NIS 2

What SMEs need to know

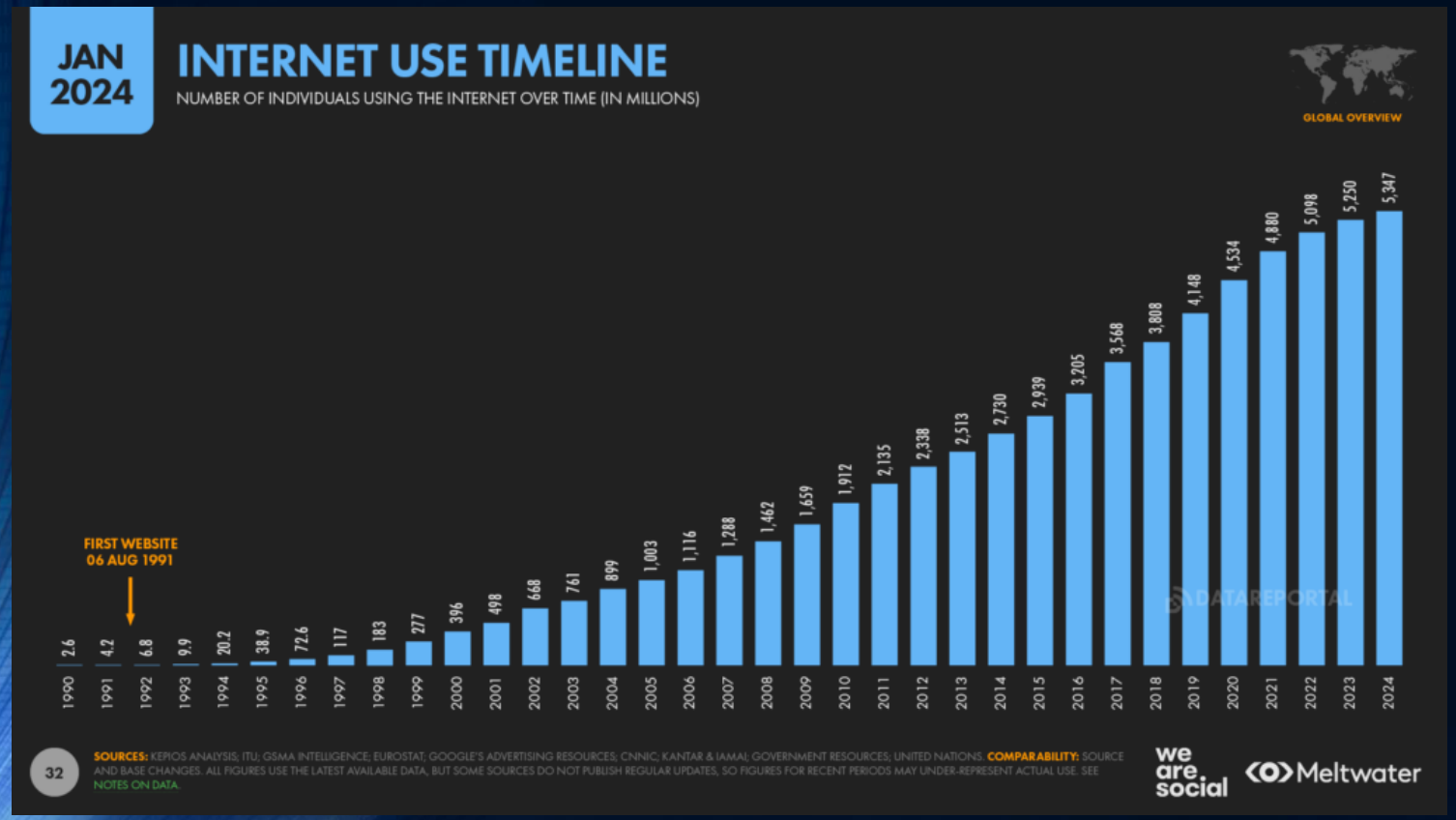
Αλίκη Διακίδου

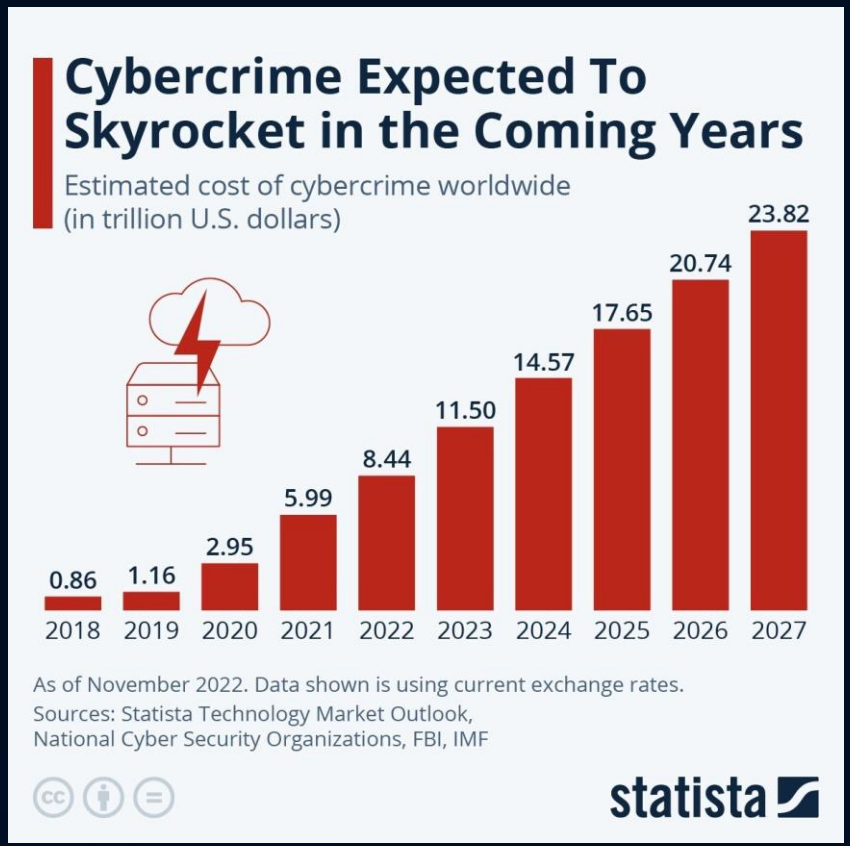
Αν. Προϊσταμένη Τμήμα Κανονιστικής Συμμόρφωσης

Γενική Δ/νση Επιτελικού Σχεδιασμού

Εθνική Αρχή Κυβερνοασφάλειας

Χρήση διαδικτύου και κυβερνοέγκλημα

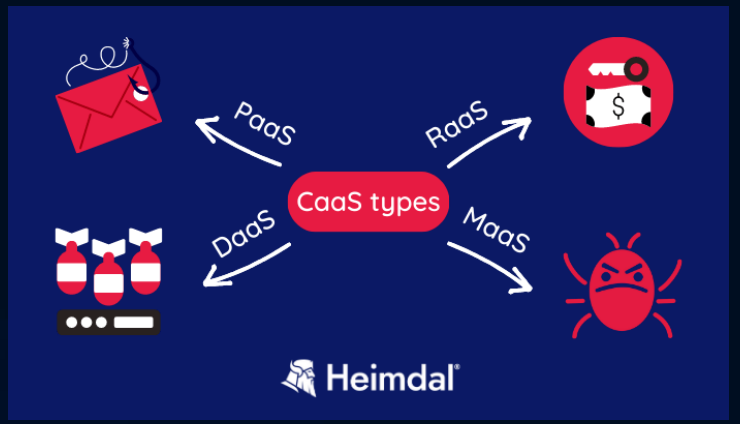




Κυβερνοέγκλημα ως υπηρεσία (CaaS)

- Ετήσιο παγκόσμιο κόστος κυβερνοεγκλήματος: επικερδέστερο από το λαθρεμπόριο ναρκωτικών. Η 3η μεγαλύτερη «οικονομία» παγκοσμίως.

- CaaS: επιχειρηματικό μοντέλο για το οργανωμένο διαδικτυακό έγκλημα, όπου κυβερνοεγκληματίες θέτουν τα εργαλεία/υπηρεσίες τους προς αγορά / ενοικίαση προς όποιον έχει κακόβουλο σκοπό. Δεν απαιτείται τεχνογνωσία από τον επιτιθέμενο, παρά μόνο:
  - Μια σύνδεση στο internet
  - Λίγα (ή περισσότερα..) χρήματα
  - Κακόβουλη πρόθεση
- CaaS: PaaS, RaaS, DaaS, MaaS



Η Οδηγία 2022/2555 (NIS 2) - Εισαγωγικές παρατηρήσεις

- ✓ Πολύ μικρή διακριτική ευχέρεια στα ΚΜ κατά τη μεταφορά της Οδηγία στο εθνικό τους δίκαιο
- ✓ Σημαντική ενίσχυση απαιτήσεων για:
  - ✓ τις αρμόδιες Εθνικές Αρχές
  - ✓ Τους υπόχρεους Οργανισμούς
    - ✓ Υποχρεώσεις λήψης μέτρων
    - ✓ Υποχρεώσεις αναφοράς περιστατικών
- ✓ Σημαντική ενδυνάμωση του πλαισίου ελέγχων, «εποπτείας και επιβολής»
  - ✓ Βασικές οντότητες: ex ante & ex post έλεγχοι
  - ✓ Σημαντικές οντότητες: μόνο ex post έλεγχοι
- ✓ Έμφαση στην ανταλλαγή πληροφοριών και την επικοινωνία μεταξύ Οργανισμών και Εθνικών Αρχών, καθώς και διευρωπαϊκής συνεργασίας
- ✓ Εφαρμογή: 18 Οκτωβρίου 2024

NIS2: Διεύρυνση του πεδίου εφαρμογής + κανόνας “size-cap”

NIS
Διαχειριστές βασικών υπηρεσιών (OES) και πάροχοι ψηφιακών υπηρεσιών (DSP)

- ΕΝΕΡΓΕΙΑ
- ΠΟΣΙΜΟ ΝΕΡΟ
- ΨΗΦΙΑΚΕΣ ΥΠΟΔΟΜΕΣ
- ΨΗΦΙΑΚΟΙ ΠΑΡΟΧΟΙ ΥΠΗΡΕΣΙΩΝ
- ΥΠΟΔΟΜΕΣ ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΩΝ ΑΓΟΡΩΝ
- ΜΕΤΑΦΟΡΕΣ
- ΥΓΕΙΑ

NIS II
Επέκταση του πεδίου εφαρμογής ώστε να συμπεριληφθούν περισσότεροι τομείς και υπηρεσίες είτε ως βασικές είτε ως σημαντικές οντότητες.

- ΠΑΡΟΧΟΙ ΔΗΜΟΣΙΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
- ΔΙΑΣΤΗΜΑ
- ΚΑΤΑΣΚΕΥΗ ΟΡΙΣΜΕΝΩΝ ΚΡΙΣΙΜΩΝ ΠΡΟΪΟΝΤΩΝ (ΟΠΩΣ ΦΑΡΜΑΚΕΥΤΙΚΑ ΠΡΟΪΟΝΤΑ, ΙΑΤΡΙΚΕΣ ΣΥΣΚΕΥΕΣ, ΧΗΜΙΚΑ)
- ΤΑΧΥΔΡΟΜΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΤΑΧΥΜΕΤΑΦΟΡΩΝ
- ΨΗΦΙΑΚΕΣ ΥΠΗΡΕΣΙΕΣ : ΥΠΗΡΕΣΙΕΣ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ ΠΛΑΤΦΟΡΜΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΚΕΝΤΡΩΝ ΔΕΔΟΜΕΝΩΝ, ΠΑΡΟΧΟΙ ΥΠΗΡΕΣΙΩΝ ΝΕΦΟΥΣ
- ΔΙΑΧΕΙΡΙΣΗ ΑΠΟΒΛΗΤΩΝ ΚΑΙ ΛΥΜΑΤΩΝ
- ΤΡΟΦΙΜΑ
- ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

Αναβαθμισμένες υποχρεώσεις οργανισμών

- Risk-based approach για βασικές και σημαντικές οντότητες και λεπτομερή μέτρα διαχείρισης κινδύνων
- Μέτρα για τον έλεγχο της εφοδιαστικής αλυσίδας
- Ανώτατη διοίκηση: εγκρίνει τα μέτρα, επιβλέπει την εφαρμογή τους, λογοδοτεί εκ μέρους του Οργανισμού, ευθύνεται έως και προσωπικώς, λαμβάνει ειδική κατάρτιση
- Υποχρέωση αναφοράς σημαντικών περιστατικών

RISK MANAGEMENT

Accountability for top management for non-compliance

Essential and important companies are required to take security measures

Companies are required to notify incidents

Μέτρα διαχείρισης κινδύνων

Χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας	Πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων	Ασφάλεια της αλυσίδας εφοδιασμού
Basic cyber-hygiene measures	Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας.	Ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών
Πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας	Ασφάλεια ανθρώπινων πόρων. Πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων	Χειρισμός περιστατικών

RISK MANAGEMENT

Accountability for top management for non-compliance

Essential and important companies are required to take security measures

Companies are required to notify incidents

Λεπτομερής καθορισμός τεχνικών και οργανωτικών μέτρων

- Έκδοση εκτελεστής πράξης COMM για DNS, TLD, cloud providers, data centers, (S)MSPs, TSPs κλπ.
- Έκδοση reference document για βασικές και σημαντικές οντότητες
- 13 «θεματικές περιοχές - οικογένειες μέτρων» και εξειδίκευσή τους σε 50 «στόχους ασφάλειας»:
  - Καθορισμός του Στόχου
  - Καθοδήγηση εφαρμογής
  - Περιοδική αναθεώρηση των μέτρων
  - Παραδείγματα εφαρμογής και evidence υλοποίησης
  - Mapping με γνωστά διεθνή πρότυπα
- Ήδη σε επεξεργασία από την ΕΑΚ η δευτερογενής νομοθεσία

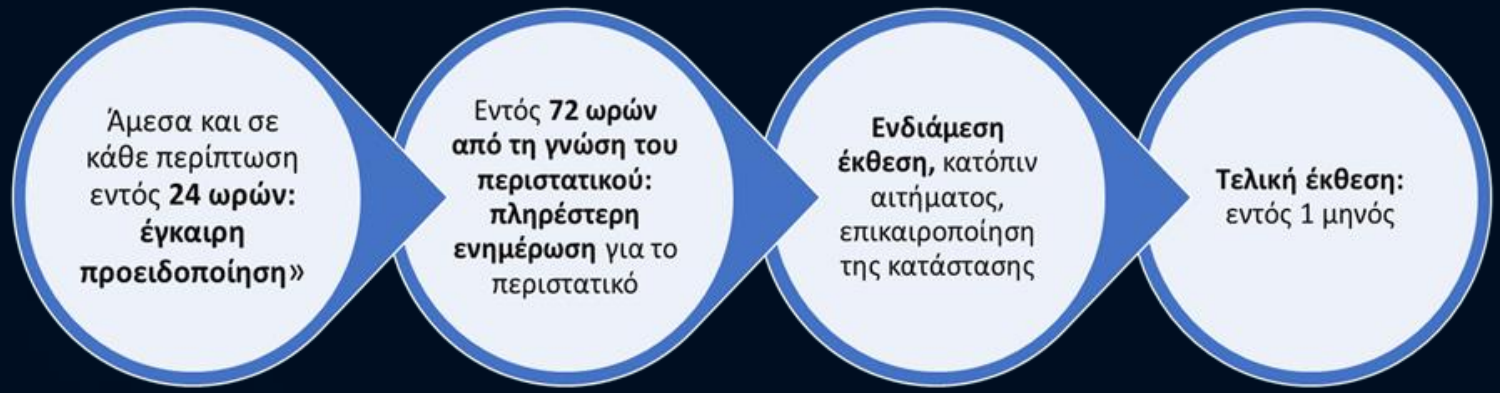
RISK MANAGEMENT

Accountability for top management for non-compliance

Essential and important companies are required to take security measures

Companies are required to notify incidents

Χρονοδιάγραμμα για την αναφορά περιστατικών ασφαλείας – προσέγγιση πολλαπλών σταδίων

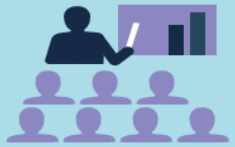


Λογοδοσία Διοίκησης

Εγκρίνει τα μέτρα διαχείρισης κινδύνων που λαμβάνουν οι φορείς σύμφωνα με το άρθρο 21

Επιβλέπει την εφαρμογή των μέτρων διαχείρισης κινδύνων

Παρακολουθεί **εκπαίδευση**



Φροντίζει για την **κατάρτιση των υπαλλήλων** του φορέα σε τακτική βάση, για να εντοπίζουν κινδύνους και να αξιολογούν πρακτικές διαχείρισης κινδύνων στον τομέα Κυβερνοασφάλειας

Λογοδοτεί για την παραβίαση των υποχρεώσεων του άρθρου 20, εκ μέρους του φορέα

Εποπτεία και επιβολή

- Αναλύονται πληρέστερα τα μέτρα εποπτείας
  - Regular- targeted audits, on-site and off-site checks, security scans
  - Διαθέσιμα μέσα για τις αρμόδιες αρχές (αίτημα παροχής πληροφοριών – πρόσβαση σε στοιχεία)
  - Προβλέπεται διαφοροποίηση των μέτρων με βάση το είδος των οντοτήτων (essential – important entities)
  - Η ανώτατη διοίκηση των βασικών και σημαντικών οντοτήτων εγκρίνει τα μέτρα διαχείρισης του κινδύνου κυβερνοασφάλειας, εποπτεύει την εφαρμογή τους και είναι υπόλογη για τη μη συμμόρφωση των οντοτήτων (άρθρο 20 nis2)
  - Τα μέλη της ανώτατης διοίκησης παρακολουθούν σε τακτική βάση ειδικές εκπαιδεύσεις, ώστε να αποκτούν επαρκείς γνώσεις και δεξιότητες για να αντιλαμβάνονται και να αξιολογούν τους κινδύνους και τις πρακτικές διαχείρισης της κυβερνοασφάλειας και τις επιπτώσεις τους στις λειτουργίες της οντότητας
  - Υποχρέωση επίδειξης συμμόρφωσης εκ μέρους των Οργανισμών

Εποπτεία και επιβολή

- Κατάλληλα, αναλογικά και αποτελεσματικά μέτρα εποπτείας και επιβολής (πλέον των προστίμων), όπως αναστολή παροχής υπηρεσιών ή απαγόρευση άσκησης διευθυντικών καθηκόντων
- Κυρώσεις για:
  - Παραβίαση απαιτήσεων σχετικά με τα μέτρα διαχείρισης κινδύνων ή
  - Μη συμμόρφωση με τις υποχρεώσεις αναφοράς περιστατικού
- Διοικητικά πρόστιμα:
  - Βασικές οντότητες: έως 10 εκατ. ευρώ ή 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, ανάλογα με το υψηλότερο
  - Σημαντικές οντότητες έως 7 εκατ. ευρώ ή 1,4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, ανάλογα με το υψηλότερο
- **Σημαντική ενίσχυση του «νομικού κινδύνου» (legal risk)**

Ενδεικτικά βήματα για οργανισμούς (1/4)

1. Gap analysis

Διαδικασία αξιολόγησης του βαθμού υφιστάμενου επιπέδου ασφάλειας πληροφοριών έναντι ενός συγκεκριμένου προτύπου/πλαισίου. Αναγνωρίζεται «τί διαθέτω σήμερα» και «τί θα πρέπει να διαθέτω» όσον αφορά στη συμμόρφωση με ένα πλαίσιο και επικεντρώνεται σε μέτρα ή λειτουργίες.

2. Risk assessment

Συστηματική διαδικασία με την οποία ο οργανισμός κατανοεί τους κινδύνους κυβερνοασφάλειας για τις λειτουργίες του (αποστολή, κρίσιμες υπηρεσίες, φήμη), για τα αγαθά του και για τα πρόσωπα. Εντοπίζονται οι απειλές και οι ευπάθειες για τα πληροφοριακά συστήματα, αξιολογείται η πιθανότητα επέλευσης περιστατικών κυβερνοασφάλειας και καθορίζονται οι δυνητικές επιπτώσεις από την επέλευση τέτοιων συμβάντων.

Ενδεικτικά βήματα για οργανισμούς (2/4)

3. Εκπόνηση πολιτικών ασφάλειας

- Σε υψηλό επίπεδο, ο οργανισμός πρέπει να ορίσει μία γενική πολιτική ασφάλειας, η οποία εγκρίνεται από την ανώτατη Διοίκηση και καθορίζει την προσέγγιση του οργανισμού όσον αφορά στη διαχείριση της ασφάλειας των πληροφοριών του.
- Σε ένα χαμηλότερο επίπεδο, η γενική πολιτική ασφάλειας υποστηρίζεται από έναν αριθμό θεματικών πολιτικών, οι οποίες καθορίζουν τους κανόνες και τις διαδικασίες σε συγκεκριμένες θεματικές ενότητες ασφάλειας (π.χ. έλεγχος πρόσβασης, συνθηματικά, φυσική ασφάλεια, ασφάλεια δικτύου, backup, αντιμετώπιση περιστατικών, διαχείριση αγαθών κ.α.).

4. Υλοποίηση μέτρων κυβερνοασφάλειας

Με βάση τα αποτελέσματα της αποτίμησης επικινδυνότητας, ο οργανισμός εφαρμόζει πλάνο αντιμετώπισης κινδύνων, το οποίο περιλαμβάνει ένα σύνολο μέτρων κυβερνοασφάλειας, τόσο σε οργανωτικό επίπεδο (πολιτικές, διαδικασίες, ορισμός CISO, εκπαίδευση κ.α.) όσο και σε τεχνικό επίπεδο (υλοποίηση τεχνολογικών μέτρων, όπως antivirus, EDR, firewalls, multi-factor authentication, network segmentation, identity and access control management, disaster recovery site κ.α.).

Ενδεικτικά βήματα για οργανισμούς (3/4)

5. Εκπαίδευση και ευαισθητοποίηση

Υλοποιείστε σεμινάρια εκπαίδευσης και ευαισθητοποίησης του προσωπικού σε θέματα κυβερνοασφάλειας:

- εκπαίδευση στο προσωπικό και σε μέλη της Διοίκησης σχετικά με βασικά θέματα κυβερνοϋγιεινής (αντιμετώπιση phishing emails, δημιουργία ισχυρών συνθηματικών, χρήση multi-factor authentication, λήψη backup κ.α.) και
- στοχευμένη εκπαίδευση σε προσωπικό ειδικών ρόλων σχετικά με εξειδικευμένα τεχνικά θέματα (ασφαλής παραμετροποίηση συσκευών, διαδικασίες αντιμετώπισης περιστατικών κ.α.).

Ενδεικτικά βήματα για οργανισμούς (4/4)

6. Διενέργεια ελέγχων

Ανά τακτά χρονικά διαστήματα, αξιολογήστε την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας που έχετε υλοποιήσει μέσω της διενέργειας ελέγχων (internal / external audits, penetration tests, αυτοαξιολόγηση κ.α.).

7. Διαδικασίες βελτίωσης / ανατροφοδότησης

Με την ενεργή συμμετοχή της Διοίκησης, ανά τακτά χρονικά διαστήματα προβείτε σε συνολική αξιολόγηση και επιθεώρηση του προγράμματος κυβερνοασφάλειας του οργανισμού σας, εντοπίζοντας λάθη και παραλείψεις και με σκοπό τη συνεχή βελτίωση και ανατροφοδότησή του.

ΤΗΡΕΙΤΕ ΕΓΓΡΑΦΑ – EVIDENCE ΥΛΟΠΟΙΗΣΗΣ

Μια νέα «αγορά» στον τομέα της κυβερνοασφάλειας (1/2)

- Μια αγορά που έως σήμερα λειτουργεί σε εθελοντική βάση, καθίσταται υποχρεωτική.
- Αφορά πρωτίστως μεσαίες επιχειρήσεις και άνω, που δραστηριοποιούνται στους τομείς της Οδηγίας (με τουλάχιστον 50 εργαζόμενους / 10 εκ. ευρώ ετήσιο κύκλο εργασιών)
- Αναμένεται να προκύψει οικονομική επιβάρυνση, ανάλογα με τον υφιστάμενο βαθμό ωριμότητας κάθε φορέα.
- Ταυτόχρονα όμως ενισχύεται η ανθεκτικότητά τους στον κυβερνοχώρο, καθίστανται λιγότερο ευάλωτες σε ζημίες από κυβερνοεπιθέσεις και ενισχύεται και η ανταγωνιστικότητά τους.

Μια νέα «αγορά» στον τομέα της κυβερνοασφάλειας (2/2)

- Αναμένεται αύξηση της ζήτησης σε υπηρεσίες, προϊόντα και ειδικούς στον τομέα της κυβερνοασφάλειας, της πληροφορικής, καθώς και σε άλλες ειδικότητες (συμβουλευτικές και νομικές υπηρεσίες, εκπαίδευση κυβερνοασφάλειας).

- Προσεκτική «ρύθμιση» και εναρμονισμένη προσέγγιση, με σεβασμό της οικονομικής ελευθερίας, με βάση τη μέχρι σήμερα εμπειρία, υπό το πρίσμα της προστασίας πτυχών της εθνικής ασφάλειας

NIS 2 & προκλήσεις για τις ΜΜΕ

- Περιορισμένοι πόροι
- Έλλειψη εξειδίκευσης
- Πολυπλοκότητα συμμόρφωσης

- Απόλυτη ασφάλεια: ένας στόχος ανέφικτος, ανορθολογικός και μη επιθυμητός..
- Στόχος αμυνόμενου:
  - Κόστος επιτυχούς επίθεσης > κίνητρο x όφελος επιτιθέμενου
  - Επίδειξη «συμμόρφωσης»
- Αλυσίδα ασφάλειας: τόσο ισχυρή όσο ο πιο αδύναμος κρίκος
  - Έλεγχος εφοδιαστικής αλυσίδας
  - Ανθρώπινος παράγοντας
  - Εκπαίδευση – ευαισθητοποίηση - κουλτούρα

Ευχαριστώ θερμά για την προσοχή σας