TASSIS & ASSOCIATES
LAW OFFICE

Κυβερνοασφάλεια και Προστασία Δεδομένων στον τομέα της Ενέργειας

eThemis
Βόλος | 9-10 Μαρτίου 2023

Part of ICTLC

Εισαγωγή

TASSIS
& ASSOCIATES
LAW OFFICE

- Η κυβερνοασφάλεια στον τομέα της ενέργειας είναι κρίσιμης σημασίας
- Τα δίκτυα ενέργειας αποτελούν κρίσιμες υποδομές
- Οι υπηρεσίες στον τομέα της ενέργειας είναι βασικές υπηρεσίες (essential services)
- Κάθε φορέας εκμετάλλευσης βασικών υπηρεσιών υπόκειται σε αυστηρούς κανόνες
- Τεχνολογία και Συνδεσιμότητα
- Συστήματα και Δίκτυα Πληροφορικής
- Πολλά και ποικίλα δεδομένα

Part of ICTLC

Προστασία δικτύων και δεδομένων

TASSIS & ASSOCIATES LAW OFFICE

➢ Απειλές:

- Κακόβουλο λογισμικό
- Phishing
- Ransomware
- Προηγμένες μόνιμες απειλές (APT) που στοχεύουν συγκεκριμένα άτομα ή τμήματα εντός του οργανισμού (social engineering) και χρησιμοποιούν έναν συνδυασμό τεχνικών και ψυχολογικών τακτικών για να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες.

Τρεις κύριες προκλήσεις που σχετίζονται με την ασφάλεια στον κυβερνοχώρο στον τομέα της ενέργειας:

- Οι συνέπειες είναι σοβαρές και άμεσα αισθητές σε ευρύ φάσμα της οικονομικής ζωής και μεγάλο αριθμό προσώπων.
- Τα προβλήματα σε ένα δίκτυο μπορούν εύκολα να μεταδοθούν και σε άλλα δίκτυα, πολλαπλασιάζοντας έτσι τις επιπτώσεις.
- Η ενεργειακή υποδομή αποτελείται τόσο από παλαιά όσο και από σύγχρονη τεχνολογία, γεγονός που καθιστά το σύστημα στο σύνολό του πολύ ευάλωτο.

Part of ICTLC

Περιπτώσεις απειλών και παραβιάσεων

TASSIS & ASSOCIATES LAW OFFICE

- Επίθεση στη Saudi Aramco το 2012, μέσω κακόβουλου λογισμικού έπληξε τα συστήματα πληροφορικής της Saudi Aramco. Πιστεύεται ότι πραγματοποιήθηκε από μια ιρανική ομάδα χάκερ και κατέστρεψε περισσότερους από 30.000 υπολογιστές.
- Κυβερνοεπίθεση στο ουκρανικό ηλεκτρικό δίκτυο τον Δεκέμβριο του 2015 προκάλεσε διακοπή ρεύματος που επηρέασε πάνω από 225.000 πελάτες στην Ουκρανία. Η επίθεση αποδόθηκε σε ρωσική ομάδα χάκερ και αφορούσε τη χρήση κακόβουλου λογισμικού για την απόκτηση πρόσβασης στα συστήματα πληροφορικής και στα συστήματα ελέγχου της εταιρείας ενέργειας.
- Επίθεση NotPetya το 2017 (ransomware) που μόλυνε υπολογιστές σε όλο τον κόσμο, συμπεριλαμβανομένων εκείνων που ανήκαν σε διάφορες ενεργειακές εταιρείες.
- Επίθεση ομάδας χάκερ Dragonfly 2.0, το 2018 σε ενεργειακές εταιρείες στις ΗΠΑ και Ευρώπη. Η ομάδα πιστεύεται ότι είχε δεσμούς με τη ρωσική κυβέρνηση και προσπαθούσε να αποκτήσει πρόσβαση σε βιομηχανικά συστήματα ελέγχου που θα μπορούσαν να χρησιμοποιηθούν για τη διακοπή του ενεργειακού εφοδιασμού.
- Κυβερνοεπίθεση το 2021 στον Colonial Pipeline τον μεγαλύτερο αγωγό καυσίμων στις ΗΠΑ και πληρωμή ransomware 4,4 εκ. δολαρίων. Η διακοπή είχε ως αποτέλεσμα την έλλειψη βενζίνης, τη διακοπή των υπηρεσιών και την κλιμάκωση του κόστους της βενζίνης. Η επίθεση συνέβη εξαιτίας του παραβιασμένου κωδικού πρόσβασης ενός υπαλλήλου.
- Κυβερνοεπίθεση στον αγωγό Άμστερνταμ-Ρότερνταμ-Αντβέρπ (ARA) το 2022 λίγους μήνες μετά από παρόμοια επίθεση σε δύο γερμανικές εταιρείες που οδήγησε στη διακοπή του εφοδιασμού με βενζίνη σε βόρειες περιοχές της Γερμανίας. Επηρεάστηκαν 11 εγκαταστάσεις της Oiltanking στη Γερμανία.

Part of ICTLC

Περιπτώσεις απειλών και παραβιάσεων

TASSIS & ASSOCIATES LAW OFFICE

- OPEL και Electrobras (βραζιλιάνικες εταιρείες κοινής ωφέλειας) το 2021 χτυπήθηκαν από επίθεση από ransomware που απέσπασε 1.000 GB δεδομένων. Και οι δύο πάροχοι ηλεκτρικής ενέργειας αναγκάστηκαν να αποσυνδεθούν από το Εθνικό Διασυνδεδεμένο Σύστημα, γεγονός που προκάλεσε προσωρινή ταλαιπωρία σε πολλούς στη χώρα. Η εταιρεία δήλωσε ότι η τήρηση των πρωτοκόλλων ασφαλείας βοήθησε στην προστασία της ακεραιότητας των δεδομένων της.

- Κυβερνοεπίθεση σε μέρος της υποδομής πληροφορικής του ΔΕΣΦΑ από κυβερνοεγκληματίες που προσπάθησαν να έχουν παράνομη πρόσβαση σε ηλεκτρονικά αρχεία με επιβεβαιωμένη επίπτωση στη διαθεσιμότητα ορισμένων συστημάτων και πιθανή διαρροή αριθμού αρχείων και δεδομένων (Αύγουστος 2022). Ο ΔΕΣΦΑ απενεργοποίησε προληπτικά τις περισσότερες από τις υπηρεσίες πληροφορικής. «Ο ΔΕΣΦΑ παραμένει ακλόνητος στη θέση του να μη συνδιαλέγεται με κυβερνοεγκληματίες».

- Παρατηρούνται αυξανόμενες οι επιθέσεις σε συστήματα βιομηχανικού αυτοματισμού (Operational Technology)

- Η Ελλάδα είναι ανάμεσα στις δέκα κυριότερες χώρες με ενεργές «μολύνσεις», όπου οι επιτιθέμενοι υπέκλεψαν πληροφορίες από παραβιασμένα συστήματα, χωρίς να είναι σαφές ποιοι ακριβώς ήταν οι στόχοι των χάκερ. Οι χώρες που έχουν πληγεί περισσότερο, είναι οι εξής: Ισπανία (27%), ΗΠΑ (24%), Γαλλία (9%), Ιταλία (8%), Γερμανία (7%), Τουρκία (6%), Ρουμανία, Πολωνία και Ελλάδα (από 5%) και Σερβία (4%).

Part of ICTLC

Οδηγίες NIS 1 και NIS 2

TASSIS & ASSOCIATES LAW OFFICE

➢ NIS 1 (οδηγία 2016/1148, ν. 4577/2018 και ΥΑ 1027/8.10.2019)

- Οι Φορείς εκμετάλλευσης βασικών υπηρεσιών (ΦΕΒΥ) στους τομείς της ενέργειας, των μεταφορών, τον τραπεζικό, τις Υποδομές Χρηματοπιστωτικών Αγορών, την Υγεία, την Ύδρευση και τις Ψηφιακές Υποδομές, οφείλουν να λαμβάνουν όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ικανοποίηση του σκοπού της Οδηγίας και ευθύνονται για το σύνολο των πράξεων οποιουδήποτε συνεργάτη, που χρησιμοποιεί για την κατασκευή, εγκατάσταση, συντήρηση ή λειτουργία των συστημάτων δικτύου και πληροφοριών του για την παροχή των βασικών υπηρεσιών του.

- Σοβαρή διατάραξη, θεωρείται οποιοδήποτε συμβάν με επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών όταν πληροί τουλάχιστον μία από τις ακόλουθες συνθήκες:

  α) Κάθε συμβάν κατά το οποίο η συνέχεια της υπηρεσίας που παρέχεται από τον φορέα επηρεάζεται για πάνω από 100.000 χρηστοώρες. Ως συνέχεια της υπηρεσίας ορίζεται η δυνατότητα παροχής της υπηρεσίας σε αποδεκτά επίπεδα **εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και αυθεντικότητας**.
  β) Κάθε συμβάν που επηρεάζει πληθυσμό **τουλάχιστον 50.000 χρηστών**.
  γ) Απειλή σε ανθρώπινη ζωή. Σε περίπτωση απώλειας ανθρώπινης ζωής το συμβάν κρίνεται αυτομάτως κοινοποιήσιμο.
  δ) Το συμβάν έχει προκαλέσει υλικές ζημιές στον ίδιο τον φορέα ή σε άλλους φορείς που υπερβαίνουν **το 1.000.000 ευρώ**.

Part of ICTLC

Οδηγίες NIS 1 και NIS 2

TASSIS & ASSOCIATES LAW OFFICE

➢ NIS 1 (οδηγία 2016/1148, ν. 4577/2018 και ΥΑ 1027/8.10.2019)

ΦΕΒΥ στην ενέργεια:

Α. Υποτομέας ηλεκτρικής ενέργειας:

α) Προμήθεια ηλεκτρικής ενέργειας σε περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής ηλεκτρικής ενέργειας ή να διαθέτει περισσότερους από 500.000 πελάτες ή να προμηθεύει το 10% της συνολικής τροφοδοτούμενης ισχύος στο Εθνικό Σύστημα Μεταφοράς Ηλεκτρικής Ενέργειας (ΕΣΜΗΕ) ή να τροφοδοτεί το ΕΣΜΗΕ με ισχύ τουλάχιστον 1,5 GW,

β) Διανομή ηλεκτρικής ενέργειας σε περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής ή να διαθέτει περισσότερους από 500.000 πελάτες συνδεδεμένους στο δίκτυο διανομής ηλεκτρικής ενέργειας.

γ) Μεταφορά ηλεκτρικής ενέργειας για τουλάχιστον το 10% των TWh που διακινούνται ετησίως στο Εθνικό Σύστημα Μεταφοράς Ηλεκτρικής Ενέργειας (ΕΣΜΗΕ) ή να διαχειρίζεται το 5TWh που διακινούνται ετησίως στο ΕΣΜΗΕ.

Β. Υποτομέας πετρελαίου:

α) Μεταφορά πετρελαίου μέσω αγωγού, άνω του 10% των ετήσιων αναγκών της χώρας σε πετρέλαιο ή τουλάχιστον 1,5 εκατομμύριο κυβικά μέτρα πετρέλαιο ετησίως.

β) Παραγωγή, διύλιση, επεξεργασία, αποθήκευση και μεταφορά πετρελαίου, πάνω από το 10% των ετήσιων αναγκών της χώρας σε πετρέλαιο ή τουλάχιστον 1,5 εκατομμύριο κυβικά μέτρα πετρέλαιο ετησίως.

Part of ICTLC

Οδηγίες NIS 1 και NIS 2

TASSIS & ASSOCIATES LAW OFFICE

- NIS 1 (οδηγία 2016/1148, ν. 4577/2018 και ΥΑ 1027/8.10.2019)

ΦΕΒΥ στην ενέργεια:

Γ. Υποτομέας αερίου:

α) Προμήθεια φυσικού αερίου στο Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου περισσότερα από 500.000.000 κυβικά μέτρα.

β) Διανομή φυσικού αερίου σε περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής ή να διαθέτει περισσότερους από 50.000 πελάτες συνδεδεμένους στο δικτύου διανομής φυσικού αερίου ή η δικαιοδοσία του να καλύπτει τα όρια μιας γεωγραφικής περιφέρειας.

γ) Μεταφορά φυσικού αερίου τουλάχιστον τα 10% ή 500.000.000 κυβικά μέτρα φυσικού αερίου που διακινούνται ετήσια στο Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου.

δ) Εγκαταστάσεις αποθήκευσης φυσικού αερίου με χωρητικότητα μεγαλύτερη από 100.000 κυβικά μέτρα υγροποιημένου φυσικού αερίου (ΥΦΑ).

ε) Διαχείριση συστημάτων ΥΦΑ με τεχνολογική ικανότητα να εισάγει περισσότερα από 10% της ετήσιας κατανάλωσης ή 500.000.000 κυβικά μέτρα φυσικού αερίου ετησίως στο Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου.

στ) Προμήθεια φυσικού αερίου σε περισσότερους από το 10% του συνόλου των πελατών του δικτύου διανομής φυσικού αερίου ή να διαθέτει τουλάχιστον 50.000 πελάτες συνδεδεμένους στο δίκτυο διανομής φυσικού αερίου.

ζ) Δυνατότητα διύλισης και επεξεργασίας φυσικού αερίου τουλάχιστον 500.000.000 κυβικά μέτρα.

Part of ICTLC

Οδηγίες NIS 1 και NIS 2

TASSIS & ASSOCIATES LAW OFFICE

➢ NIS 1 (οδηγία 2016/1148, ν. 4577/2018 και ΥΑ 1027/8.10.2019) – **ΚΥΡΩΣΕΙΣ**

- **Αν διαπιστωθεί ότι ΦΕΒΥ δεν κοινοποιεί ή κοινοποιεί με αδικαιολόγητη καθυστέρηση συμβάν με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών του, επιβάλλεται: αα) πρόστιμο μέχρι του ποσού των δεκαπέντε χιλιάδων (15.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων, ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.**
- **Αν διαπιστωθεί ότι ΦΕΒΥ δεν λαμβάνει κατάλληλα και αναλογικά, τεχνικά και οργανωτικά, προληπτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των δικτύων και των συστημάτων πληροφοριών που χρησιμοποιεί για τις υπηρεσίες αυτές, επιβάλλεται: αα) πρόστιμο μέχρι του ποσού των πενήντα χιλιάδων (50.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων, ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.**
- **Αν διαπιστωθεί ότι φυσικό ή νομικό πρόσωπο δεν παρέχει ή παρέχει με αδικαιολόγητη καθυστέρηση οποιαδήποτε σχετική πληροφορία που ζητείται κατά τη διενέργεια ελέγχου ή τη διερεύνηση περιστατικού, επιβάλλεται: αα) πρόστιμο μέχρι του ποσού των πενήντα χιλιάδων (50.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων, ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.**

Part of ICTLC

Οδηγίες NIS 1 και NIS 2

TASSIS & ASSOCIATES LAW OFFICE

➢ NIS 2 (Οδηγία (ΕΕ) 2022/2555)

Αποτελεί μια επικαιροποιημένη και πιο ολοκληρωμένη έκδοση της πρώτης Οδηγίας διότι:

- **Καθορίζει λεπτομερέστερες απαιτήσεις για την αναφορά περιστατικών, συμπεριλαμβανομένων συγκεκριμένων χρονικών πλαισίων για την αναφορά και των τύπων περιστατικών που πρέπει να αναφέρονται.**
- **Δημιουργεί την απαραίτητη δομή διαχείρισης κρίσεων στον κυβερνοχώρο (CyCLONe)**
- **Περιλαμβάνει λεπτομερέστερες απαιτήσεις ασφάλειας για τους ΦΕΒΥ όπως απαιτήσεις για κρυπτογράφηση και έλεγχο ταυτότητας.**
- **Εισάγει αυστηρότερες κυρώσεις για τη μη συμμόρφωση, συμπεριλαμβανομένων προστίμων ύψους έως και 2% του παγκόσμιου κύκλου εργασιών μιας εταιρείας.**
- **Δίνει μεγαλύτερη έμφαση στη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, συμπεριλαμβανομένης της δημιουργίας ενός κέντρου ικανοτήτων για την κυβερνοασφάλεια.**
- **Εισάγει νέες διαδικασίες όπως οι peer αξιολογήσεις για την ενίσχυση της συνεργασίας και της ανταλλαγής γνώσεων μεταξύ των κρατών μελών.**
- **Συνολικά, αποτελεί σημαντική επικαιροποίηση της οδηγίας NIS 1, αντικατοπτρίζοντας την αυξανόμενη σημασία της ασφάλειας στον κυβερνοχώρο και το εξελισσόμενο τοπίο απειλών.**

Part of ICTLC

Νομοθεσία προσωπικών δεδομένων

TASSIS & ASSOCIATES LAW OFFICE

- Η προστασία δεδομένων και η ασφάλεια στον κυβερνοχώρο είναι δύο στενά συνδεδεμένοι τομείς που ασχολούνται με τη διασφάλιση ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, κλοπή ή κατάχρηση. Η προστασία δεδομένων αναφέρεται στα μέτρα που λαμβάνονται για την προστασία προσωπικών ή ευαίσθητων πληροφοριών, ενώ η κυβερνοασφάλεια αναφέρεται στην προστασία των συστημάτων και των δικτύων υπολογιστών από απειλές στον κυβερνοχώρο.
- Η προστασία δεδομένων περιλαμβάνει τη χρήση ΚΤΟΜ για να διασφαλιστεί ότι οι ευαίσθητες πληροφορίες δεν αποκαλύπτονται ή δεν τίθενται σε κίνδυνο. Αυτό περιλαμβάνει την κρυπτογράφηση, τους ελέγχους πρόσβασης, την ασφαλή αποθήκευση και τη δημιουργία αντιγράφων ασφαλείας και ανάκτησης δεδομένων.
- Οι κανονισμοί προστασίας δεδομένων, όπως ο GDPR, απαιτούν από τους οργανισμούς να εφαρμόζουν τις αρχές της προστασίας της ιδιωτικής ζωής από τον σχεδιασμό, ώστε να διασφαλίζεται ότι η επεξεργασία των προσωπικών δεδομένων γίνεται με τρόπο που προστατεύει τα ατομικά δικαιώματα.
- Η κυβερνοασφάλεια επικεντρώνεται στην προστασία των συστημάτων και των δικτύων υπολογιστών από μη εξουσιοδοτημένη πρόσβαση, κακόβουλο λογισμικό, επιθέσεις phishing και άλλες απειλές στον κυβερνοχώρο. Αυτό περιλαμβάνει επίσης έναν συνδυασμό ΚΤΟΜ, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών, λογισμικό προστασίας από ιούς, εκπαίδευση των εργαζομένων και σχέδια αντιμετώπισης περιστατικών.
- Τόσο η προστασία των π.δ. όσο και η ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας για τις επιχειρήσεις και τους ιδιώτες προκειμένου να προστατευθούν από τις απειλές στον κυβερνοχώρο και να διασφαλίσουν την ιδιωτικότητα και την ασφάλεια των ευαίσθητων πληροφοριών. Είναι σημαντικό να υπάρχει μια ολοκληρωμένη προσέγγιση που να περιλαμβάνει τόσο την προστασία δεδομένων όσο και την κυβερνοασφάλεια για την προστασία από πιθανές απειλές.

Part of ICTLC

Νομοθεσία προσωπικών δεδομένων

TASSIS & ASSOCIATES LAW OFFICE

- Ο τομέας της ενέργειας είναι ένας σημαντικός κλάδος που συλλέγει και επεξεργάζεται ευαίσθητες πληροφορίες, όπως άμεσα δεδομένα πελατών (προσωπικά στοιχεία και οικονομικά δεδομένα) και πληροφορίες που έμμεσα δημιουργούν ένα αξιοποιήσιμο προφίλ φυσικών προσώπων (ώρες χρήσης, στοιχεία κατανάλωσης, μέση αξία ανά οικογένεια/καταναλωτή) που μπορεί να οδηγήσει σε αυτοματοποιημένη ατομική λήψη αποφάσεων του άρθρου 22 του ΓΚΠΔ.

- Η προστασία αυτών των πληροφοριών είναι ζωτικής σημασίας για: α) την προστασία των φυσικών προσώπων, β) την διασφάλιση της ακεραιότητας, της αξιοπιστίας και της ασφάλειας των ενεργειακών συστημάτων αλλά και γ) του asset που λέγεται πελατολόγιο (Google –Nest).

- Συνολικά, η προστασία των δεδομένων αποτελεί κρίσιμη πτυχή του ενεργειακού τομέα και οι εταιρείες πρέπει να εφαρμόζουν ολοκληρωμένα μέτρα για τη διαφύλαξη ευαίσθητων πληροφοριών, τη συμμόρφωση με τους κανονισμούς και την προστασία από απειλές κυβερνοασφάλειας.

Part of ICTLC

Βέλτιστες πρακτικές

TASSIS & ASSOCIATES LAW OFFICE

- ΓΕΝΙΚΕΣ ΑΡΧΕΣ
- Αξιολογήσεις κινδύνων
- Τμηματοποίηση του δικτύου
- Έλεγχοι πρόσβασης
- Σχέδια αντιμετώπισης περιστατικών
- Εκπαίδευση των εργαζομένων

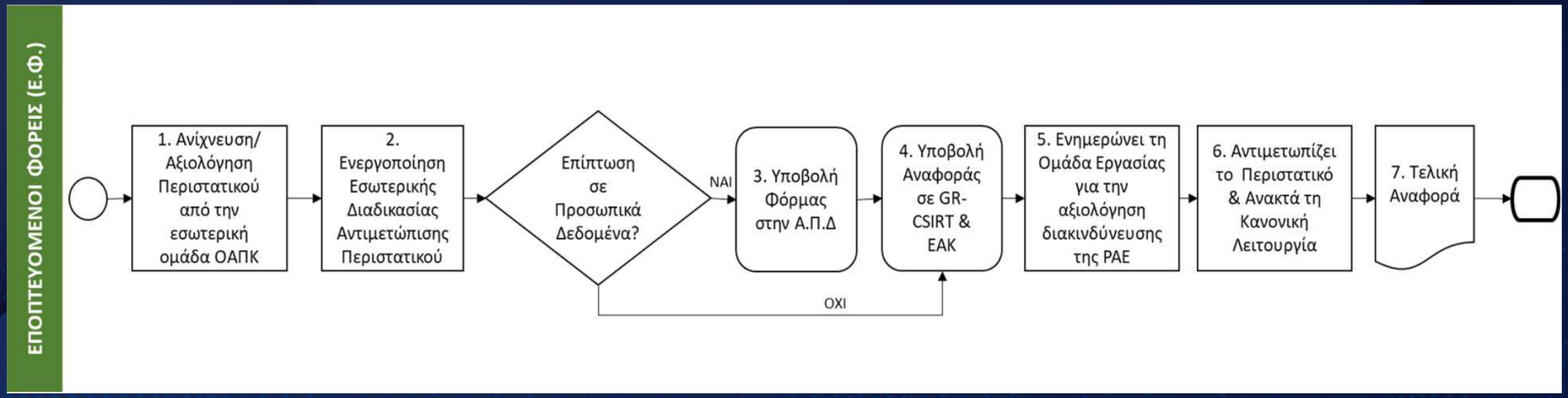
Part of ICTLC

Προστασία δικτύων και δεδομένων

TASSIS & ASSOCIATES LAW OFFICE

- ΡΑΕ (Κανονισμός (ΕΕ) 2019/941)

Σχέδιο Ετοιμότητας Αντιμετώπισης Κινδύνων στον τομέα του ηλεκτρισμού της Ελλάδας
Διαχείριση Κρίσης η.ε λόγω Κυβερνοεπιθέσεων - Ενέργειες Ε.Φ και ροή πληροφορίας



Part of ICTLC

Προστασία δικτύων και δεδομένων

TASSIS & ASSOCIATES LAW OFFICE

ΕΑΚ - Εγχειρίδιο Κυβερνοασφάλειας (2021)

1. Καταγραφή υλικού και λογισμικού
2. Ασφαλής διαμόρφωση εξοπλισμού και εφαρμογών
3. Περιορισμός χρήσης και εκτέλεσης προγραμμάτων και υπηρεσιών
4. Έλεγχος πρόσβασης
5. Αυθεντικοποίηση χρηστών
6. Ασφάλεια δικτύων
7. Προστασία από κακόβουλο λογισμικό
8. Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων (event logs)
9. Ασφάλεια διαδικτυακών εφαρμογών
10. Απομακρυσμένη εργασία
11. Χρήση κρυπτογραφίας
12. Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας
13. Διαχείριση κινδύνων στην εφοδιαστική αλυσίδα (supply chain risk management)
14. Υλοποίηση τεχνικών ελέγχων κυβερνοασφάλειας
15. Μέτρα φυσικής ασφάλειας εγκαταστάσεων
16. Λήψη αντιγράφων ασφαλείας (backup)
17. Αντιμετώπιση περιστατικών κυβερνοασφάλειας
18. Διασφάλιση επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή

Part of ICTLC

TASSIS & ASSOCIATES
LAW OFFICE

ΕΥΧΑΡΙΣΤΩ

info@tassis.com

Part of ICTLC