερνοασπίδα<br>• Ασφαλής υποδομή κβαντικής επικοινωνίας (QCI)<br>• Κέντρο βιομηχανικής, τεχνολογικής και ερευνητικής επάρκειας για την κυβερνοασφάλεια και Δίκτυο κέντρων συντονισμού<br>• Ευρωπαϊκοί κόμβοι ψηφιακής καινοτομίας<br><br>**Πολιτικές ενέργειες:**<br>• Σχέδιο έκτακτης ανάγκης για μεγαλύτερη παγκόσμια ασφάλεια στο διαδίκτυο<br>• Ολοκλήρωση της εφαρμογής της εργαλειοθήκης της ΕΕ για το 5G<br>• Κοινή μονάδα κυβερνοχώρου (Joint Cyber Unit) σε επίπεδο ΕΕ<br>• Σχέδιο δράσης για τη βελτίωση της ψηφιακής ικανότητας των διωκτικών αρχών<br>• Εργαλειοθήκη της ΕΕ για τη διπλωματία στον κυβερνοχώρο<br>• ο Εξωτερική ατζέντα της ΕΕ για την οικοδόμηση ικανοτήτων και δυνατοτήτων κυβερνοασφάλειας<br>• ο Υποστήριξη διεθνών διαδικασιών τυποποίησης |
| **Χρονοδιάγραμμα** | • Αύξηση των δημόσιων επενδύσεων για την κυβερνοασφάλεια μέσω του προγράμματος «Ψηφιακή Ευρώπη», του προγράμματος «Ορίζοντας Ευρώπη» και του σχεδίου ανάκαμψης για την Ευρώπη.<br>• ο Πανευρωπαϊκό δίκτυο κέντρων επιχειρήσεων ασφαλείας<br>• ο Συμμόρφωση με την Οδηγία NIS 2, την Οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων και την Πράξη για την κυβερνοανθεκτικότητα |

Στην ενοποιημένη στρατηγική της «Ψηφιακή Πυξίδα»[10], που υιοθετήθηκε το 2021, η Επιτροπή καθόρισε περαιτέρω το όραμά της για την ευρωπαϊκή πορεία προς μια ψηφιοποιημένη οικονομία και κοινωνία που βασίζεται στην αλληλεγγύη, την ευημερία και τη βιωσιμότητα, εδράζεται στην ενδυνάμωση των πολιτών και των επιχειρήσεων, και διασφαλίζει την ασφάλεια και την ανθεκτικότητα του ψηφιακού οικοσυστήματος και των εφοδιαστικών αλυσίδων της.

[9] *Ευρωπαϊκή Επιτροπή και Ύπατος Εκπρόσωπος της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας, Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία, Βρυξέλλες, 16.12.2020, JOIN(2020) 18 final: https://ec.europa.eu/newsroom/dae/redirection/document/72164.*

[10] *Ανακοίνωση της Επιτροπής, Ψηφιακή Πυξίδα 2030: Η ευρωπαϊκή οδός για την ψηφιακή δεκαετία, Βρυξέλλες, 9.3.2021, COM(2021) 118 final: https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf.*

Μετά την ίδρυση της Εθνικής Αρχής Κυβερνοασφάλειας, το ελληνικό Υπουργείο Ψηφιακής Διακυβέρνησης υιοθέτησε την Εθνική Στρατηγική Κυβερνοασφάλειας 2020 – 2025[11], οραματιζόμενο ένα σύγχρονο και ασφαλές ψηφιακό περιβάλλον πληροφοριακών και δικτυακών υποδομών, εφαρμογών και υπηρεσιών προς όφελος της οικονομικής και κοινωνικής ευημερίας της χώρας.

Η Εθνική Στρατηγική Κυβερνοασφάλειας καθορίζει τους ακόλουθους πέντε στρατηγικούς στόχους που συνοδεύονται από συγκεκριμένες πρωτοβουλίες για την υλοποίησή τους: (i) λειτουργικό σύστημα διακυβέρνησης της κυβερνοασφάλειας, (ii) θωράκιση των κρίσιμων υποδομών και διασφάλιση των νέων τεχνολογιών, (iii) βελτιστοποίηση της διαχείρισης περιστατικών, της καταπολέμησης του κυβερνοεγκλήματος και της προστασίας της ιδιωτικότητας, (iv) σύγχρονο περιβάλλον για επενδύσεις στην κυβερνοασφάλεια με έμφαση στην προαγωγή της έρευνας και της ανάπτυξης, και (v) ανάπτυξη ικανοτήτων, προαγωγή της ενημέρωσης και ευαισθητοποίησης.

> Η Εθνική Στρατηγική παρέχει ένα **σαφές σχέδιο δράσης** για την Εθνική Αρχή Κυβερνοασφάλειας και υπογραμμίζει τη σταδιακή πρόοδο **της ικανότητας των ελληνικών δημόσιων φορέων να εφαρμόζουν συνεκτικές πολιτικές** στον τομέα της διακυβέρνησης της κυβερνοασφάλειας, να επιβάλλουν κανονισμούς και να ασκούν εποπτεία στον ιδιωτικό τομέα.

| Τομέας εστίασης | Εθνική Στρατηγική Κυβερνοασφάλειας |
|---|---|
| **Σκοπός** | Δημιουργία ενός σύγχρονου και ασφαλούς ψηφιακού περιβάλλοντος πληροφοριακών και δικτυακών υποδομών, εφαρμογών και υπηρεσιών στην Ελλάδα |
| **Κύριες ενέργειες** | • Βελτιστοποίηση οργανωτικών δομών και διαδικασιών<br>• Εφαρμογή ενδελεχούς αξιολόγησης κινδύνων και αποτελεσματικού σχεδιασμού έκτακτης ανάγκης<br>• ο Ενίσχυση των εθνικών, ευρωπαϊκών και διεθνών συνεργασιών<br>• Κατανόηση των τεχνολογικών εξελίξεων και των επιπτώσεών τους στην ψηφιακή διακυβέρνηση<br>• Αναβάθμιση της προστασίας των κρίσιμων υποδομών<br>• Ενοποίηση συστημάτων και εφαρμογών με την εφαρμογή ενισχυμένων απαιτήσεων ασφαλείας<br>• Βελτιστοποίηση των μεθόδων, τεχνικών και εργαλείων που χρησιμοποιούνται για την ανάλυση, την αντιμετώπιση και την αναφορά περιστατικών<br>• Ενίσχυση των μηχανισμών αποτροπής και της επιχειρησιακής συνεργασίας<br>• Κυβερνοασφάλεια για την προστασία της ιδιωτικότητας<br>• Ενθάρρυνση πρωτοβουλιών έρευνας και ανάπτυξης<br>• Παροχή επενδυτικών κινήτρων<br>• Αξιοποίηση των συμπράξεων ιδιωτικού και δημόσιου τομέα<br>• Ανάπτυξη ικανοτήτων με τη διοργάνωση ασκήσεων κυβερνοασφάλειας<br>• Εφαρμογή σύγχρονων εκπαιδευτικών και επιμορφωτικών μεθόδων και εργαλείων<br>• Προώθηση της ενημέρωσης και της ευαισθητοποίησης των φορέων και των πολιτών για την κυβερνοασφάλεια |
| **Χρονοδιάγραμμα** | • Ανάπτυξη εθνικού μητρώου καταγραφής απειλών, αξιολόγηση κινδύνων και σχεδιασμός έκτακτης ανάγκης<br>• Εφαρμογή ολοκληρωμένου πλαισίου κυβερνοασφάλειας για τα δίκτυα 5G<br>• Εφαρμογή πλαισίου μέτρων και δράσεων ασφάλειας για το Internet of Things (IoT)<br>• Έκδοση ειδικών απαιτήσεων ασφάλειας για τα δημόσια έργα ΤΠΕ<br>• Καθορισμός απαιτήσεων για τους παρόχους υπηρεσιών κυβερνοασφάλειας |

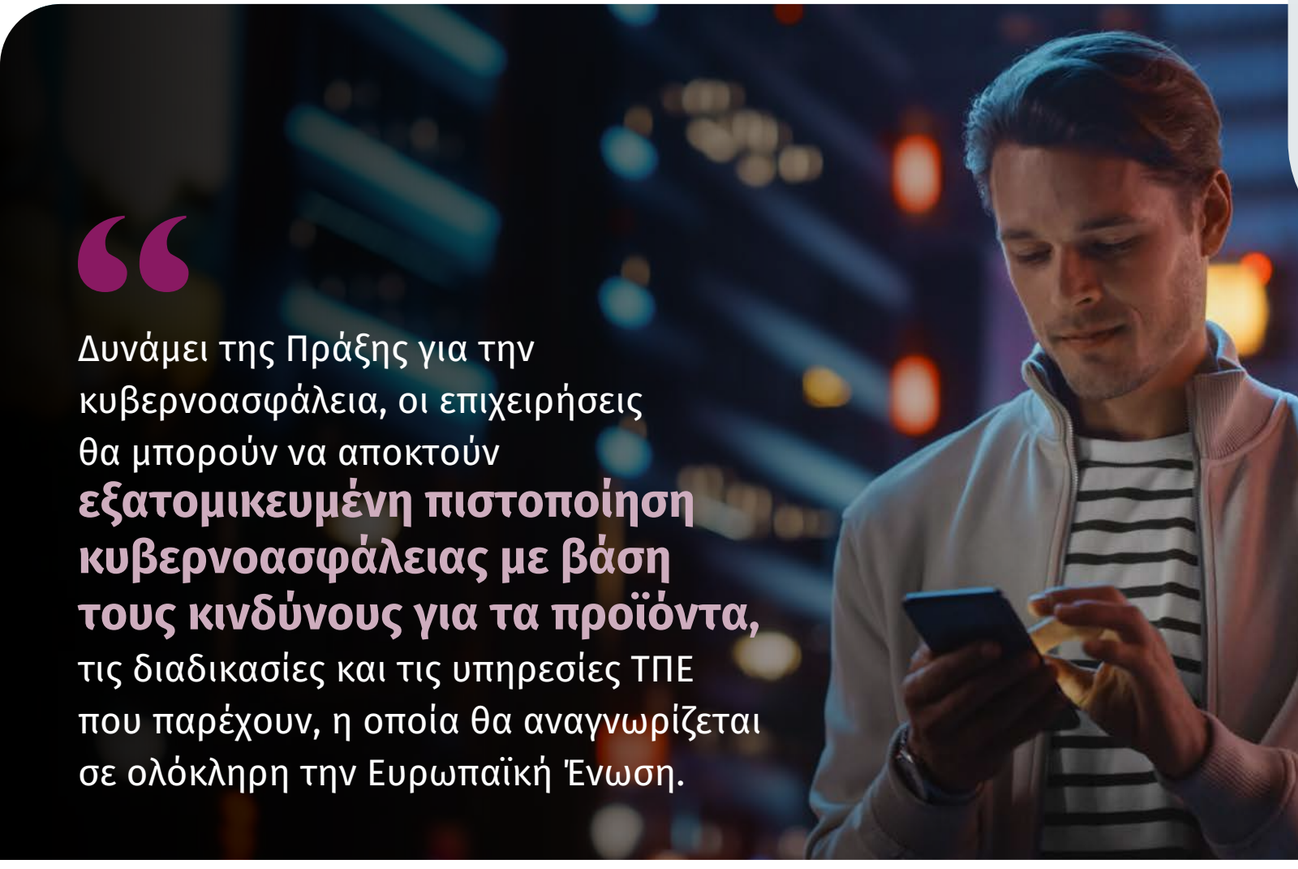
[11] *Υπουργική Απόφαση υπ' αρ. 34368/07-12-2020, Υιοθέτηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020 - 2025: https://mindigital.gr/wp-content/uloads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf.*

## 3.3 Νομοθεσία

Στο πλαίσιο της Στρατηγικής κυβερνοασφάλειας της ΕΕ, η Ευρωπαϊκή Ένωση έχει ήδη θεσπίσει την Πράξη για την κυβερνοασφάλεια και την κλαδική Πράξη για την ψηφιακή επιχειρησιακή ανθεκτικότητα (DORA) για τον χρηματοπιστωτικό τομέα, οι οποίες έχουν άμεση εφαρμογή στην Ελλάδα. Επιπλέον, η θέσπιση του ελληνικού νόμου-πλαισίου 4577/2018 για την κυβερνοασφάλεια καθορίζει τις βασικές απαιτήσεις κυβερνοασφάλειας για τους φορείς παροχής βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών στη χώρα.

Με στόχο την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας, κυβερνοανθεκτικότητας και εμπιστοσύνης εντός της Ένωσης, η Πράξη για την κυβερνοασφάλεια[12] ενισχύει τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και θεσπίζει ένα πλαίσιο για την καθιέρωση ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας για προϊόντα, διαδικασίες και υπηρεσίες ΤΠΕ.

Επιπλέον, τα άρθρα 15-27 του Νόμου 4961/2022 καθορίζουν τους εθνικούς κανόνες που συμπληρώνουν την Πράξη για την κυβερνοασφάλεια, ορίζοντας ιδίως την Εθνική Αρχή Κυβερνοασφάλειας ως εθνική αρχή πιστοποίησης κυβερνοασφάλειας και προσδιορίζοντας τις αρμοδιότητές της.



> Δυνάμει της Πράξης για την κυβερνοασφάλεια, οι επιχειρήσεις θα μπορούν να αποκτούν **εξατομικευμένη πιστοποίηση κυβερνοασφάλειας με βάση τους κινδύνους για τα προϊόντα,** τις διαδικασίες και τις υπηρεσίες ΤΠΕ που παρέχουν, η οποία θα αναγνωρίζεται σε ολόκληρη την Ευρωπαϊκή Ένωση.

| Τομέας εστίασης | Πράξη για την κυβερνοασφάλεια |
|---|---|
| **Πεδίο εφαρμογής** | • Θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας που θα βεβαιώνουν ότι τα προϊόντα, οι υπηρεσίες και οι διαδικασίες ΤΠΕ συμμορφώνονται με συγκεκριμένες απαιτήσεις ασφάλειας με σκοπό την προστασία της διαθεσιμότητας, της αυθεντικότητας, της ακεραιότητας ή της εμπιστευτικότητας δεδομένων ή λειτουργιών ή υπηρεσιών |
| **Κύρια σημεία** | • Διεύρυνση των αρμοδιοτήτων του ENISA, συμπεριλαμβανομένης της οικοδόμησης ικανοτήτων, της συνεργασίας σε επίπεδο ΕΕ και της πιστοποίησης και τυποποίησης της κυβερνοασφάλειας<br>• Κανόνες για τη θέσπιση ευρωπαϊκού πλαισίου πιστοποίησης της κυβερνοασφάλειας και της διαδικασίας προετοιμασίας, υιοθέτησης και αναθεώρησης των ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας - ενώπιον του ENISA και της Επιτροπής<br>• Κανόνες για τον ορισμό των εθνικών αρχών πιστοποίησης κυβερνοασφάλειας και τη διαπίστευση των φορέων αξιολόγησης της συμμόρφωσης |
| **Εφαρμογή** | • Τα κράτη μέλη θα θεσπίσουν τους κανόνες για τις αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις που θα επιβάλλονται σε περίπτωση παραβίασης των ευρωπαϊκών σχημάτων πιστοποίησης κυβερνοασφάλειας. |
| **Χρονοδιάγραμμα** | • Η Πράξη για την κυβερνοασφάλεια τέθηκε σε ισχύ στις 7 Ιουλίου 2019. |

[12] *Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 σχετικά με τον ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, Επίσημη Εφημερίδα L 151, 7.6.2019, σελ. 15–69: https://eur-lex.europa.eu/eli/reg/2019/881/oj.*

Η βασική νομοθετική πράξη για τη ρύθμιση της κυβερνοασφάλειας είναι ο Νόμος 4577/2018, ο οποίος μεταφέρει την Οδηγία 2016/1148/ΕΕ για την κυβερνοασφάλεια στην ελληνική νομοθεσία[13]. Ο Νόμος ορίζει σημαντικές υποχρεώσεις κυβερνοασφάλειας για τους φορείς παροχής βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών. Οι επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής του Νόμου υποχρεούνται (i) να ορίζουν υπεύθυνο ασφάλειας πληροφοριών, (ii) να λαμβάνουν τεχνικά και οργανωτικά μέτρα για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών, (iii) να λαμβάνουν μέτρα για την πρόληψη και την ελαχιστοποίηση των επιπτώσεων των συμβάντων που επηρεάζουν την ασφάλεια των δικτύων και των συστημάτων πληροφοριών, και (iv) να ενημερώνουν την Εθνική Αρχή Κυβερνοασφάλειας και την Ομάδα Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών για συμβάντα που έχουν σοβαρές επιπτώσεις στην επιχειρησιακή συνέχεια.

Οι διατάξεις του Νόμου 4577/2018 εξειδικεύονται περαιτέρω και εφαρμόζονται με την Υπουργική Απόφαση 1027/2019[14], η οποία καθορίζει λεπτομερώς τις απαιτήσεις ασφάλειας πληροφοριών για τους υπόχρεους φορείς βάσει του Νόμου, προβλέπει τη διαδικασία κοινοποίησης των συμβάντων ασφάλειας πληροφοριών στην Εθνική Αρχή Κυβερνοασφάλειας, καθορίζει τη μεθοδολογία προσδιορισμού των φορέων παροχής βασικών υπηρεσιών, και ορίζει τη διαδικασία και τα κριτήρια για την επιβολή κυρώσεων. Σύμφωνα με την Απόφαση, οι υπόχρεες οντότητες οφείλουν να διενεργούν αυτοαξιολογήσεις του επιπέδου ασφάλειας των πληροφοριών τους, κάνοντας χρήση του οδηγού και του εργαλείου αυτοαξιολόγησης της Εθνικής Αρχής Κυβερνοασφάλειας[15].

Επιπλέον, τα άρθρα 15-27 του Νόμου 4961/2022 καθορίζουν το οργανωτικό πλαίσιο για τον ορισμό των υπευθύνων ασφάλειας πληροφοριών και τα μέτρα κυβερνοασφάλειας στον δημόσιο τομέα. Επιπλέον, τα άρθρα 20-33 του Νόμου 5002/2022 καθορίζουν τους κανόνες για την υιοθέτηση ενός Εθνικού Σχεδίου Αποτίμησης Επικινδυνότητας Συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών και τη δημιουργία ενός Εθνικού Κέντρου Επιχειρήσεων Ασφαλείας (SOC).

Οι υπόχρεες οντότητες οφείλουν, βάσει του Νόμου 4577/2018, να θεσπίσουν και να εφαρμόσουν ένα οργανωτικό πλαίσιο για την κυβερνοασφάλεια, καθώς και την τεχνική υποδομή, ώστε να είναι σε θέση να επιτύχουν και να διατηρήσουν υψηλό επίπεδο ασφάλειας σε σχέση με τα δίκτυα και τα συστήματα πληροφοριών τους.

Τέλος, το ελληνικό νομοθετικό πλαίσιο για την κυβερνοασφάλεια συμπληρώνεται από τις διατάξεις του Νόμου 4411/2016[16], ο οποίος ενσωμάτωσε την Οδηγία 2013/40/ΕΕ σχετικά με τις επιθέσεις κατά συστημάτων πληροφοριών και ορίζει τα αντίστοιχα ποινικά αδικήματα και τις σχετικές κυρώσεις.

[13] *ΦΕΚ Α' 199/03-12-2018.* [14] *ΦΕΚ 3739/Β/08-10-2019.*
[15] *https://mindigital.gr/wp-content/uploads/2022/11/Cybersecurity-Self-Assessment-Tool-English-version.zip.* [16] *ΦΕΚ 142/Α/03-08-2016.*



| Τομέας εστίασης | Ελληνικός Νόμος για την Κυβερνοασφάλεια 4577/2018 |
|---|---|
| **Πεδίο εφαρμογής** | • Φορείς παροχής βασικών υπηρεσιών στους τομείς της ενέργειας, των μεταφορών, των πιστωτικών ιδρυμάτων, των υποδομών χρηματοπιστωτικών αγορών, της υγείας, της ύδρευσης και των ψηφιακών υποδομών<br>• Πάροχοι ψηφιακών υπηρεσιών, ιδίως επιχειρήσεις ηλεκτρονικού εμπορίου και γενικά ψηφιακές υπηρεσίες, μηχανές αναζήτησης και πάροχοι λύσεων cloud computing |
| **Βασικές απαιτήσεις** | Οι υπόχρεες οντότητες οφείλουν:<br>• Να υιοθετήσουν μια γενική πολιτική ασφάλειας πληροφοριών και να ορίσουν έναν υπεύθυνο ασφάλειας πληροφοριών.<br>• Να εφαρμόζουν τις τεχνικές και οργανωτικές απαιτήσεις σε ό,τι αφορά τον προσδιορισμό των κινδύνων, την προστασία της ασφάλειας των πληροφοριών και τη διαχείριση και τον περιορισμό των συμβάντων.<br>• Να ενημερώνουν άμεσα και χωρίς αδικαιολόγητη καθυστέρηση την Εθνική Αρχή Κυβερνοασφάλειας, την Ομάδα Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών και τους αποδέκτες των επηρεαζόμενων υπηρεσιών σε περίπτωση συμβάντος που έχει σοβαρό αντίκτυπο στην επιχειρησιακή συνέχεια. |
| **Εφαρμογή** | Η Εθνική Αρχή Κυβερνοασφάλειας έχει τις ακόλουθες εξουσίες και αρμοδιότητες:<br>• Αξιολόγηση της συμμόρφωσης των υπόχρεων οντοτήτων με τον Νόμο 4577/2018<br>• Υποχρέωση των υπόχρεων οντοτήτων για την προσκόμιση των απαραίτητων πληροφοριών, συμπεριλαμβανομένων των πολιτικών ασφάλειας<br>• Υποχρέωση των υπόχρεων οντοτήτων για την αποκατάσταση κάθε αδυναμίας συμμόρφωσης<br>Μετά από γνωμοδότηση της Εθνικής Αρχής Κυβερνοασφάλειας, ο Υπουργός Ψηφιακής Διακυβέρνησης μπορεί να επιβάλει πρόστιμα:<br>• Έως 15.000 ευρώ σε περίπτωση μη κοινοποίησης/καθυστέρησης κοινοποίησης<br>• Έως 50.000 ευρώ σε περίπτωση μη παροχής ή αδικαιολόγητης καθυστέρησης στην παροχή πληροφοριών ή σε περίπτωση μη λήψης των απαιτούμενων μέτρων<br>• Έως 200.000 ευρώ σε περίπτωση υποτροπής |
| **Χρονοδιάγραμμα** | • Έκδοση της Υπουργικής Απόφασης σχετικά με τις απαιτήσεις ασφάλειας και τη διαδικασία κοινοποίησης προς την Εθνική Αρχή Κυβερνοασφάλειας<br>• Δημοσίευση του εθνικού καταλόγου υπόχρεων οντοτήτων βάσει του Νόμου 4577/2018<br>• Υιοθέτηση Εθνικού Σχεδίου Αποτίμησης Επικινδυνότητας Συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών |

Μέσα σε διάστημα δύο ετών από την έναρξη της εφαρμογής του κανονισμού DORA, **οι χρηματοπιστωτικές οντότητες και οι φορείς της αγοράς στο οικοσύστημα FinTech** θα πρέπει να αναβαθμίσουν τα πλαίσια ασφάλειας πληροφοριών τους, προκειμένου να συμμορφωθούν με τις αυστηρότερες απαιτήσεις του Κανονισμού.

Εκτός από τις οριζόντιες απαιτήσεις που ισχύουν για τους φορείς παροχής βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών, η ενωσιακή και η ελληνική νομοθεσία για την κυβερνοασφάλεια προβλέπουν επιμέρους υποχρεώσεις για τον χρηματοπιστωτικό τομέα και τον τομέα των ηλεκτρονικών επικοινωνιών.

Συγκεκριμένα, ο Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα (DORA) θεσπίζει ενιαίες απαιτήσεις σχετικά με την ασφάλεια των δικτύων και των συστημάτων πληροφοριών που υποστηρίζουν τις επιχειρηματικές διαδικασίες των χρηματοπιστωτικών οντοτήτων. Ο κανονισμός DORA αποτελεί την πιο φιλόδοξη πρωτοβουλία της ΕΕ μέχρι σήμερα για τη διασφάλιση της ασφάλειας και της ανθεκτικότητας του ευρωπαϊκού χρηματοπιστωτικού τομέα σε συνθήκες ραγδαίου ψηφιακού μετασχηματισμού. Επιπλέον, ο κανονισμός DORA παρέχει νέες, διευρυμένες εξουσίες στις εθνικές και ευρωπαϊκές εποπτικές αρχές για την εποπτεία των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ. Ένα άλλο σημαντικό σημείο είναι ότι ο κανονισμός DORA αναθέτει στις αρχές ηλεκτρονικής ασφάλειας τη θέσπιση των δευτερεύοντων κανόνων που θα καταστήσουν δυνατή τη λειτουργική εφαρμογή του πλαισίου ασφαλείας της Πράξης. Για την προώθηση της καινοτομίας, ο Κανονισμός προβλέπει επίσης ένα αναλογικό σύνολο υποχρεώσεων για τις χρηματοπιστωτικές οντότητες που χαρακτηρίζονται ως πολύ μικρές επιχειρήσεις και την εφαρμογή της αρχής της αναλογικότητας κατά την εποπτεία της εφαρμογής τους από τους φορείς της αγοράς.

| Τομέας εστίασης | DORA |
|---|---|
| **Πεδίο εφαρμογής** | Πιστωτικά και χρηματοπιστωτικά ιδρύματα, πάροχοι υπηρεσιών κρυπτοστοιχείων, τόποι διαπραγμάτευσης και αποθετήρια, επιχειρήσεις επενδύσεων, διαχειριστές οργανισμών εναλλακτικών επενδύσεων, εταιρείες διαχείρισης, οργανισμοί αξιολόγησης πιστοληπτικής ικανότητας, πάροχοι υπηρεσιών αναφοράς δεδομένων, πάροχοι υπηρεσιών crowdfunding και, επίσης, τρίτοι πάροχοι υπηρεσιών ΤΠΕ. |
| **Βασικές απαιτήσεις** | • Αναφορά συμβάντων ΤΠΕ<br>• Δοκιμή ψηφιακής επιχειρησιακής ανθεκτικότητας<br>• Ανταλλαγή πληροφοριών για κυβερνοαπειλές και ευπάθειες<br>• Διαχείριση κινδύνων ΤΠΕ τρίτων |
| **Εφαρμογή** | Οι αρμόδιες αρχές θα έχουν όλες τις απαιτούμενες αρμοδιότητες εποπτείας, έρευνας και επιβολής κυρώσεων για την εκπλήρωση των καθηκόντων τους βάσει αυτού του Κανονισμού. |
| **Χρονοδιάγραμμα** | • Ο κανονισμός DORA τέθηκε σε ισχύ στις 27 Δεκεμβρίου 2022.<br>• Ο Κανονισμός θα εφαρμόζεται από τις 17 Ιανουαρίου 2025.<br>• Η Επιτροπή θα εκδώσει πράξεις κατ' εξουσιοδότηση για τη θέσπιση του κρίσιμου πλαισίου εποπτείας προμηθευτών του Κανονισμού.<br>• Εντός 24 μηνών από την έναρξη ισχύος του Κανονισμού, οι αρχές ηλεκτρονικής ασφάλειας οφείλουν να εκδώσουν από κοινού τα ρυθμιστικά τεχνικά πρότυπα (RTS) και τα εκτελεστικά τεχνικά πρότυπα (ITS) του Κανονισμού. |

Από την άλλη πλευρά, τα άρθρα 109-223 του Νόμου 4727/2020, τα οποία μεταφέρουν την Οδηγία (ΕΕ) 2018/1972 για τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών[17] στην ελληνική νομοθεσία, καθορίζουν τις απαιτήσεις κυβερνοασφάλειας στον τομέα των ηλεκτρονικών επικοινωνιών. Σύμφωνα με τις σχετικές διατάξεις του Νόμου 4727/2020, οι πάροχοι δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούνται να λαμβάνουν μέτρα ασφάλειας πληροφοριών, όπως αυτά καθορίζονται από τις αποφάσεις της ελληνικής Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών[18]. Υποχρεούνται επίσης να κοινοποιούν τα συμβάντα ασφάλειας πληροφοριών στην Αρχή και, όταν αυτά έχουν σοβαρές επιπτώσεις, και στους επηρεαζόμενους χρήστες των δικτύων τους. Επιπλέον, το άρθρο 24 του Νόμου 4961/2022 προβλέπει ότι οι πάροχοι δικτύων ηλεκτρονικών επικοινωνιών υποχρεούνται να εφαρμόζουν σχέδια αξιολόγησης κινδύνων στον κυβερνοχώρο και προμήθειας όσον αφορά στον εξοπλισμό ραδιοεπικοινωνιών.

Επιπλέον, με στόχο να διασφαλιστεί η ανάπτυξη ασφαλών δικτύων και υπηρεσιών κινητών επικοινωνιών 5G σε ολόκληρη την Ευρώπη, η Ευρωπαϊκή Επιτροπή δημιούργησε τον Ιανουάριο του 2020 την εργαλειοθήκη της ΕΕ για το 5G με την υποστήριξη του ENISA[19].

| Τομέας εστίασης | Law 4727/2020 |
|---|---|
| **Πεδίο εφαρμογής** | Πάροχοι δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών |
| **Βασικές απαιτήσεις** | Οι υπόχρεες οντότητες οφείλουν:<br>• Να λάβουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων ασφάλειας και την πρόληψη συμβάντων ασφάλειας που επηρεάζουν τα δίκτυα και τις υπηρεσίες τους.<br>• Να ενημερώνουν την ελληνική Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών και, σε περίπτωση σοβαρών επιπτώσεων, τους επηρεαζόμενους χρήστες, σε περίπτωση συμβάντος ασφάλειας πληροφοριών.<br>• Να εφαρμόζουν σχέδια αξιολόγησης κινδύνων στον κυβερνοχώρο και προμηθειών αναφορικά με τον εξοπλισμό ραδιοεπικοινωνιών. |
| **Εφαρμογή** | Η ελληνική Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών έχει τις ακόλουθες εξουσίες:<br>• Έκδοση κανονισμών σχετικά με τη διασφάλιση του απορρήτου των επικοινωνιών<br>• Διενέργεια ελέγχων σε παρόχους δικτύων/υπηρεσιών επικοινωνιών<br>• Επιβολή προστίμων έως 1.500.000 ευρώ |
| **Χρονοδιάγραμμα** | • Ο Νόμος 4727/2020 τέθηκε σε ισχύ στις 23 Σεπτεμβρίου 2020.<br>• Η Ελλάδα καλείται να αναλάβει περαιτέρω πρωτοβουλίες προκειμένου να διασφαλίσει την ασφαλή ανάπτυξη δικτύων 5G στη χώρα σύμφωνα με τις απαιτήσεις της εργαλειοθήκης της ΕΕ για το 5G. |

Η εργαλειοθήκη προσδιορίζει ένα κοινό σύνολο μέτρων για την αντιμετώπιση **των κύριων κινδύνων κυβερνοασφάλειας των δικτύων 5G**, το οποίο θα πρέπει να εφαρμοστεί στα αντίστοιχα σχέδια σε εθνικό και ενωσιακό επίπεδο.


[17] *Επίσημη Εφημερίδα L 333, 27.12.2022, σελ. 1–79: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.*
[18] *Βλ. π.χ. Απόφαση αριθ. 165/2011 της ΑΔΑΕ για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (ΦΕΚ Β' 2715/17-11-2011) και Απόφαση αριθ. 205/2013, Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών (ΦΕΚ 1742/Β/15-7-2013).*
[19] *Ομάδα συνεργασίας NIS, Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468.*

Τέλος, τα άρθρα 32-42 του Νόμου 4961/2022 «για τις αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, την ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις»[20] θεσπίζουν ένα ισχυρό πλαίσιο κανόνων για την ασφάλεια των πληροφοριών των συσκευών IoT. Οι διατάξεις του νόμου θεσπίζουν ένα προηγμένο σύνολο υποχρεώσεων ασφάλειας πληροφοριών για τους κατασκευαστές, τους εισαγωγείς, τους διανομείς και τους φορείς εκμετάλλευσης συσκευών IoT, συμπεριλαμβανομένων των υποχρεώσεων ενσωμάτωσης των κατάλληλων μέτρων ασφάλειας στις συσκευές και διορισμού υπευθύνων ασφάλειας IoT. Η Εθνική Αρχή Κυβερνοασφάλειας ορίζεται ως η αρμόδια αρχή για την εποπτεία της εφαρμογής του πλαισίου ασφάλειας IoT του Νόμου 4961/2022.

| Τομέας εστίασης | Νόμος 4961/2022 |
|---|---|
| **Πεδίο εφαρμογής** | Κατασκευαστές, εισαγωγείς, διανομείς και φορείς εκμετάλλευσης συσκευών IoT |
| **Βασικές απαιτήσεις** | • Οι κατασκευαστές IoT υποχρεούνται να υιοθετήσουν μέτρα που διασφαλίζουν το κατάλληλο επίπεδο κυβερνοασφάλειας στις συσκευές τους.[21]<br>• Οι κατασκευαστές, εισαγωγείς και διανομείς IoT υποχρεούνται να συνοδεύουν τις συσκευές IoT με μια δήλωση συμμόρφωσης με τις τεχνικές προδιαγραφές ασφαλείας που αναφέρονται στον νόμο.<br>• Κάθε κατασκευαστής θα πρέπει να διαθέτει μια διαδικασία διαχείρισης συσκευών IoT για τις περιπτώσεις στις οποίες διαπιστώνεται από τον χρήστη ότι: α) έχει προκύψει κάποιο συμβάν ασφάλειας ή β) υπάρχει ευπάθεια στις παραμέτρους ασφάλειας της συσκευής.<br>• Οι φορείς εκμετάλλευσης IoT υποχρεούνται i) να ακολουθούν τις τεχνικές προδιαγραφές ασφαλείας κάθε συσκευής, ii) να διορίζουν υπεύθυνο ασφάλειας IoT για την παρακολούθηση των αντίστοιχων μέτρων ασφαλείας, iii) να τηρούν μητρώο των διασυνδεδεμένων συσκευών IoT, iv) να διενεργούν εκτιμήσεις αντίκτυπου στην προστασία των δεδομένων, και v) να παρέχουν καθοδήγηση και πληροφορίες στους χρήστες για θέματα ασφάλειας πληροφοριών. |
| **Εφαρμογή** | Η Εθνική Αρχή Κυβερνοασφάλειας έχει τις ακόλουθες εξουσίες:<br>• Να απαιτεί από τους κατασκευαστές, εισαγωγείς ή διανομείς συσκευών IoT να λαμβάνουν όλα τα απαραίτητα διορθωτικά μέτρα προκειμένου να συμμορφώνονται με την ισχύουσα νομοθεσία.<br>• Να διατάζει την προσωρινή απόσυρση από την αγορά συσκευών IoT που παρουσιάζουν κινδύνους και την εκ νέου κυκλοφορία τους μόνο εφόσον έχουν εξαλειφθεί οι κίνδυνοι αυτοί.<br>Το Υπουργείο Ψηφιακής Διακυβέρνησης μπορεί να επιβάλει πρόστιμα ύψους έως 15.000 ευρώ και, σε περίπτωση υποτροπής, έως 100.000 ευρώ σε περίπτωση παράβασης του νόμου. |
| **Χρονοδιάγραμμα** | • Ο Νόμος 4961/2022 τέθηκε σε ισχύ στις 27 Ιουλίου 2022.<br>• Ο Υπουργός Ψηφιακής Διακυβέρνησης αναμένεται να εκδώσει αποφάσεις σχετικά με τις τεχνικές προδιαγραφές και τα μέτρα ασφαλείας των συσκευών τεχνολογίας IoT, τις υποχρεώσεις των κατασκευαστών, των εισαγωγέων και των προμηθευτών τέτοιων προϊόντων, καθώς και τις σχετικές κυρώσεις σε περίπτωση μη συμμόρφωσης. |

> Για την προμήθεια συσκευών IoT ή/και την παροχή υπηρεσιών που σχετίζονται με το IoT στην ελληνική αγορά, οι επιχειρήσεις που δραστηριοποιούνται στο εθνικό οικοσύστημα IoT υποχρεούνται να δημιουργήσουν **κατάλληλα πλαίσια ασφάλειας πληροφοριών** σύμφωνα με τις διατάξεις του νόμου.

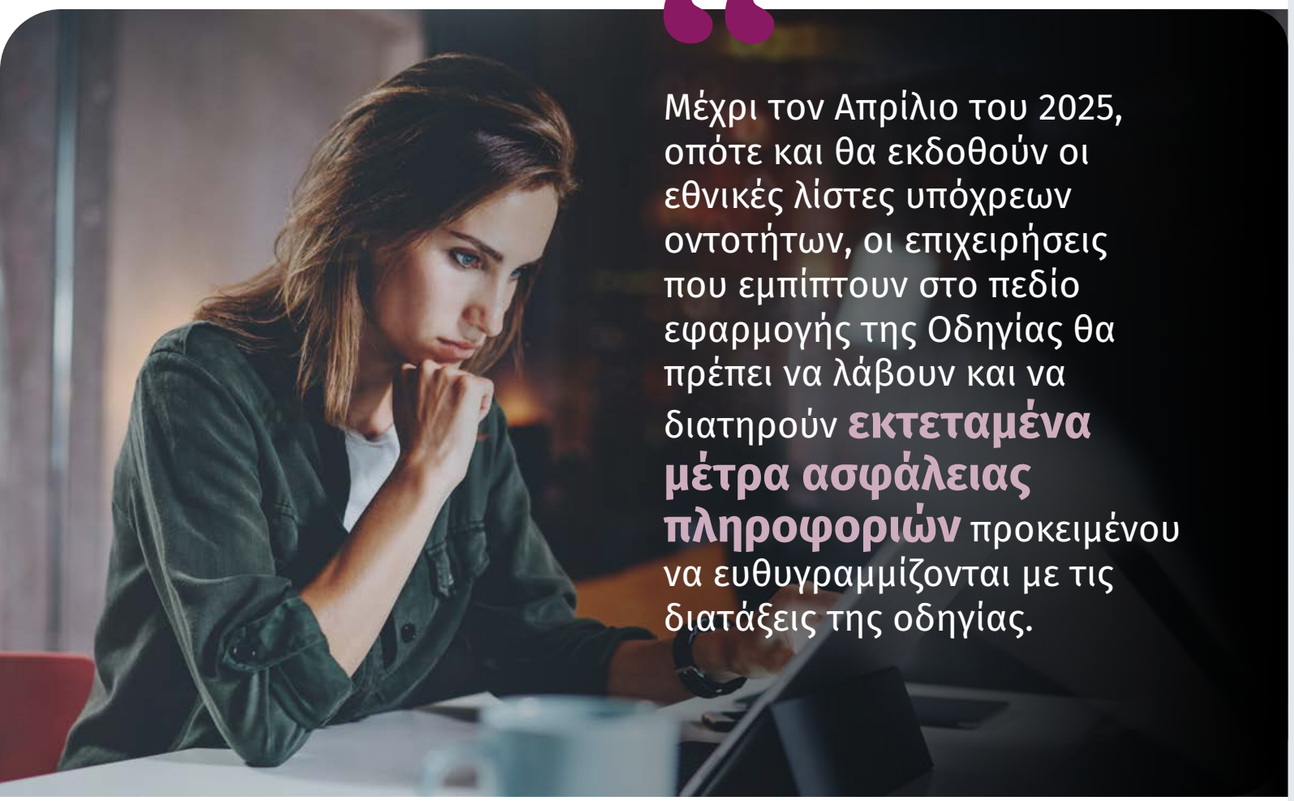
[20] *ΦΕΚ 146/Α/27-07-2022.*

[21] *Ειδικά μέτρα κυβερνοασφάλειας για τις συσκευές IoT θα καθοριστούν σε επικείμενη Απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης.*

## 3.4 Κανονιστικές εξελίξεις

Στο πλαίσιο των στρατηγικών Κυβερνοασφάλειας και Ψηφιακής Πυξίδας της Ευρωπαϊκής Επιτροπής, τα θεσμικά όργανα της Ευρωπαϊκής Ένωσης έχουν υιοθετήσει ή πρόκειται να υιοθετήσουν σημαντικές νομοθεσίες στον τομέα της κυβερνοασφάλειας, με σημαντικότερες τις Οδηγίες NIS και CER και την Πράξη για την κυβερνοανθεκτικότητα.

Η Οδηγία NIS[22] αντικαθιστά την Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS) με σκοπό την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας σε όλη την Ευρωπαϊκή Ένωση και, κατ' επέκταση, τη βελτίωση της συνολικής λειτουργίας της εσωτερικής αγοράς. Σε σύγκριση με την Οδηγία NIS, η Οδηγία NIS2 επεκτείνει το ουσιαστικό πεδίο εφαρμογής των υποχρεώσεων κυβερνοασφάλειας σε νέες κατηγορίες οντοτήτων, καθιερώνει κοινά προηγμένα σχήματα κυβερνοασφάλειας και θεσμούς συντονισμού και συνεργασίας μεταξύ των κρατών-μελών, αναβαθμίζει τις απαιτήσεις διαχείρισης κινδύνων και αναφοράς συμβάντων κυβερνοασφάλειας και, τέλος, προβλέπει αρμοδιότητες επιβολής με την κατάλληλη αποτρεπτική δύναμη για τις εποπτικές αρχές. Με την εφαρμογή της για τις μεσαίες και μεγάλες επιχειρήσεις, η Οδηγία NIS2 διευρύνει το πεδίο εφαρμογής των υποχρεώσεων κυβερνοασφάλειας σε μεγάλο κομμάτι της οικονομίας και, κατ' επέκταση, αναμένεται να βελτιώσει σημαντικά την ανθεκτικότητα του δημόσιου και ιδιωτικού τομέα.



> Μέχρι τον Απρίλιο του 2025, οπότε και θα εκδοθούν οι εθνικές λίστες υπόχρεων οντοτήτων, οι επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας θα πρέπει να λάβουν και να διατηρούν **εκτεταμένα μέτρα ασφάλειας πληροφοριών** προκειμένου να ευθυγραμμίζονται με τις διατάξεις της οδηγίας.

[22] *Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση τη οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2): https://eur-lex.europa.eu/eli/dir/2022/2555/oj.*



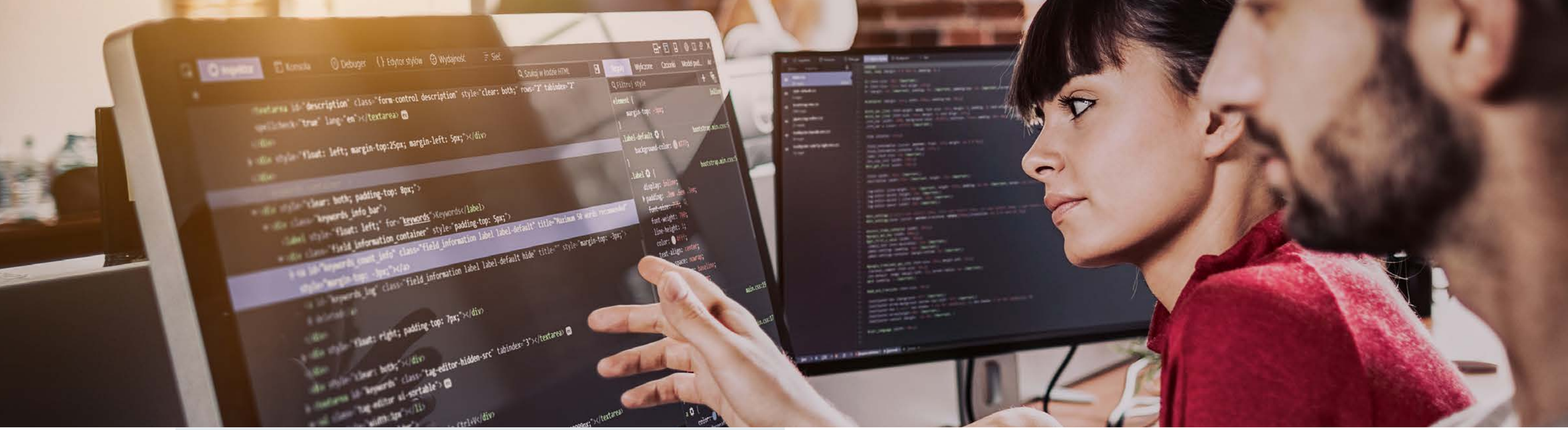
| Τομέας εστίασης | Οδηγία NIS II |
|---|---|
| **Πεδίο εφαρμογής** | • Μεσαίες και μεγάλες επιχειρήσεις (με περισσότερους από 50 εργαζόμενους και ετήσιο τζίρο πάνω από 10 εκατομμύρια ευρώ)<br>• Κρίσιμες οντότητες που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας CERD<br>• Πάροχοι δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών<br>• Πάροχοι υπηρεσιών εμπιστοσύνης<br>• Μητρώα ονομάτων τομέων ανώτατου επιπέδου και πάροχοι υπηρεσιών συστημάτων ονομάτων τομέων<br>• Οντότητες που είναι οι αποκλειστικοί πάροχοι μιας υπηρεσίας σε ένα κράτος-μέλος ή πάροχοι υπηρεσιών που θα μπορούσαν να έχουν αντίκτυπο στη δημόσια ασφάλεια ή υγεία ή θα μπορούσαν να οδηγήσουν σε συστημικούς κινδύνους ή να έχουν διασυνοριακές επιπτώσεις, σε περίπτωση διατάραξης<br>• Οντότητες δημόσιας διοίκησης |
| **Βασικές απαιτήσεις** | • Πολιτικές για την ανάλυση κινδύνων και την ασφάλεια των συστημάτων πληροφοριών<br>• Επιχειρησιακή συνέχεια, αποκατάσταση καταστροφών και διαχείριση κρίσεων<br>• Ασφάλεια προμηθευτικής αλυσίδας, συμπεριλαμβανομένων των πτυχών ασφάλειας π ου σχετίζονται με τις σχέσεις μεταξύ της κάθε οντότητας και των προμηθευτών ή τ ων παρόχων υπηρεσιών της<br>• Ασφάλεια στην αγορά, ανάπτυξη και συντήρηση συστημάτων δικτύωσης και πληροφοριών, συμπεριλαμβανομένης της αντιμετώπισης και κοινοποίησης των ευπαθειών<br>• Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας<br>• Πρακτικές κυβερνο-υγιεινής και εκπαίδευση σε θέματα κυβερνοασφάλειας<br>• Πολιτικές για τη χρήση κρυπτογραφίας και κρυπτογράφησης<br>• Αξιολόγηση κινδύνων κυβερνοασφάλειας, ασφάλεια ανθρώπινου δυναμικού, πολιτικές ελέγχου πρόσβασης και διαχείριση πόρων<br>• Χρήση πολυπαραγοντικού ελέγχου ταυτότητας ή άλλων λύσεων ελέγχου ταυτότητας<br>• Υποχρεώσεις αναφοράς συμβάντων, βάσει των οποίων οι καλυπτόμενες οντότητες οφείλουν να ενημερώνουν τις Ομάδες Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών ή τις αρμόδιες αρχές και τους αποδέκτες των υπηρεσιών τους για συμβάντα που επηρεάζουν την ικανότητά τους να παρέχουν αυτές τις υπηρεσίες, συμπεριλαμβανομένης μιας πρώιμης προειδοποίησης, εντός 24 ωρών από τη στιγμή που θα λάβουν γνώση του σημαντικού περιστατικού, και μιας ειδοποίησης συμβάντος, εντός 72 ωρών |
| **Εφαρμογή** | Οι αρμόδιες αρχές έχουν τις εξής αρμοδιότητες βάσει της Οδηγίας:<br>• Διεξαγωγή επιθεωρήσεων εντός και εκτός των εγκαταστάσεων<br>• Επιβολή διοικητικών προστίμων ύψους έως 10 εκατομμυρίων ευρώ ή 2% επί του ετήσιου παγκόσμιου τζίρου της εταιρείας, όποιο ποσό είναι μεγαλύτερο<br>• Επιβολή της δημοσίευσης των περιστατικών μη συμμόρφωσης ή/και αναστολή των πιστοποιήσεων και εγκρίσεων για τις υπηρεσίες που παρέχει η οντότητα<br>• Επιβολή προσωρινής απαγόρευσης της απασχόλησης του ατόμου που είναι υπεύθυνο για την παραβίαση σε διευθυντικές θέσεις στην οντότητα |
| **Χρονοδιάγραμμα** | • Η Οδηγία NIS 2 τέθηκε σε ισχύ στις 16 Ιανουαρίου 2023.<br>• Τα κράτη-μέλη θα πρέπει να μεταφέρουν τις διατάξεις της Οδηγίας στο εθνικό τους δίκαιο μέχρι τις 17 Οκτωβρίου 2024.<br>• Τα κράτη-μέλη θα πρέπει να καταρτίσουν μια λίστα με τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας έως τις 17 Απριλίου 2025.<br>• Η Επιτροπή θα εκδώσει οδηγίες για την εφαρμογή του Άρθρου 4 (1) και 4 (2) της Οδηγίας μέχρι τις 17 Ιουλίου 2023. |

Η Οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων (CERD)[23] θέτει ένα εναρμονισμένο πλαίσιο κανόνων για την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων στην ευρωπαϊκή εσωτερική αγορά. Η Οδηγία CERD αποσκοπεί στην αντιμετώπιση του δυναμικού τοπίου απειλών για τις κρίσιμες υποδομές σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, στο οποίο περιλαμβάνονται οι εξελισσόμενες υβριδικές απειλές, οι τρομοκρατικές απειλές, ο αυξημένος κίνδυνος λόγω φυσικών καταστροφών και κλιματικής αλλαγής, και οι αυξανόμενες αλληλεξαρτήσεις μεταξύ της υποδομής και των διαφόρων κλάδων.

| Τομέας εστίασης | Οδηγία CERD |
|---|---|
| **Πεδίο εφαρμογής** | Πάροχοι βασικών υπηρεσιών στους τομείς της ενέργειας, των μεταφορών, της τραπεζικής, των υποδομών χρηματοπιστωτικών αγορών, της υγείας, της ύδρευσης και αποχέτευσης, των ψηφιακών υποδομών, της δημόσιας διοίκησης, του διαστήματος και της παραγωγής, επεξεργασίας και διανομής τροφίμων |
| **Βασικές απαιτήσεις** | Οι κρίσιμες οντότητες οφείλουν να λάβουν τα παρακάτω μέτρα για να διασφαλίσουν την ανθεκτικότητα των βασικών υπηρεσιών τους (Κεφάλαιο III Οδηγίας CERD):<br>• Διεξαγωγή αξιολογήσεων κινδύνων αναφορικά με τους κινδύνους που θα μπορούσαν να διαταράξουν την παροχή των βασικών υπηρεσιών<br>• Λήψη κατάλληλων και αναλογικών τεχνικών και οργανωτικών μέτρων, και μέτρων ασφάλειας, για τη διασφάλιση της ανθεκτικότητάς τους<br>• Διεξαγωγή ελέγχων ιστορικού για τα φυσικά πρόσωπα που είναι σε θέση να επηρεάσουν το επίπεδο της ανθεκτικότητάς τους<br>• Ενημέρωση των αρμόδιων φορέων, άμεσα και χωρίς αναίτια καθυστέρηση, για περιστατικά που θα μπορούσαν να επηρεάσουν σημαντικά την παροχή βασικών υπηρεσιών |
| **Εφαρμογή** | Οι αρμόδιοι εθνικοί φορείς θα έχουν την αρμοδιότητα και τα μέσα προκειμένου:<br>• Να ζητούν πληροφορίες και αποδεικτικά στοιχεία για τα μέτρα που έχουν λάβει οι κρίσιμες οντότητες.<br>• Να διεξάγουν επιτόπιες επιθεωρήσεις στις υποδομές και στις εγκαταστάσεις των κρίσιμων οντοτήτων.<br>• Να εποπτεύουν τα μέτρα που έχουν λάβει οι κρίσιμες οντότητες.<br>• Να διεξάγουν ή να ζητούν τη διεξαγωγή ελέγχων για τις κρίσιμες οντότητες.<br>• Να επιβάλλουν αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις σε περιπτώσεις παράβασης, και να προβαίνουν στη λήψη όλων των απαιτούμενων ενεργειών για τη διασφάλιση της εφαρμογής των μέτρων. |
| **Χρονοδιάγραμμα** | • Η Οδηγία CERD τέθηκε σε ισχύ στις 16 Ιανουαρίου 2023.<br>• Τα κράτη-μέλη οφείλουν να μεταφέρουν την Οδηγία στην εθνική τους νομοθεσία και να υιοθετήσουν εθνικές στρατηγικές για την ανθεκτικότητα των κρίσιμων οντοτήτων μέχρι τις 17 Ιανουαρίου 2026.<br>• Τα κράτη-μέλη οφείλουν να καταρτίσουν εθνικές λίστες κρίσιμων οντοτήτων μέχρι τις 17 Ιουλίου 2026. |

Για τον σκοπό αυτό, η Οδηγία προβλέπει υποχρεώσεις για τις κρίσιμες οντότητες, ώστε να είναι σε θέση να **ενισχύουν την ικανότητά τους να προλαμβάνουν, να προστατεύουν, να αντιδρούν, να αντιστέκονται, να μετριάζουν, να απορροφούν, να προσαρμόζονται και να ανακάμπτουν** από περιστατικά που ενδέχεται να διαταράξουν την παροχή βασικών υπηρεσιών.»

[23] *Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου, Επίσημη Εφημερίδα L 333, 27.12.2022, σελ. 164–198: https://eur-lex.europa.eu/eli dir/2022/2557/oj*



Από την εφαρμογή της Πράξης, οι κατασκευαστές και οι επιχειρήσεις που μετέχουν στην εφοδιαστική αλυσίδα προϊόντων με ψηφιακά στοιχεία θα έχουν χρονικό περιθώριο δύο ετών για **τη λήψη των απαιτούμενων τεχνικών και οργανωτικών μέτρων ασφάλειας** βάσει της Πράξης.

Η Πράξη για την κυβερνοασφάλεια[24] είναι μια πρόταση για την έκδοση ενός Κανονισμού από την Ευρωπαϊκή Επιτροπή που θα επιβάλλει οριζόντιες απαιτήσεις κυβερνοασφάλειας για τα προϊόντα υλικού και λογισμικού με ψηφιακά στοιχεία, με σκοπό την ενίσχυση της ασφάλειας των εν λόγω προϊόντων στην εσωτερική αγορά. Σύμφωνα με την Πράξη, κατά τη διάθεση ενός προϊόντος με ψηφιακά στοιχεία στην αγορά, οι κατασκευαστές οφείλουν να διασφαλίζουν ότι το εν λόγω προϊόν έχει σχεδιαστεί, αναπτυχθεί και παραχθεί με γνώμονα τις βασικές απαιτήσεις για την κυβερνοασφάλεια, και να πραγματοποιούν αξιολόγηση συμμόρφωσης του προϊόντος. Παράλληλα, οι εισαγωγείς θα μπορούν να διαθέτουν στην αγορά μόνο προϊόντα με ψηφιακά στοιχεία που συμμορφώνονται με τις βασικές απαιτήσεις της Πράξης, ενώ οι διανομείς θα πρέπει να επιδεικνύουν τη δέουσα επιμέλεια σε ό,τι αφορά τις απαιτήσεις αυτού του Κανονισμού. Επιπρόσθετα, κάθε προϊόν με ψηφιακά στοιχεία θα πρέπει να συνοδεύεται από ένα συγκεκριμένο σύνολο πληροφοριών και οδηγιών για τους χρήστες σχετικά με την κυβερνοασφάλεια. Περαιτέρω, τα κρίσιμα προϊόντα με ψηφιακά στοιχεία θα πρέπει να συμμορφώνονται με τις προηγμένες απαιτήσεις κυβερνοασφάλειας. Τέλος, οι κατασκευαστές θα πρέπει να αναφέρουν τυχόν ευπάθειες και περιστατικά ασφάλειας πληροφοριών που σχετίζονται με τα προϊόντα τους στον ENISA εντός 24 ωρών από τη στιγμή που θα λαμβάνουν γνώση αυτών των ευπαθειών ή περιστατικών.

[24] *Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020, COM/2022/454 final: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=cele%3A52022PC0454.*

| Τομέας εστίασης | Πράξη για την κυβερνοανθεκτικότητα |
|---|---|
| **Πεδίο εφαρμογής** | Κατασκευαστές, εξουσιοδοτημένοι αντιπρόσωποι, εισαγωγείς και διανομείς προϊόντων με ψηφιακά στοιχεία |
| **Βασικές απαιτήσεις** | • Γενικές απαιτήσεις ασφάλειας προϊόντων και βασικές απαιτήσεις κυβερνοασφάλειας<br>• Κυβερνοασφάλεια βάσει σχεδίασης και σε όλες τις φάσεις παραγωγής των προϊόντων<br>• Κατάρτιση αναφορών αξιολόγησης κινδύνων κυβερνοασφάλειας και διεξαγωγή αξιολογήσεων συμμόρφωσης<br>• Αποτελεσματική αντιμετώπιση των ευπαθειών για την αναμενόμενη διάρκεια ζωής των προϊόντων ή για περίοδο πέντε ετών από την κυκλοφορία τους στην αγορά<br>• Αναφορά ευπαθειών και περιστατικών ασφάλειας πληροφοριών στον ENISA εντός 24 ωρών<br>• Σαφείς και κατανοητές οδηγίες για τη χρήση των προϊόντων με ψηφιακά στοιχεία<br>• Παροχή ενημερώσεων ασφάλειας για τουλάχιστον πέντε χρόνια |
| **Εφαρμογή** | • Η μη συμμόρφωση με τις βασικές απαιτήσεις κυβερνοασφάλειας θα υπόκειται σε διοικητικές κυρώσεις ύψους έως 15.000.000 ευρώ ή 2,5% επί του συνολικού ετήσιου διεθνούς τζίρου της εταιρείας κατά το προηγούμενο οικονομικό έτος, όποιο ποσό είναι μεγαλύτερο.<br>• Η μη συμμόρφωση με άλλες υποχρεώσεις θα υπόκειται σε διοικητικές κυρώσεις ύψους έως 10.000.000 ευρώ ή 2% επί του συνολικού ετήσιου διεθνούς τζίρου της εταιρείας κατά το προηγούμενο οικονομικό έτος, όποιο ποσό είναι μεγαλύτερο. |
| **Χρονοδιάγραμμα** | Οι οικονομικοί φορείς θα έχουν προθεσμία δύο ετών από την έναρξη ισχύος για να προσαρμοστούν στις απαιτήσεις της Πράξης. |

Σύμφωνα με το άρθρο 48.2 της Πράξης για την κυβερνοασφάλεια, ο ENISA έχει προτείνει ένα πανευρωπαϊκό σχήμα πιστοποίησης κυβερνοασφάλειας για τις υπηρεσίες cloud (EUCS)[25] . Το προτεινόμενο σχήμα EUCS αποσκοπεί στην ενίσχυση του επιπέδου ασφάλειας των υπηρεσιών cloud που παρέχονται στην εσωτερική αγορά της Ευρωπαϊκής Ένωσης. Για τον σκοπό αυτό, το Σχήμα προβλέπει τρία επίπεδα πιστοποίησης, ανάλογα με το επίπεδο κυβερνοασφάλειας των υπηρεσιών cloud: «βασικό», «σημαντικό» και «υψηλό». Σε ό,τι αφορά τη δομή, το Σχήμα καθιερώνει ένα σύνολο στόχων ασφάλειας και προβλέπει συγκεκριμένες προϋποθέσεις ανά στόχο, οι οποίες χαρακτηρίζονται ως «βασικές», «σημαντικές» ή «υψηλές» ανάλογα με τις διασφαλίσεις ασφάλειας που προσφέρουν. Το EUCS ενσωματώνει επίσης απαιτήσεις διαφάνειας για τις πληροφορίες ασφάλειας που καθίστανται δημόσια διαθέσιμες μέσω ενός κεντρικού ιστότοπου, όπως η τοποθεσία επεξεργασίας και αποθήκευσης δεδομένων. Κατ' αυτόν τον τρόπο, το Σχήμα επιδιώκει να παράσχει στους πελάτες υπηρεσιών cloud τη δυνατότητα να λαμβάνουν τεκμηριωμένες αποφάσεις για το επίπεδο της κυβερνοασφάλειας των παρόχων υπηρεσιών cloud που χρησιμοποιούν.

> Το EUCS αναμένεται να θέσει **τα πρότυπα κυβερνοασφάλειας για τον κλάδο των υπηρεσιών cloud στην Ευρωπαϊκή Ένωση** και να ενισχύσει την εμπιστοσύνη των χρηστών στις πιστοποιημένες υπηρεσίες.

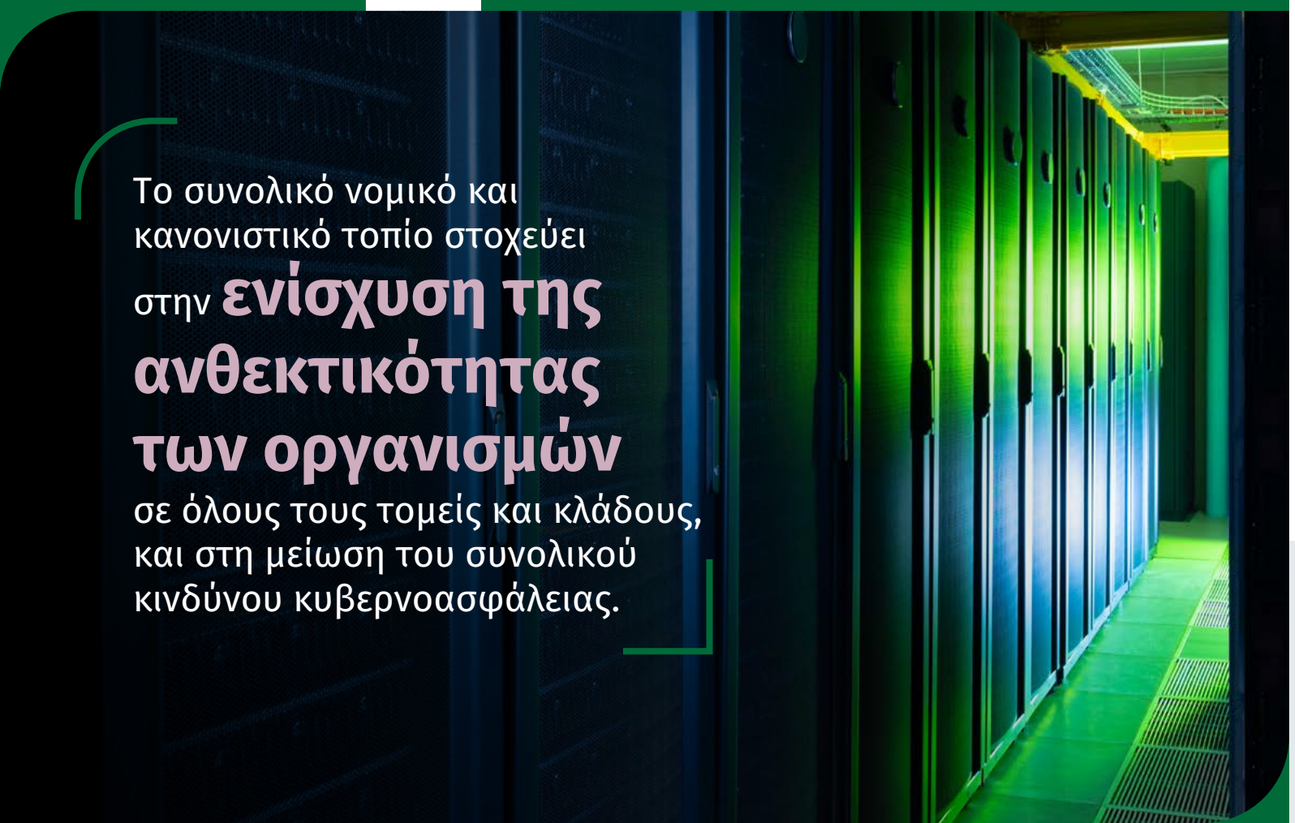
| Τομέας εστίασης | Ευρωπαϊκό σχήμα πιστοποίησης κυβερνοασφάλειας για υπηρεσίες cloud |
|---|---|
| **Πεδίο εφαρμογής** | • Οριζόντια εφαρμογή για όλες τις κατηγορίες υπηρεσιών cloud<br>• Απευθύνεται σε όλους τους παρόχους υπηρεσιών cloud |
| **Κύρια χαρακτηριστικά** | • Εθελοντικό σχήμα πιστοποίησης<br>• Ισχύει σε όλη την Ευρωπαϊκή Ένωση<br>• Τρία επίπεδα διασφάλισης: Βασικό, Σημαντικό και Υψηλό<br>• Πιστοποίηση διάρκειας τριών ετών με δυνατότητα ανανέωσης |
| **Βασικές απαιτήσεις** | • Επίτευξη στόχων ασφάλειας<br>• Απαιτήσεις ελέγχων ασφάλειας ανά στόχο<br>• Εγγυήσεις διαφάνειας<br>• Απαιτήσεις συντήρησης |
| **Χρονοδιάγραμμα** | • Δεκέμβριος 2020: Δημόσια διαβούλευση του ENISA<br>• Ιούλιος - Οκτώβριος 2023: Εκτιμώμενη έναρξη ενεργειών συντονισμού και υποστήριξης, επιτροπολογία EUCS (η επιτροπολογία είναι μια διαδικασία που ακολουθείται από τις επιτροπές της Ευρωπαϊκής Επιτροπής προκειμένου να διαμορφωθεί μια νομοθεσία)<br>• Τελευταίο τρίμηνο του 2023: Έκδοση από τον ENISA<br>• Αρχές του 2024: Έγκριση από την Ευρωπαϊκή Επιτροπή |

[25] *ENISA (2020). EUCS – Σχήμα υπηρεσιών cloud, Δεκέμβριος 2020: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/@download/fullReport.*



# 4

# Τρέχουσες προκλήσεις για την κυβερνοασφάλεια στην ελληνική αγορά



Το συνολικό νομικό και κανονιστικό τοπίο στοχεύει στην **ενίσχυση της ανθεκτικότητας των οργανισμών** σε όλους τους τομείς και κλάδους, και στη μείωση του συνολικού κινδύνου κυβερνοασφάλειας.

## 4.1 Επισκόπηση των προκλήσεων κυβερνοασφάλειας

Τα τελευταία χρόνια, η Ελλάδα έχει κάνει σημαντικές προσπάθειες για την ενίσχυση των δυνατοτήτων ψηφιοποίησης μέσα από μια σειρά κατάλληλων πρωτοβουλιών. Ωστόσο, είναι σαφές ότι το νομικό και κανονιστικό τοπίο της κυβερνοασφάλειας είναι αρκετά εκτενές, γεγονός που δημιουργεί πολλαπλές και συχνά αλληλεπικαλυπτόμενες απαιτήσεις και ευθύνες, και κατά συνέπεια οδηγεί σε μια σειρά προκλήσεων συμμόρφωσης για τις ελληνικές εταιρείες.

Οι κύριες βασικές πηγές από τις οποίες ανακύπτουν αυτές οι προκλήσεις συμμόρφωσης είναι οι εξής:

- Κατακερματισμός του κανονιστικού και νομοθετικού τοπίου
- Οργανωτικά και διοικητικά ζητήματα
- Διαχείριση συμμόρφωσης τρίτων μερών
- Διαθεσιμότητα ταλέντων/δεξιοτήτων για την αποτελεσματική διαχείριση της συμμόρφωσης με τους κανονισμούς για την κυβερνοασφάλεια

Ειδικότερα, το συνολικό νομικό και κανονιστικό τοπίο στοχεύει στην ενίσχυση της ανθεκτικότητας των οργανισμών ενάντια σε απειλές στον κυβερνοχώρο σε όλους τους τομείς και κλάδους, και στη μείωση του συνολικού κινδύνου κυβερνοασφάλειας. Ωστόσο, τα επίσημα, υφιστάμενα νομικά και κανονιστικά συστήματα που είναι αρμόδια για τη δημιουργία των κατάλληλων κανονισμών και των νομοθετικών πλαισίων πασχίζουν να προσαρμοστούν στην ταχύτητα με την οποία εισάγονται νέες τεχνολογίες και, έτσι, δημιουργείται ένα συνολικό τοπίο το οποίο είναι κατακερματισμένο και, εν τέλει, ιδιαίτερα δύσκολο στην αποτελεσματική διαχείρισή του.

Η διαχειριστική προσπάθεια που απαιτείται από πλευράς επιχειρήσεων, προκειμένου να διασφαλίσουν τη συμμόρφωσή τους με τις διευρυνόμενες απαιτήσεις, συμπεριλαμβανομένων του χρόνου και του κόστους, αλλά και των συνολικών δεξιοτήτων, της ανάπτυξης ταλέντων και της εκπαίδευσης, δημιουργεί επιπλέον δυσκολίες. Το πρόβλημα αυτό εντείνεται ακόμη περισσότερο, αν συνυπολογίσει κανείς την ταχεία ψηφιοποίηση και τις σχετικές τεχνολογικές εξελίξεις, ειδικά όπως έχουν διαμορφωθεί οι συνθήκες μετά την πανδημία, και δη σε συνδυασμό με ζητήματα που αφορούν τον βαθμό εμπλοκής και δέσμευσης της διοίκησης σε ό,τι αφορά την κυβερνοασφάλεια, αλλά και τα διαθέσιμα κονδύλια και τις σχετικές επενδύσεις.

Τέλος, λόγω της προαναφερθείσας ταχύτατης εξέλιξης της τεχνολογίας, οι επιχειρήσεις είναι πιθανότερο να οδηγηθούν σε αυξανόμενη εξάρτηση από τρίτους για την αποτελεσματική υιοθέτηση των νέων τεχνολογιών και την προσαρμογή τους στο συνεχώς μεταβαλλόμενο τοπίο. Η εξάρτηση από τρίτους, ωστόσο, μπορεί να αυξήσει τους σχετικούς κινδύνους συμμόρφωσης, εξαιτίας των διαφορετικών επιπέδων ωριμότητας και της απουσίας κατάλληλων μηχανισμών παρακολούθησης και διαχείρισης.

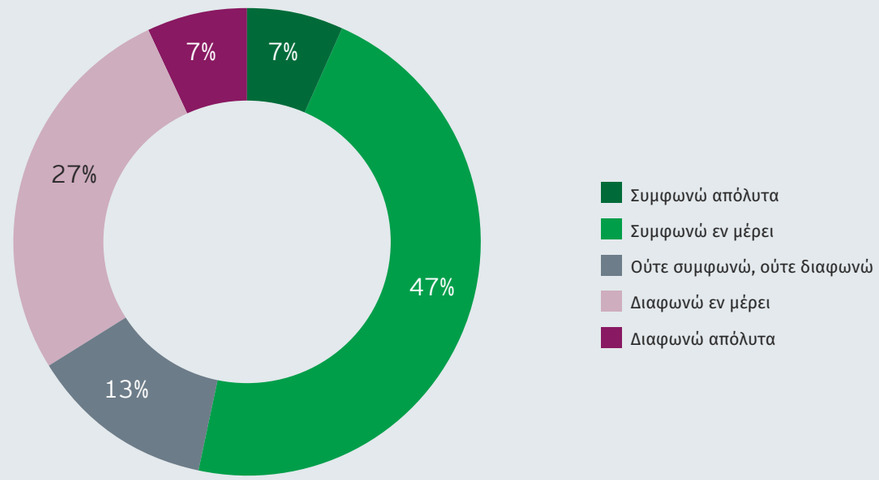
## 4.2 Προκλήσεις για την κυβερνοασφάλεια στην ελληνική αγορά

Στο πλαίσιο της παρούσας έκθεσης, διανεμήθηκε ένα ερωτηματολόγιο σε επαγγελματίες της κυβερνοασφάλειας σε διάφορες επιχειρήσεις, από διαφορετικούς τομείς και κλάδους, προκειμένου να προσδιοριστούν με μεγαλύτερη ακρίβεια οι προκλήσεις που αντιμετωπίζουν ως αποτέλεσμα της νομοθεσίας και των κανονισμών για την κυβερνοασφάλεια.

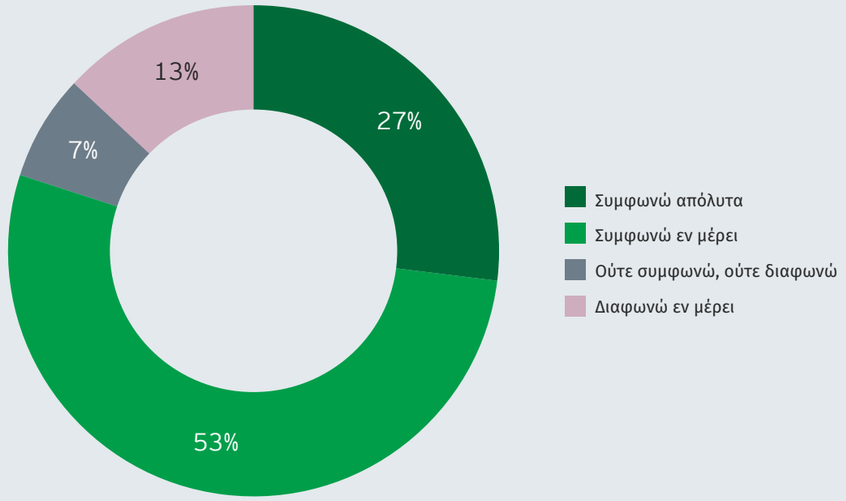
Με βάση τις απαντήσεις τους, έγινε σαφές ότι οι ερωτηθέντες, στο σύνολό τους, έχουν την άποψη ότι, κατά κανόνα, οι κανονισμοί για την κυβερνοασφάλεια συμβάλλουν στη μείωση των κινδύνων για τις επιχειρήσεις και ενισχύουν τη λήψη αποτελεσματικών αποφάσεων και τις σχετικές επενδύσεις. Παράλληλα, στην πλειοψηφία τους, οι ερωτηθέντες συμφωνούν επίσης ότι οι απαιτήσεις συμμόρφωσης προάγουν την κατάλληλη κουλτούρα γύρω από την κυβερνοασφάλεια. Επιπρόσθετα, οι μισοί και πλέον από τους ερωτηθέντες θεωρούν ότι τα διοικητικά έξοδα που απαιτούνται για τη διασφάλιση της συμμόρφωσης με το κανονιστικό τοπίο για την κυβερνοασφάλεια επιβαρύνουν τις επιχειρήσεις.

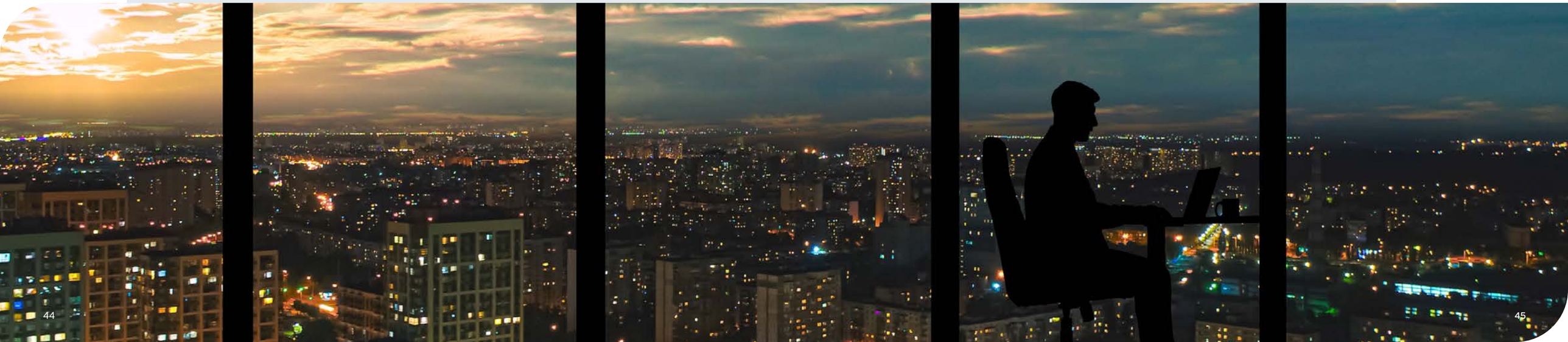
Παρόλ' αυτά, η πλειοψηφία των ερωτηθέντων συμφωνούν ότι το κανονιστικό τοπίο είναι κατακερματισμένο και οι σχετικές απαιτήσεις συχνά είναι αντικρουόμενες ή αλληλεπικαλυπτόμενες, με αποτέλεσμα η διαχείρισή τους να είναι χρονοβόρα και πολύπλοκη, ενώ δηλώνουν ότι η προσπάθεια, οι πόροι, οι δεξιότητες, τα εργαλεία και τα έξοδα που απαιτούνται για τη διασφάλιση της συμμόρφωσης μιας επιχείρησης με τις απαιτήσεις των κανονισμών για την κυβερνοασφάλεια δεν εκτιμώνται κατάλληλα και έγκαιρα. Επιπλέον, οι περισσότεροι ερωτηθέντες συμφωνούν ότι, εν τέλει, η παρακολούθηση των μεταβολών στο κανονιστικό τοπίο για την κυβερνοασφάλεια είναι δύσκολη και χρονοβόρα, αν και είναι μάλλον αβέβαιο ότι η προσπάθεια συμμόρφωσης με τις σχετικές απαιτήσεις θα μπορούσε να θεωρηθεί ως το πλέον αγχωτικό κομμάτι της δουλειάς τους.

**Ο διαχειριστικός χρόνος και τα έξοδα που απαιτούνται για τη διασφάλιση της συμμόρφωσης με τους κανονισμούς περί κυβερνοασφάλειας αποτελούν επιβάρυνση για την επιχείρηση**




**Το ρυθμιστικό τοπίο για την κυβερνοασφάλεια είναι κατακερματισμένο**

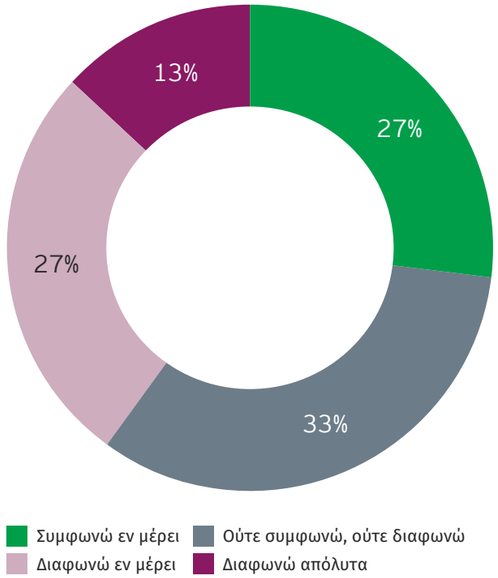


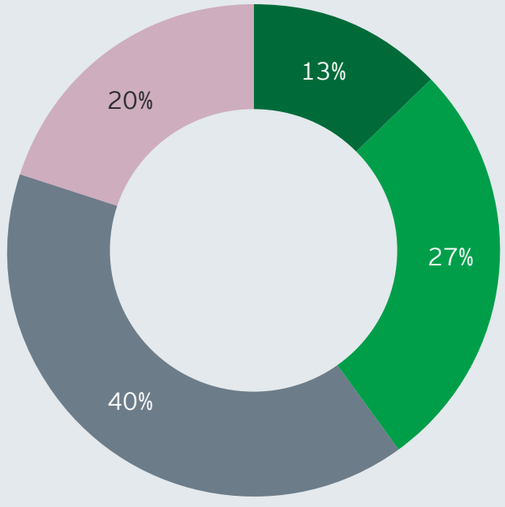
Περίπου οι μισοί από τους ερωτηθέντες δήλωσαν, επίσης, ότι έχουν εμπιστοσύνη στην ικανότητα της επιχείρησής τους να διαχειριστεί τις απαιτήσεις συμμόρφωσης στις οποίες υπόκειται, ενώ σχεδόν όλοι συμφωνούν ότι το συνολικό κανονιστικό τοπίο έχει διευκολύνει το έργο τους, ειδικά σε ό,τι αφορά την αιτιολόγηση της ανάγκης για νέες πρωτοβουλίες σχετικά με την κυβερνοασφάλεια. Ταυτόχρονα, ωστόσο, η πλειοψηφία των ερωτηθέντων δήλωσε ότι απαιτούνται περαιτέρω επενδύσεις στον τομέα της κυβερνοασφάλειας προκειμένου να ενισχυθεί η θέση της εκάστοτε επιχείρησης έναντι των κανονιστικών αρχών σε περίπτωση ελέγχου για τη συμμόρφωσή της με τις ισχύουσες απαιτήσεις για την κυβερνοασφάλεια.

Σε ό,τι αφορά τη διαχείριση τρίτων μερών, η πλειοψηφία των ερωτηθέντων συμφώνησαν ότι η αυξημένη εξάρτηση από τρίτους μπορεί να οδηγήσει σε πραγματικούς κινδύνους συμμόρφωσης, λόγω πιθανών διαφοροποιήσεων ως προς τη συνολική ωριμότητά τους, ενώ υπάρχει μεγάλος βαθμός αβεβαιότητας ως προς το αν η εκάστοτε επιχείρηση έχει σαφή εικόνα και έλεγχο επί των εν λόγω τρίτων μερών προκειμένου να μπορεί να διαχειρίζεται κατάλληλα τους σχετικούς κινδύνους συμμόρφωσης.

**Η επιχείρηση έχει σαφή εικόνα και έλεγχο σε ό,τι αφορά τα τρίτα μέρη για τη σωστή διαχείριση των σχετικών κινδύνων συμμόρφωσης**



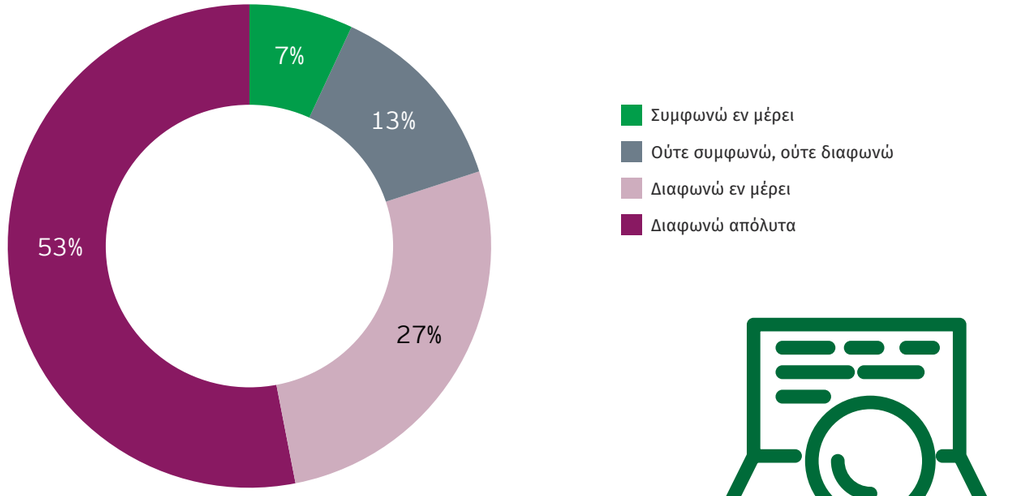

**Η επιχείρηση έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέσα ελέγχου και τα σχετικά εργαλεία για την επίτευξη και τη συνεχή παρακολούθηση της συμμόρφωσης με τους ισχύοντες κανονισμούς για την κυβερνοασφάλεια**

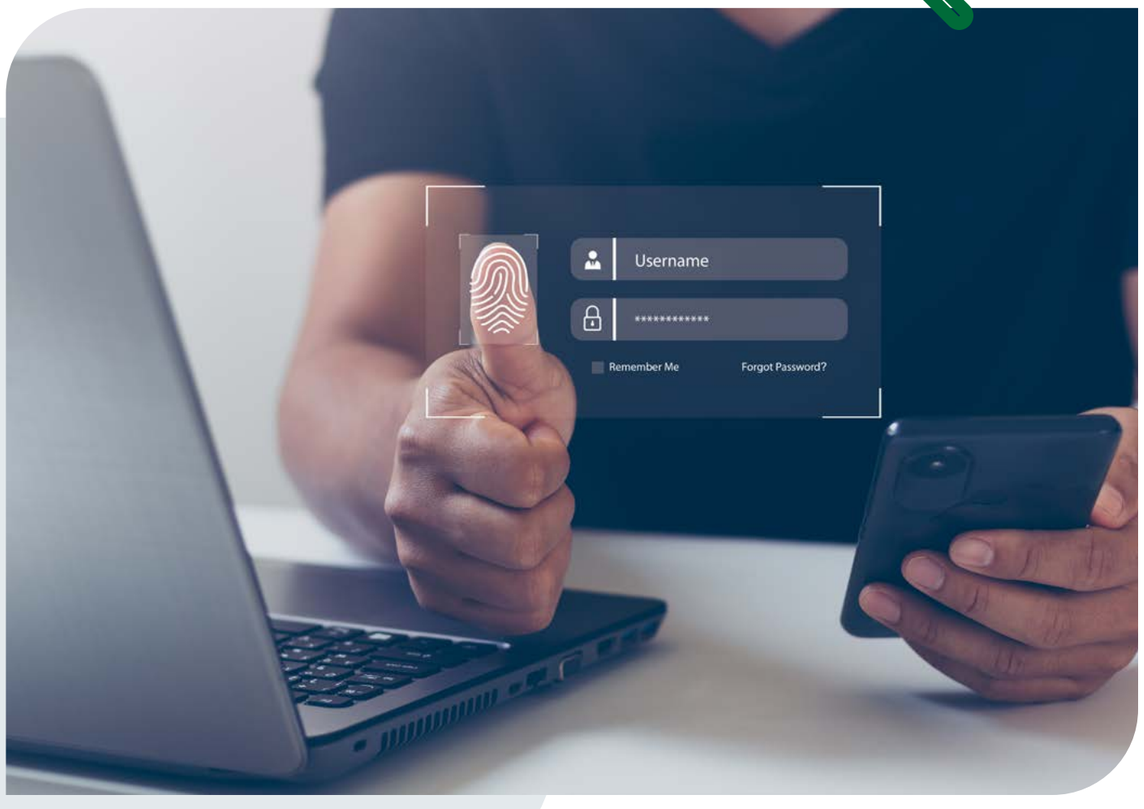



Σε ό,τι αφορά τις επιπτώσεις της πανδημίας, η πλειοψηφία των ερωτηθέντων δήλωσε ότι ο κίνδυνος μη συμμόρφωσης με το κανονιστικό τοπίο έχει αυξηθεί εξαιτίας της πανδημίας και, κατά συνέπεια, της εξάπλωσης του υβριδικού μοντέλου εργασίας ενώ, ταυτόχρονα, οι περισσότεροι υποστήριξαν ότι οι επιχειρήσεις προχωρούν στην ανάπτυξη νέων τεχνολογιών με εξαιρετικά γρήγορους ρυθμούς που δεν παρέχουν τα απαιτούμενα χρονικά περιθώρια για την κατάλληλη αξιολόγηση ή εποπτεία σε επίπεδο κανονιστικής συμμόρφωσης. Επιπρόσθετα, υπάρχει μεγάλος βαθμός αβεβαιότητας σχετικά με το αν η εκάστοτε επιχείρηση έχει εφαρμόσει τα κατάλληλα τεχνολογικά μέσα ελέγχου και αν χρησιμοποιεί τα σχετικά εργαλεία για την εξασφάλιση και τη συνεχή παρακολούθηση της συμμόρφωσής της.

Τέλος, οι περισσότεροι ερωτηθέντες έκριναν ότι η ανεύρεση των κατάλληλων πόρων σε επίπεδο ταλέντων ή δεξιοτήτων για την αποτελεσματική αντιμετώπιση των θεμάτων συμμόρφωσης παρουσιάζει δυσκολίες.

**Είναι σχετικά εύκολο να βρει κανείς τους κατάλληλους πόρους για την αποτελεσματική αντιμετώπιση των προκλήσεων συμμόρφωσης**



Η τελευταία έρευνα Global Information Security Survey (GISS) της EY επιβεβαιώνει σε μεγάλο βαθμό τα παραπάνω συμπεράσματα υπό ένα διακλαδικό και παγκόσμιο πρίσμα:

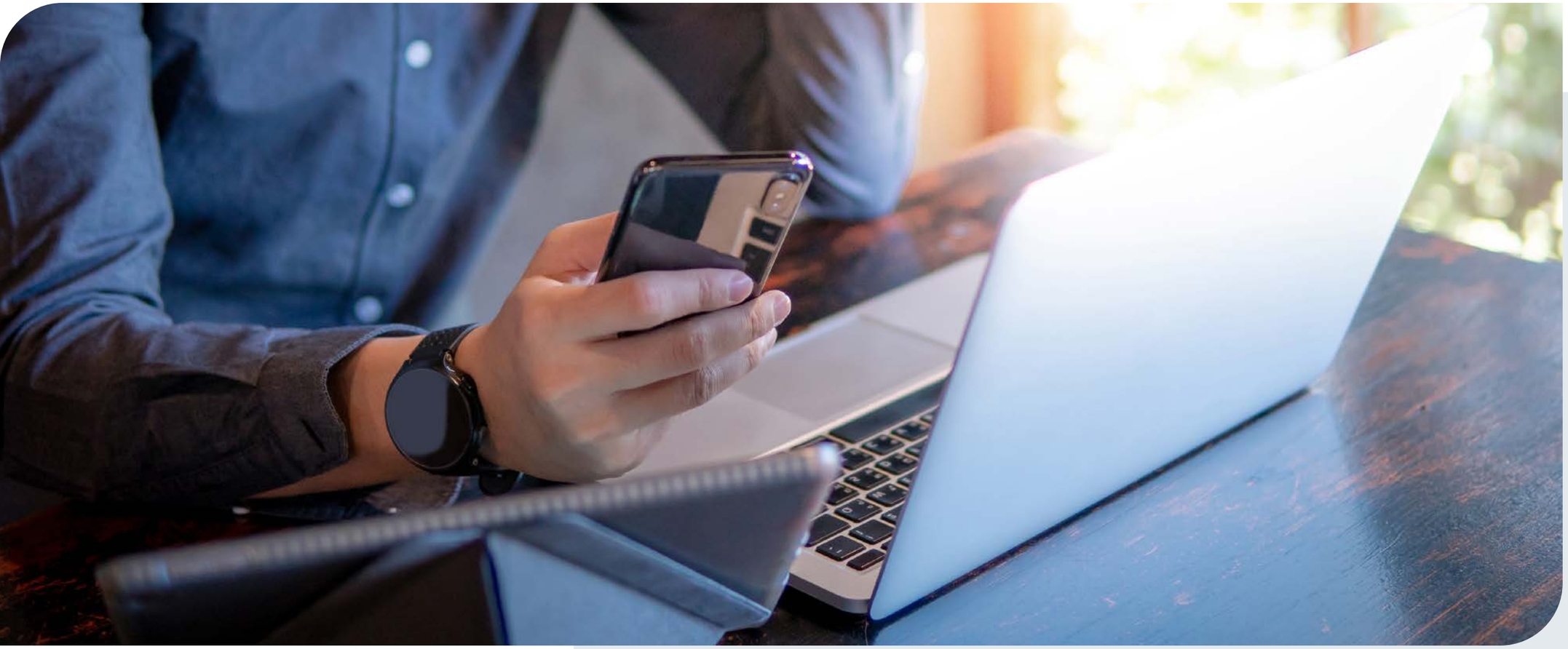
- Η συντριπτική πλειοψηφία (87%) των ερωτηθέντων διεθνώς συμφωνούν ότι, σε γενικές γραμμές, οι απαιτήσεις συμμόρφωσης με τους κανονισμούς για την κυβερνοασφάλεια, είτε αυτές αφορούν έναν συγκεκριμένο κλάδο είτε επιβάλλονται από το κράτος, οδηγούν στις κατάλληλες στοχευμένες ενέργειες και συμπεριφορές στο εσωτερικό της εκάστοτε επιχείρησης.
- Ωστόσο, περίπου οι μισοί (51%) από τους ερωτηθέντες έκριναν ότι η διασφάλιση και η διαχείριση της συμμόρφωσης στο πλαίσιο του ολοένα και πιο κατακερματισμένου κανονιστικού τοπίου αποτελεί μία από τις πλέον πολύπλοκες πτυχές της εργασίας τους.
- Οι περισσότεροι (60%) πιστεύουν ότι το παραπάνω κανονιστικό τοπίο θα γίνει ακόμα πιο κατακερματισμένο και, ως εκ τούτου, χρονοβόρο ως προς τη διαχείρισή του στο μέλλον.

Προκειμένου να αντιμετωπίσουν τις προκλήσεις που αναλύονται πιο πάνω, και σύμφωνα με τις ίδιες απαντήσεις, οι ελληνικές εταιρείες έχουν προχωρήσει σε διάφορες ενέργειες στο πλαίσιο της διαδρομής τους προς τη συμμόρφωση. Οι ενέργειες αυτές μπορούν να συνοψιστούν ως εξής:

- Βελτίωση των ικανοτήτων διακυβέρνησης και της ιεράρχησης μέσα από την υλοποίηση νέων τεχνολογιών
- Αύξηση των κατάλληλων πόρων
- Τακτικοί έλεγχοι διαδικασιών, επιτόπου δοκιμές και σχετικές ασκήσεις
- Διεξαγωγή εκπαιδευτικών και ενημερωτικών εκστρατειών
- Καθιέρωση αποτελεσματικότερων μεθοδολογιών διαχείρισης κινδύνων και συμμόρφωσης
- Διεξαγωγή αναλύσεων κενών, όπου κρίνεται απαραίτητο
- Μεγαλύτερη έμφαση στην αυτοματοποίηση
- Υιοθέτηση βέλτιστων πρακτικών του κλάδου μέσω των σχετικών πλαισίων
- Συνεργασία με ειδικούς στον τομέα της κυβερνοασφάλειας

Συνοψίζοντας τις απαντήσεις, καθίσταται σαφές ότι, αν και οι κανονισμοί για την κυβερνοασφάλεια συμβάλλουν θετικά στη μείωση του συνολικού κινδύνου των επιχειρήσεων σε αυτόν τον τομέα, καθώς υποστηρίζουν τη λήψη αποτελεσματικότερων αποφάσεων και την ανάπτυξη μιας ισχυρότερης κουλτούρας σχετικά με την κυβερνοασφάλεια, το τοπίο αναμένεται να κατακερματιστεί ακόμα περισσότερο και, κατ' επέκταση, να παρουσιάζει περισσότερες δυσκολίες στη διαχείρισή του.

Παρότι οι περισσότερες επιχειρήσεις έχουν ξεκινήσει να λαμβάνουν τα απαραίτητα μέτρα για την αντιμετώπιση αυτής της πρόκλησης, το πρόβλημα εντείνεται περαιτέρω από το γεγονός ότι, κατά την άποψη των περισσότερων επιχειρήσεων, υπάρχει έλλειψη εξειδικευμένων επαγγελματιών, αλλά και απουσία δέσμευσης από πλευράς διοίκησης, σε συνδυασμό με προβληματισμούς σε επίπεδο προϋπολογισμού και μια ευρύτερη δυσκολία στον προσδιορισμό των σχετικών κανονιστικών απαιτήσεων εξαιτίας του αυξανόμενου κατακερματισμού.



# 5

# Πώς μπορεί να σας βοηθήσει η Microsoft να αντιμετωπίσετε αυτές τις προκλήσεις

**Το Microsoft Defender for Cloud** επιδιώκει να βελτιώσει τη συνολική θέση των επιχειρήσεων σε ό,τι αφορά την κυβερνοασφάλεια.

## 5.1 Χαρτοφυλάκιο προϊόντων

Η σουίτα λύσεων cloud και ασφάλειας της Microsoft έχει σχεδιαστεί έτσι ώστε να βοηθά όλες τις επιχειρήσεις, ανεξαρτήτως τομέα και κλάδου, στον ψηφιακό μετασχηματισμό τους, αλλά και στην αντιμετώπιση των σχετικών προκλήσεων. Οι εταιρείες μπορούν να αξιοποιήσουν τις ενοποιημένες δυνατότητες ασφάλειας της Microsoft τόσο στις λύσεις cloud που χρησιμοποιούν όσο και στα τοπικά τους συστήματα, προκειμένου να βελτιώσουν την ασφάλεια σε όλα τα επίπεδα και, κατά συνέπεια, να διαχειριστούν αποτελεσματικά τα θέματα συμμόρφωσης.

Ειδικότερα, το Microsoft Defender for Cloud επιδιώκει να βελτιώσει τη συνολική θέση των επιχειρήσεων σε ό,τι αφορά την κυβερνοασφάλεια, παρέχοντας μια κεντρική λύση διαχείρισης ασφάλειας για την αποτελεσματική παρακολούθηση των φόρτων εργασίας και τη λήψη εξατομικευμένων προτάσεων ασφάλειας βάσει διαδικασιών συσχετισμού που καθίστανται εφικτές μέσω του ενσωματωμένου μηχανισμού αναλύσεων ασφάλειας.

Η λύση αυτή υποστηρίζει τα παρακάτω:

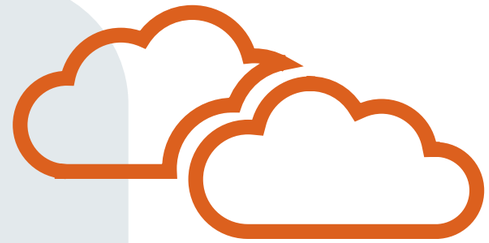
Κεντρική διαχείριση πολιτικών που βοηθά στον εντοπισμό των παραβιάσεων των εφαρμοζόμενων πολιτικών ασφάλειας βάσει καθορισμένων συνθηκών

- Κάλυψη πολλαπλών περιβαλλόντων cloud μέσω της δυνατότητας σύνδεσης στα εν λόγω περιβάλλονται με agentless μεθόδους
- Cloud / Advanced Cloud Security Posture Management (CSPM) μέσω του dashboard
- Κατάσταση ασφάλειας με επίγνωση δεδομένων που επιτρέπει τον αυτόματο εντοπισμό των χώρων αποθήκευσης που περιέχουν ευαίσθητα δεδομένα
- Διαχείριση και βελτίωση ασφάλειας με ανάθεση εργασιών σε κατόχους πόρων και παρακολούθηση της προόδου της ευθυγράμμισης της κατάστασης ασφάλειας με την καθορισμένη πολιτική ασφάλειας

Σε επίπεδο διαχείρισης και προστασίας δεδομένων, το Microsoft Purview προσφέρει μια ενοποιημένη λύση για τη διαχείριση των on-premises, multi-cloud και SaaS (Software-as-a-Service) δεδομένων της επιχείρησης. Η καθιέρωση της εξ αποστάσεως εργασίας ως αποτέλεσμα της πανδημίας σε συνδυασμό με την αύξηση των επιθέσεων από εθνικά κράτη και τις συνεχείς εξελίξεις σε επίπεδο κανονισμών έχουν οδηγήσει στην ανάγκη δημιουργίας μιας ολιστικής και επικαιροποιημένης χαρτογράφησης του τοπίου των δεδομένων με αυτοματοποιημένο εντοπισμό δεδομένων, ταξινόμηση ευαίσθητων δεδομένων και ολοκληρωμένη παρακολούθηση της προέλευσης και πορείας των δεδομένων, η οποία θα επιτρέπει στις επιχειρήσεις να αναπτύσσουν έναν ενοποιημένο χάρτη των πόρων δεδομένων τους, και των σχέσεων αυτών, ώστε να απολαμβάνουν πιο αποτελεσματική διαχείριση δεδομένων.

Ειδικότερα, το Microsoft Purview υποστηρίζει τα εξής:

- Ενισχυμένες δυνατότητες εντοπισμού και διερεύνησης μέσω του Insider Risk Management
- Εντοπισμός εγγράφων και δεδομένων μέσω του eDiscovery, ώστε να μπορούν οι επιχειρήσεις να ανταποκρίνονται τόσο σε εσωτερικές έρευνες όσο και σε εξωτερικά αιτήματα
- Δυνατότητες εντοπισμού παραβίασης του κώδικα δεοντολογίας μέσω του Communication Compliance
- Ενοποιημένες δυνατότητες διαχείρισης δεδομένων και συμμόρφωσης, μέσω των λύσεων Data Lifecycle Management, Data Loss Prevention και Information Protection



Το Azure Monitor προσφέρει μια ξεχωριστή, ολοκληρωμένη λύση για την ενίσχυση των δυνατοτήτων ασφάλειας του περιβάλλοντος cloud, αλλά και της συνολικής προσαρμοστικότητας και επεκτασιμότητας του cloud της επιχείρησης, μέσα από τη συλλογή, ανάλυση και ανταπόκριση σε δεδομένα τηλεμετρίας που λαμβάνει από το περιβάλλον cloud ή ακόμα και από on-premises περιβάλλοντα.

Η λύση αυτή παρέχει τις εξής δυνατότητες:

- Βελτιωμένη παρακολούθηση και δυνατότητα παρατήρησης μέσα από τη συλλογή δεδομένων από πολλαπλές πηγές και πλατφόρμες δεδομένων
- Παρακολούθηση της διαδρομής των δεδομένων μέσα από ένα σύνολο διαφορετικών μηχανισμών, ανάλογα με τα δεδομένα και τον προορισμό
- Επιλεγμένες δυνατότητες οπτικοποίησης για την παροχή αναλυτικών πληροφοριών για εφαρμογές web, container, εικονικά συστήματα (VM) και πόρους δικτύου μέσω dashboard, βιβλίων εργασίας, Power BI και Grafana
- Ανάλυση της παρακολούθησης δεδομένων μέσα από το περιβάλλον εξερεύνησης μετρήσεων, αναλύσεις καταγραφών και αναλύσεις αλλαγών
- Δυνατότητες ανταπόκρισης μέσα από αυτοματοποιημένες διαδικασίες, με αξιοποίηση των ειδοποιήσεων, της αυτόματης κλιμάκωσης και του Azure Logic Apps για τη λήψη ειδοποιήσεων, τον δυναμικό έλεγχο του αριθμού των εκτελούμενων πόρων και τη δημιουργία αυτοματοποιημένων ροών εργασιών

Τέλος, οι λύσεις ασφάλειας όπως η σουίτα Microsoft 365 Defender και το Microsoft Sentinel μπορούν να χρησιμοποιηθούν για την προστασία τελικών σημείων, εφαρμογών και υπηρεσιών σε περιβάλλοντα cloud και on-premises, αξιοποιώντας τις σχετικές δυνατότητες SIEM και XDR για τη βελτίωση της αποτελεσματικότητας και της αποδοτικότητας, και παράλληλα επιτρέποντας στις εταιρείες να προστατεύουν κατάλληλα την ψηφιακή υποδομή τους.




## 5.2 Ενδεικτικά Use Cases

Από τις τραπεζικές συναλλαγές μέχρι τα καταναλωτικά αγαθά, τη βιομηχανία και την ενέργεια, επιχειρήσεις όλων των κλάδων χρησιμοποιούν τα προϊόντα και τις υπηρεσίες της Microsoft για την ολοκληρωμένη κάλυψη των αναγκών τους σε επίπεδο ασφάλειας, αλλά και την εκπλήρωση των υποχρεώσεων συμμόρφωσης σε ένα δυναμικό κανονιστικό τοπίο. Οι παρακάτω ιστορίες επιτυχίας δείχνουν πώς ορισμένες από τις μεγαλύτερες εταιρείες στον κόσμο κατόρθωσαν να διαχειριστούν τις προκλήσεις που αντιμετώπιζαν με τη βοήθεια του εκτενούς χαρτοφυλακίου προϊόντων της Microsoft.

### i) Αποτελεσματικότερη ενοποίηση των επιπέδων ασφάλειας για μεγαλύτερη προστασία

**Ποιος:** MSC Mediterranean Shipping Company S.A. (MSC)

**Τι:** Η MSC αναζητούσε αποτελεσματικούς τρόπους για να προστατεύει τα πλοία, τα φορτία και τα δεδομένα της, όπου κι αν βρίσκονται. Ενσωματώνοντας τις δυνατότητες ασφάλειας του Microsoft 365, η εταιρεία μπόρεσε να ενισχύσει τα επίπεδα ασφαλειάς της, να εντοπίσει τους κρυφούς κινδύνους τόσο στα τοπικά συστήματα όσο και στις λύσεις cloud, και να αυτοματοποιήσει τις εργασίες ρουτίνας, έτσι ώστε η ομάδα ασφάλειας να μπορεί να επικεντρώνεται στην καινοτομία.

**Πώς:** Η επιχείρηση προχώρησε στην ανάπτυξη του Microsoft 365 E5, συμπεριλαμβανομένων των Windows 10 Enterprise, Office 365 και Enterprise Mobility + Security, αξιοποιώντας τις δυνατότητες διαλειτουργικότητας των παρεχόμενων προϊόντων ασφάλειας για την ενίσχυση και την απλοποίηση των αμυντικών της μέσων. Το Azure Security Center θεωρείται ο «απόλυτος προορισμός» της εταιρείας για το σύνολο της υποδομής της Azure, καλύπτοντας πάνω από 750 εικονικά συστήματα, ενώ η εταιρεία μπορεί επίσης να το αξιοποιήσει και για την τοπικά εγκατεστημένη υποδομή της. Η MSC έχει αναπτύξει επίσης το Azure Active Directory (Azure AD) για τη διαχείριση ταυτοτήτων και πρόσβασης μέσω των λειτουργιών Privileged Identity Management και Identity Protection. Παράλληλα, χρησιμοποιεί τα Azure Information Protection και Microsoft Threat Protection για τη διευκόλυνση της συμμόρφωσης με τους σχετικούς κανονισμούς και την έγκαιρη ανίχνευση και αντιμετώπιση απειλών, αντίστοιχα.

### ii) Αξιοποίηση των δυνατοτήτων του Azure για τη δημιουργία των θεμελίων για μακροπρόθεσμη ανάπτυξη

**Ποιος:** Metinvest

**Τι:** Η εταιρεία ήθελε να κλιμακώσει και να επεκτείνει τις δυνατότητες των υπάρχοντων κέντρων δεδομένων της. Με την υποστήριξη του συνεργάτη της σε θέματα IT και καινοτομίας, της Metinvest Digital, η ομάδα ανέπτυξε μια στρατηγική συμμαχία με τη Microsoft και την Infopulse για τη μεταφορά 680 διακομιστών στο Azure.

**Πώς:** Η Metinvest αξιοποίησε τις δυνατότητες του Azure Security Center για προηγμένη προστασία από τις απειλές και ενοποιημένη διαχείριση ασφάλειας, παρακολουθώντας και συντηρώντας την ασφάλεια στο cloud μέσω των λύσεων Azure Monitor και Security Center, καθιστώντας έτσι εφικτή τη σύνδεση όλων των υπηρεσιών και έχοντας μια ολοκληρωμένη εικόνα των συνδρομών, των μισθωτών και των δραστηριοτήτων. Επιπρόσθετα, χρησιμοποιεί το Azure Bastion για τη διασφάλιση της ασφαλούς πρόσβασης στους διακομιστές, ενώ το Azure Files έχει αντικαταστήσει τους τοπικούς διακομιστές αρχείων της εταιρείας, διασφαλίζοντας την πλήρως διαχειριζόμενη και κοινή πρόσβαση στα εταιρικά αρχεία.

### iii) Χρήση των λύσεων Microsoft Security για την επανασχεδίαση των τραπεζικών δυνατοτήτων για ένα ψηφιακό κοινό

**Ποιος:** ING Bank

**Τι:** Η μεγάλη ιστορία και οι διαφοροποιούμενοι κανονισμοί ανά τον κόσμο καθιστούν το τοπίο IT ιδιαίτερα πολύπλοκο για την ING. Η προορατική ομάδα IT του οργανισμού γνώριζε ότι η ενοποίηση ήταν το κλειδί για τη βελτίωση της ασφάλειας, αλλά χρειαζόταν μια συντονισμένη λύση ασφάλειας για την προστασία των ψηφιακών πόρων.

**Πώς:** Η τράπεζα επέλεξε τις λύσεις Microsoft Security, όπως το Microsoft Sentinel for SIEM και τις δυνατότητες XDR, και τη σουίτα Microsoft Defender για την προστασία των τελικών σημείων, των ταυτοτήτων και των εφαρμογών cloud. Το Microsoft Defender for Cloud προσφέρει στην ING μια ενιαία προβολή του multi-cloud περιβάλλοντός της, το οποίο επιτυγχάνεται μέσω της χρήσης του Azure Arc για την αποτύπωση όλων των καταγραφών και των σημάτων από τις πλατφόρμες της. Στη συνέχεια, το Microsoft Sentinel αναλύει τις καταγραφές και τα σήματα, επιτρέποντας στους αναλυτές ασφάλειας της εταιρείας να ελέγχουν και να αντιμετωπίζουν τις πιθανές απειλές γρήγορα και προληπτικά. Με τα Microsoft Defender for Endpoint και Microsoft 365 Defender, συμπεριλαμβανομένης της προστασίας e-mail, η ING διεύρυνε τη στρατηγική της XDR. Εστιάζοντας απόλυτα στην εκπλήρωση κάθε κανονιστικής απαίτησης, η ING εγκαθιστά τώρα το Microsoft Purview Compliance Manager και δοκιμάζει τη λύση Microsoft Purview Data Loss Prevention.

### iv) Στρατηγική Zero Trust με την υποστήριξη των λύσεων Microsoft Security

**Ποιος:** Siemens

Τι: Όταν ξεκίνησε τη μετάβασή της στο cloud, η Siemens ήθελε να δώσει έμφαση στην προληπτική ασφάλεια σε πραγματικό χρόνο προκειμένου να εφαρμόσει μια προσέγγιση Zero Trust. Χρειαζόταν ένα πολύ καλά συντονισμένο σύνολο λύσεων ασφάλειας για την προστασία ταυτοτήτων, δεδομένων και τελικών σημείων.

**Πώς:** Έχοντας ξεκινήσει ήδη να αξιοποιεί τις εφαρμογές ενίσχυσης παραγωγικότητας του Microsoft 365, η Zero έθεσε σε εφαρμογή της στρατηγική της Zero Trust προστατεύοντας τρεις τομείς: ταυτότητες (συμπεριλαμβανομένης της πρόσβασης εξωτερικών χρηστών), δεδομένα και τελικά σημεία. Παράλληλα, αξιοποίησε το σύνολο των πλούσιων δυνατοτήτων ασφάλειας που ενσωματώνει η λύση, όπως τα Azure Active Directory, Microsoft Defender for Identity, Microsoft Endpoint Manager, Microsoft Defender for Endpoint κ.ά. Με το Microsoft Defender for Identity, η Siemens προστατεύει και παρακολουθεί όλες τις on-premises ταυτότητες, καθώς και τα δεδομένα και τις συσκευές, εφαρμόζοντας πολιτικές πρόσβασης υπό συνθήκες. Με το Privileged Identity Management διαχειρίζεται την πρόσβαση σε όλους τους πόρους του Microsoft 365 και στις συσκευές που διαχειρίζεται μέσω του Microsoft Intune, του Azure, αλλά και άλλων εφαρμογών SaaS τρίτων εταιρειών. Η Siemens χρησιμοποιεί, επίσης, το Microsoft Information Protection για την ταξινόμηση και προστασία των δεδομένων, και το Microsoft Defender for Cloud Apps για τη διαχείριση της κοινοποίησης δεδομένων και της πρόσβασης σε πόρους και εφαρμογές. Η εταιρεία σκοπεύει να υλοποιήσει και το Microsoft Defender for Endpoint, προκειμένου να εντοπίζει προβλήματα διαμόρφωσης και ευπάθειες σε πραγματικό χρόνο, και να παρακολουθεί και να μπλοκάρει τις απειλές προς τελικά σημεία.

### v) Επιτυχής αντιμετώπιση επίθεσης ransomware

**Ποιος:** G&J Pepsi-Cola Bottlers

**Τι:** Όταν δέχθηκε επίθεση ransomware Cobalt Strike, η G&J Pepsi-Cola Bottlers δεν χρειάστηκε να δώσει χρήματα ή να χάσει δεδομένα, χάρη στην επιδέξια αποκατάσταση αρχείων μέσω του Microsoft Azure Backup. Μετά την επίθεση και την επιτυχή αντιμετώπισή της, η εταιρεία ξεκίνησε μια εκτεταμένη αναβάθμιση στην ασφάλεια των συστημάτων της.

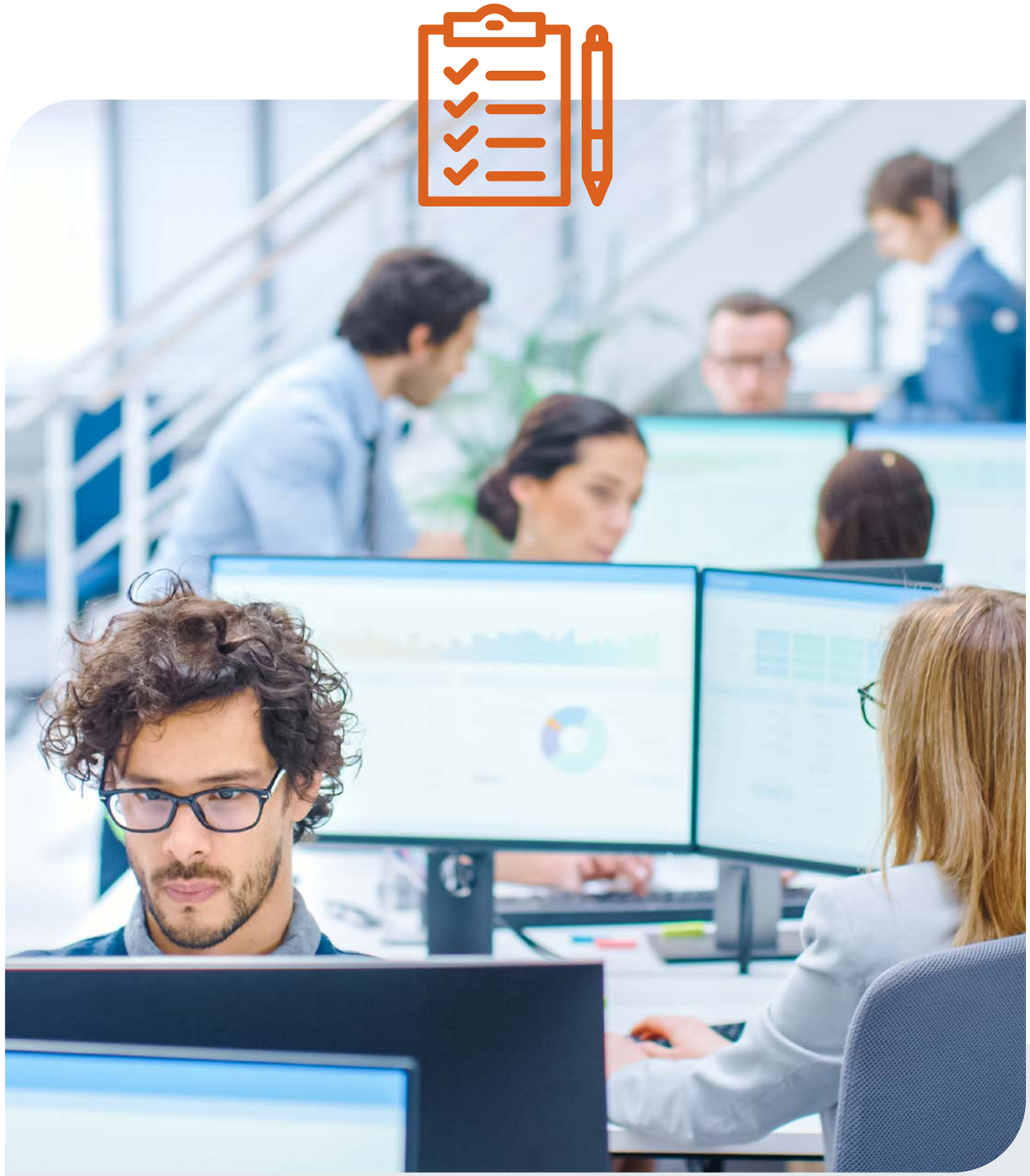
**Πώς:** Η εταιρεία είχε επενδύσει στη διαχείριση τελικών σημείων με το Microsoft Defender for Endpoint, το Intune και άλλες δυνατότητες του Microsoft 365 Defender. Όταν ανακάλυψε την επίθεση ransomware, η ομάδα ασφάλειας της G&J Pepsi χρησιμοποίησε το Microsoft Defender for Endpoint για να εντοπίσει και να απενεργοποιήσει όλα τα εικονικά συστήματα που είχαν εκτεθεί, απομονώνοντας κάθε συσκευή που θεωρούσε ότι θα μπορούσαν να χρησιμοποιήσουν οι χάκερ για πλευρική κίνηση. Με το Azure Backup, προχώρησε στην επαναφορά των δεδομένων σε κάθε διακομιστή. Η εταιρεία δεν υπέστη καμία απώλεια δεδομένων, ξεπέρασε τους περιορισμούς στην παρακολούθηση συμβάντων ασφάλειας προσλαμβάνοντας έναν υπεύθυνο εντοπισμού και αντιμετώπισης συμβάντων, και πλέον χρησιμοποιεί το Microsoft Graph Data Connect για εύκολη ορατότητα. Μετά την ολοκλήρωση της διαδικασίας αποκατάστασης, η εταιρεία έθεσε σε εφαρμογή ένα ενισχυμένο πρόγραμμα κυβερνοασφάλειας, το οποίο τελειοποίησε την ήδη προηγμένη ασφάλειά της, και επέκτεινε τη χρήση των Microsoft Defender for Endpoint και Microsoft Intune.

### vi) Βελτίωση και απλοποίηση κατοχής και κοινοποίησης δεδομένων

**Ποιος:** bp

**Τι:** Η τεράστια πλατφόρμα δεδομένων της εταιρείας έχει ζωτικό ρόλο στην υλοποίηση του οράματός της για μεγαλύτερη ποικιλομορφία και ενοποίηση των πηγών ενέργειας, επιτρέποντας την κοινοποίηση και διαχείριση δεδομένων στο σύνολο των επιχειρηματικών μονάδων της πιο γρήγορα και πιο αποτελεσματικά από ποτέ.

**Πώς:** Το Data Hub της bp είναι μια multi-cloud λύση, η οποία έχει σχεδιαστεί για την ενοποίηση της αλυσίδας αξίας δεδομένων και την παροχή μιας συνεπούς εμπειρίας δεδομένων βάσει προφίλ χρήστη στα περιβάλλοντα cloud Microsoft και άλλων παρόχων της εταιρείας. Με το Microsoft Purview, η bp επιδιώκει να εξασφαλίσει ενοποιημένη διαχείριση των multi-cloud δεδομένων μέσω αυτοματοποιημένου εντοπισμού δεδομένων, ταξινόμησης των ευαίσθητων δεδομένων και ολοκληρωμένης παρακολούθησης της προέλευσης και της πορείας των δεδομένων. Έτσι, τα δεδομένα της εταιρείας, από οποιοδήποτε σημείο της πλατφόρμας δεδομένων κι αν προέρχονται, είναι επαληθευμένα, κατάλληλα, εξαιρετικά αξιόπιστα και ασφαλή. Με τον τρόπο αυτόν, οι χρήστες μπορούν να είναι σίγουροι ότι τα δεδομένα που λαμβάνουν για αναλυτικούς και εμπορικούς σκοπούς είναι επαληθευμένα και κατάλληλα. Σύντομα θα υπάρχει δυνατότητα άντλησης μεγαλύτερων όγκων δεδομένων από κάθε σημείο του οργανισμού με πολύ λιγότερους περιορισμούς, έτσι ώστε να είναι δυνατή η δημιουργία ενός οικοσυστήματος επαναχρησιμοποιήσιμων προϊόντων δεδομένων σε επίπεδο εταιρείας.



# 6 Το μέλλον

Το ψηφιακό τοπίο αλλάζει με γοργούς ρυθμούς. Οι ανεξέλεγκτες τεχνολογικές εξελίξεις έχουν ανοίξει τον δρόμο για πολλές νέες ευπάθειες που μπορούν να εκμεταλλευτούν πιθανά κακόβουλα μέρη, τα οποία αξιοποιούν επίσης τις νέες τεχνολογίες για τη δημιουργία νέων και πιο προηγμένων κυβερνοαπειλών. Ο αυξημένος ρυθμός υιοθέτησης νέων τεχνολογιών, όπως η επιχειρησιακή τεχνολογία (OT) και το Internet of Things (IoT), το Blockchain και οι τεχνολογίες που αξιοποιούν τις δυνατότητες της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (ML), έχει δημιουργήσει νέα πεδία απειλών και επιθέσεων για τις επιχειρήσεις, τους δημόσιους οργανισμούς και τους πολίτες σε παγκόσμιο επίπεδο.

Γενικά, ο αριθμός και η σοβαρότητα των κυβερνοεπιθέσεων έχουν αυξηθεί. Το ίδιο ισχύει και για τις επιπτώσεις που μπορεί να έχουν στους εκάστοτε στόχους, καθώς πλέον δεν αποσκοπούν στη διάταξη της λειτουργίας των επιχειρήσεων μόνο, αλλά και στην υπονόμευση κρίσιμων κρατικών υποδομών. Το γεγονός αυτό αποτελεί σημαντική πρόκληση για τις επιχειρήσεις, οι οποίες καλούνται να διασφαλίσουν ότι είναι σε θέση να παρακολουθούν τις εξελίξεις, να προσαρμόζονται στις νέες τεχνολογίες και, ταυτόχρονα, να παραμένουν ασφαλείς στον κυβερνοχώρο.

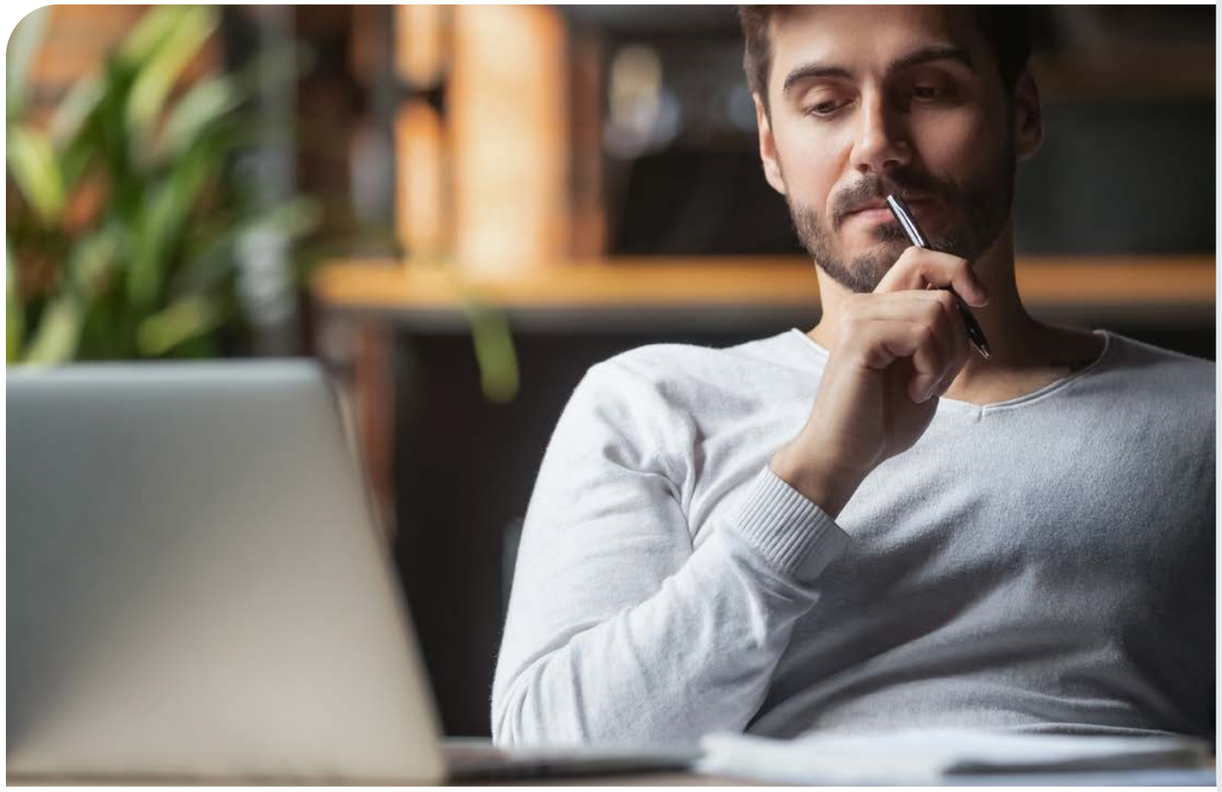
Το πρόβλημα αυτό εντείνεται περαιτέρω αν συνυπολογίσει κανείς και το κυρίαρχο νομοθετικό και κανονιστικό τοπίο. Το ευρύτερο κανονιστικό περιβάλλον και οι απαιτήσεις συμμόρφωσης που απορρέουν από αυτό παρουσιάζουν ολοένα και μεγαλύτερες τάσεις κατακερματισμού καθώς, όπως και οι επιχειρήσεις, προσπαθούν να προσαρμοστούν στις γρήγορες τεχνολογικές εξελίξεις.

Στόχος της Microsoft είναι να παρέχει συνεχώς **καινοτόμες λύσεις** που θα προετοιμάζουν τους πελάτες της για τις σχετικές τεχνολογικές εξελίξεις.

Είναι, λοιπόν, σαφές ότι οι επιχειρήσεις θα πρέπει να εξοπλιστούν κατάλληλα προκειμένου να διασφαλίσουν την ικανότητά τους να προσαρμόζονται στις νέες τεχνολογίες, να διατηρούν τα ζητήματα κυβερνοασφάλειας υπό έλεγχο και να συμμορφώνονται με τις απαιτήσεις των κλαδικών, κρατικών ή τοπικών κανονισμών με αποτελεσματικό τρόπο. Κατ' επέκταση, η αξιοποίηση των κατάλληλων εργαλείων για τη διευκόλυνση των παραπάνω σκοπών παίζει κρίσιμο ρόλο τόσο για τις καθημερινές διαδικασίες όσο και μακροπρόθεσμα.

Η σουίτα λύσεων ασφάλειας της Microsoft για περιβάλλοντα cloud, on-premises περιβάλλοντα και υβριδικές αρχιτεκτονικές απευθύνεται σε όλες τις επιχειρήσεις, ανεξαρτήτως τομέα και κλάδου, και μπορεί να τις βοηθήσει να ενισχύσουν τις ικανότητές τους σε επίπεδο κυβερνοασφάλειας και να απλοποιήσουν τη συμμόρφωσή τους με τους κανονισμούς, ώστε να είναι σε θέση να επικεντρωθούν στην ανάπτυξή τους. Ταυτόχρονα, στόχος της Microsoft είναι να παρέχει συνεχώς καινοτόμες λύσεις που θα προετοιμάζουν τους πελάτες της για τις σχετικές τεχνολογικές εξελίξεις. Για παράδειγμα, το ολοκαίνουριο Security Copilot της Microsoft είναι ένα εργαλείο ανάλυσης ασφάλειας που αξιοποιεί τις δυνατότητες της τεχνητής νοημοσύνης και της μηχανικής μάθησης και μπορεί να βοηθήσει τις επιχειρήσεις να ανταποκρίνονται άμεσα στις απειλές και να αξιολογούν τα σήματα κινδύνων και διαδικασιών με αστραπιαία ταχύτητα, βελτιώνοντας τις συνολικές δυνατότητες αντιμετώπισης περιστατικών, εντοπισμού απειλών και αναφοράς συμβάντων ασφάλειας.

Ταυτόχρονα, η διευρυμένη στρατηγική συμμαχία της Microsoft με την EY εξασφαλίζει ολοκληρωμένες υπηρεσίες ασφάλειας για τις επιχειρήσεις, οι οποίες θα τις βοηθήσουν στην επίτευξη του ψηφιακού μετασχηματισμού τους μέσα από την αντιμετώπιση των σχετικών επιχειρηματικών και κανονιστικών προκλήσεων, επιτρέποντάς τους έτσι να κάνουν τη μετάβαση στο cloud και να καινοτομήσουν σε αυτό το περιβάλλον, χρησιμοποιώντας τις συμβουλευτικές υπηρεσίες για επιχειρηματικά και τεχνολογικά θέματα που προσφέρει η EY σε συνδυασμό με τις λύσεις ασφάλειας και cloud της Microsoft.



## EY | Building a better working world

Στην EY, σκοπός μας είναι η δημιουργία ενός καλύτερου εργασιακού κόσμου, παράγοντας μακροπρόθεσμη αξία για τους πελάτες μας, τους ανθρώπους μας και την κοινωνία, και οικοδομώντας εμπιστοσύνη στις κεφαλαιαγορές.

Αξιοποιώντας τα δεδομένα και την τεχνολογία, οι πολυσυνθετικές ομάδες μας, σε περισσότερες από 150 χώρες, οικοδομούν την εμπιστοσύνη μέσω της διασφάλισης της καλής λειτουργίας των επιχειρήσεων και βοηθούν τους πελάτες μας να αναπτυχθούν, να μετασχηματιστούν και να λειτουργήσουν αποτελεσματικότερα.

Μέσω των Ελεγκτικών, Συμβουλευτικών, Νομικών και Φορολογικών Υπηρεσιών μας, καθώς και μέσω των Συμβουλευτικών Υπηρεσιών Εταιρικής Στρατηγικής και Συναλλαγών, οι ομάδες της EY θέτουν καλύτερες ερωτήσεις, για να καταλήξουν σε νέες απαντήσεις στα περίπλοκα ζητήματα που αντιμετωπίζει ο κόσμος μας σήμερα.



ey.com

Για περισσότερες πληροφορίες, παρακαλούμε επικοινωνήστε με:

**Παναγιώτης Παπαγιαννακόπουλος**
Εταίρος, Deputy CESA Cyber Security Services Leader,
EY Ελλάδος
**T** +30 210 2886 676
**E** panagiotis.papagiannakopoulos@gr.ey.com

**Αντώνιος Μπρούμας**
Senior Manager, Digital Law,
Platis - Anastasiadis & Associates Law Partnership, EY Law
**T** +30 210 6171 502
**E** antonios.broumas@gr.ey.com

**Νικόλαος Γαργάλης**
Manager, Technology Consulting Cybersecurity,
EY Ελλάδος
**T** +30 210 2886 835
**E** nikolaos.gargalis@gr.ey.com

EY @EY_Greece EY Greece
eygreece EY Greece

## Microsoft

Με έτος ίδρυσης το 1975, Η Microsoft (Nasdaq "MSFT" @microsoft) καθιστά δυνατή την ψηφιακή μετάβαση στην εποχή του ευφυούς υπολογιστικού νέφους και του «ευφυούς άκρου» (intelligent edge). Η αποστολή της είναι να ενδυναμώσει κάθε άτομο και κάθε οργανισμό στον πλανήτη για να πετύχει περισσότερα.

Η Microsoft ξεκίνησε τις δραστηριότητές της στην Ελλάδα το 1992. Τα τελευταία 30 χρόνια, η Microsoft Hellas προσφέρει λογισμικό, υπηρεσίες, συσκευές και λύσεις που βοηθούν ανθρώπους και επιχειρήσεις να αξιοποιήσουν πλήρως τις δυνατότητές τους. Το 2020 η Microsoft ξεκίνησε την πρωτοβουλία Gr for Growth, μία σημαντική τεχνολογική δέσμευση απέναντι στους πολίτες, τον Δημόσιο τομέα και τις επιχειρήσεις κάθε μεγέθους της Ελλάδας για τεχνολογία και νέους πόρους που δημιουργούν πρόσθετες ευκαιρίες ανάπτυξης.

Στο πλαίσιο της πρωτοβουλίας αυτής, η Microsoft θα κατασκευάσει ένα συγκρότημα τριών Datacenter στην Αττική, βάζοντας τη χώρα στον παγκόσμιο χάρτη cloud υποδομών της Microsoft – το μεγαλύτερο του κόσμου - διασφαλίζοντας έτσι πρόσβαση σε επιχειρησιακού επιπέδου υπηρεσίες Cloud «χαμηλής καθυστέρησης». Ταυτόχρονα, για να υποστηρίξει τους Έλληνες πολίτες στους επαγγελματικούς και αλλά και προσωπικούς τους στόχους, η Microsoft θα εκπαιδεύσει ένα ανθρώπινο δυναμικό 100.000 πολιτών στις ψηφιακές δεξιότητες, μέχρι το 2025.



microsoft.com

Για περισσότερες πληροφορίες, παρακαλούμε επικοινωνήστε με:

**Δημήτριος Πάτσος**
CISSP, CISM, CDPSE, CCSK Sr Specialist,
Security Specialist Technology Unit
Microsoft Greece, Cyprus, Malta
**T** +30 211 1206 371
**E** dpatsos@microsoft.com

**Δημήτρης Χουστουλάκης**
Sr Partner Development Manager
Global Partner Solutions (GPS)
Southeast Europe, Microsoft
**T** +30 211 1206 152
**E** dichoust@microsoft.com

**Σταμάτης Κασμάς**
Sr Business Strategy Manager
Data Centre Lead
Microsoft Greece, Cyprus, Malta
**T** +30 211 1206 038
**E** stamatis.kasmas@microsoft.com

Microsoft Microsoft
Microsoft Greece