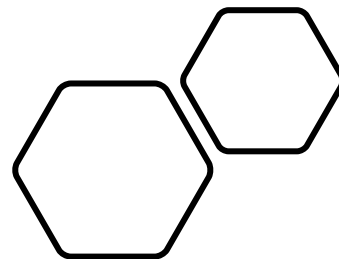



Γνωστές επιθέσεις σε πληροφοριακά συστήματα και η αντιμετώπισή τους βάσει της ελληνικής νομοθεσίας



Θα συζητήσουμε γνωστές επιθέσεις σε πληροφοριακά συστήματα, κρατικά και μη, τις επιπτώσεις τους σε θέματα εθνικής ασφάλειας και τις νομικές δυνατότητες αντιμετώπισής τους, με βάση το εθνικό νομοθετικό πλαίσιο.

The background features abstract black geometric shapes on a white background. There is a large black shape in the top left corner, a smaller black hexagon in the upper middle, and a large black shape in the bottom left corner that contains the text. The text is white and reads:

Θα ξεκινήσουμε αναλύοντας **3 επιθέσεις** που θεωρήσαμε ότι ταιριάζουν στο αντικείμενο που πραγματευόμαστε και στη συνέχεια θα περάσουμε στην **περιγραφή** του νομοθετικού πλαισίου και στα αντίστοιχα άρθρα.

1) Επίθεση στο ηλεκτρικό δίκτυο της Ουκρανίας - Γενική Περιγραφή

- Ομάδα Ρώσων hackers εξαπολύει επίθεση με στόχο το **ηλεκτρικό δίκτυο**, την **κυβέρνηση** και **συστήματα βιομηχανικού ελέγχου** και **τηλεμετρίας** της Ουκρανίας.
- Έγινε χρήση του λογισμικού **Black Energy 3** για εξαπάτηση χρηστών μέσω ηλεκτρονικού ταχυδρομείου, μέσω του οποίου παρακινούνταν οι χρήστες να ανοίξουν ένα κακόβουλο αρχείο Word, Excel ή PDF.
- Μέσω του Black Energy 3 εκτελούνται **επιθέσεις DoS** και **υποκλέπτονται** δεδομένα όπως τα **προσωπικά διαπιστευτήρια του χρήστη**.
- Τέλος, πραγματοποιείται λήψη αυτόματα του λογισμικού **KillDisk**, το οποίο χρησιμοποιείται για τον **τερματισμό υπηρεσιών** και την **καταστροφή σημαντικών αρχείων** του συστήματος.

1) Επίθεση στο ηλεκτρικό δίκτυο της Ουκρανίας - Επιπτώσεις

- Η επίθεση επηρέασε **3 εταιρείες παραγωγής ηλεκτρικού ρεύματος**, σε διαφορετικές περιοχές του κράτους, με αποτέλεσμα περίπου **225,000 πολίτες** να μην έχουν ηλεκτρικό ρεύμα. Ταυτόχρονα λόγω της επίθεσης DoS στα τηλεφωνικά κέντρα, κανείς δεν μπορούσε να ενημερωθεί.
- Η απόδοση ευθυνών σε ομάδα Ρώσων hackers, αποτελεί και αυτή με τη σειρά της έναν παράγοντα που προσδίδει στη βαρύτητα της συγκεκριμένης επίθεσης και θέτει σοβαρά ζητήματα εθνικής ασφάλειας. Για την κυβέρνηση της Ουκρανίας και οποιασδήποτε χώρας σε αντίστοιχη κατάσταση, μία τέτοια επίθεση συνεπάγεται **αβεβαιότητα των πολιτών και ανασφάλεια**, καθώς αποδεικνύεται ότι το κράτος **δεν ήταν σε θέση να προστατέψει** τα πληγέντα συστήματα και τα δεδομένα των αξιωματούχων της.

2) SolarWinds – Γενική Περιγραφή

- Αποτελεί μία **επίθεση αλυσίδας**: ένας επιτιθέμενος αποκτά πρόσβαση σε ένα σύστημα παραβιάζοντας κάποιο από τα υποσυστήματα του, εκμεταλλευόμενος μια αδυναμία που έχει το συγκεκριμένο υποσύστημα.
- Οι επιτιθέμενοι απέκτησαν πρόσβαση σε χιλιάδες μηχανήματα μέσω του λογισμικού **Orion της εταιρείας SolarWinds**, του οποίου τις ενημερώσεις μόλυναν με αποτέλεσμα, οι τροποποιημένες ενημερώσεις στη συνέχεια να διανέμονταν επί μήνες στους πελάτες της SolarWinds ως γνήσιες.
- Ο κακόβουλος κώδικας περιείχε αρκετές δικλίδες που του επέτρεπαν να **αποφεύγει την ανίχνευση**.
- Βασικές λειτουργίες του αποτελούν: η αποστολή στους επιτιθέμενους πληροφοριών σχετικών με την **τοπολογία του δικτύου** καθώς και δεδομένων όπως τις **πληροφορίες σχετικά με το μηχάνημα, αρχεία και μηνύματα ηλεκτρονικού ταχυδρομείου**.

2) SolarWinds – Επιπτώσεις

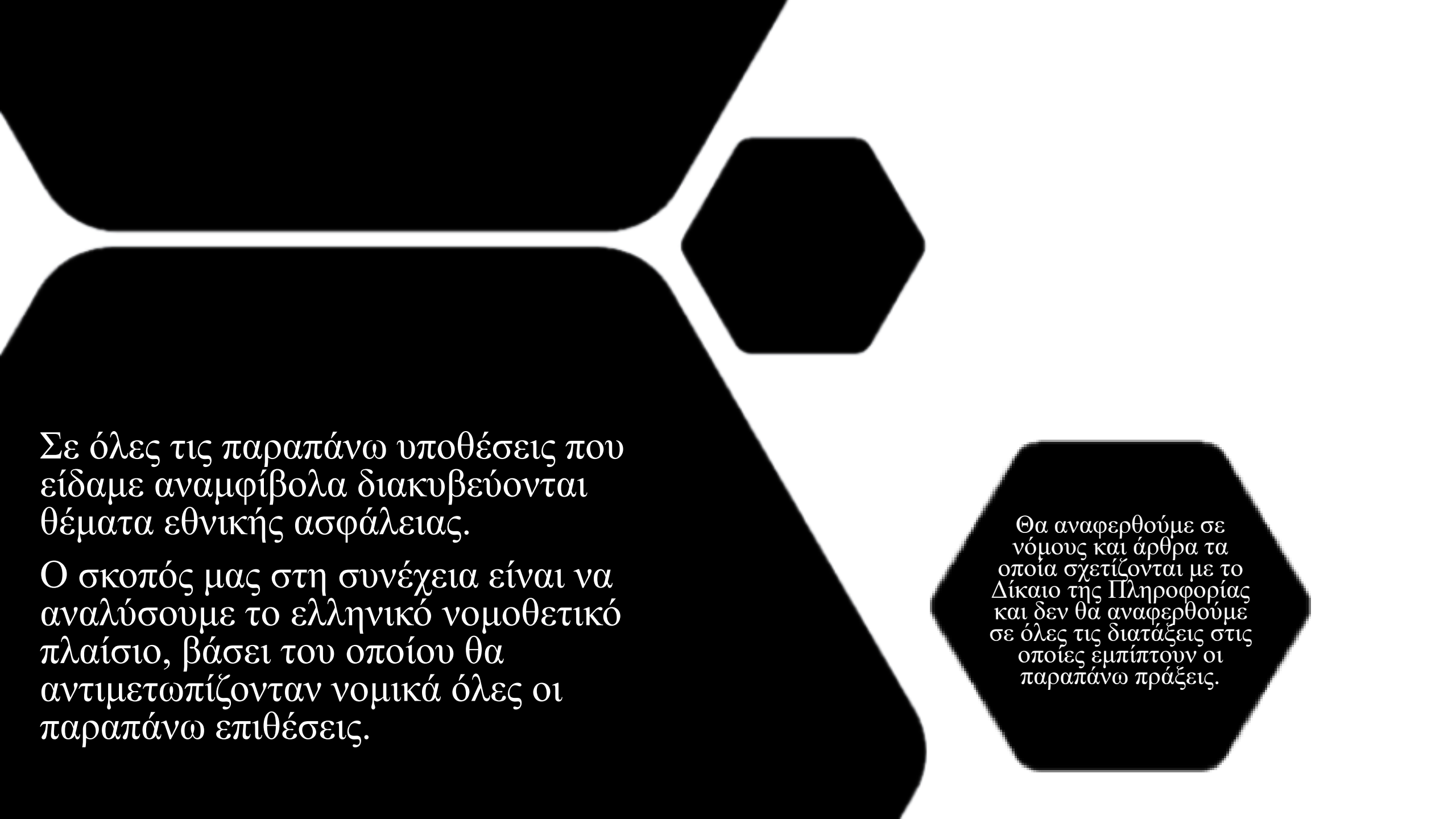
- Παρ' όλο που δεν είναι δυνατόν να προσδιοριστούν ακριβώς τα δεδομένα που έχουν διαρρεύσει, είναι δεδομένο ότι αποτελούν επίσημα **κρατικά στοιχεία**, όπως **απόρρητα έγγραφα** και **εμπορικές συμφωνίες** αλλά και **προσωπικά δεδομένα στελεχών της κυβέρνησης**.
- Η επίθεση ανακαλύφθηκε την περίοδο των Αμερικανικών Προεδρικών εκλογών, επομένως υπήρξε ο κίνδυνος, τα δεδομένα αυτά να χρησιμοποιηθούν με σκοπό της **άσκηση επιρροής στα αποτελέσματα**, αν και κάτι τέτοιο δεν φαίνεται να συνέβη.
- Τέλος, αρκετές ανησυχίες υπήρξαν σχετικά με τον ενδεχόμενο αντίκτυπο **στην οικονομία της χώρας** σε περίπτωση χρήσης των δεδομένων αυτών, ακόμη και για μία ενδεχόμενη **φυσική ζημιά σε κρίσιμες υποδομές** όπως στην περίπτωση της Ουκρανίας.

3) Athens Affair – Γενική Περιγραφή

- Αποτελεί το σκάνδαλο **τηλεφωνικών υποκλοπών** στην Ελλάδα που έλαβε χώρα τα έτη 2004-2005 και αφορά την «παγίδευση» τηλεφωνικών αριθμών και την **υποκλοπή συνομιλιών 100 πελατών** της εταιρείας κινητής τηλεφωνίας Vodafone Greece.
- Οι επιτιθέμενοι hackers μπήκαν στο τηλεφωνικό δίκτυο της Vodafone, υπονομεύοντας και χρησιμοποιώντας για δικούς τους σκοπούς, το ήδη υπάρχον **σύστημα «νόμιμης συνακρόασης»** - επιτρέπει να παγιδευτούν συγκεκριμένοι τηλεφωνικοί αριθμοί μέσω μίας νόμιμης διαδικασίας.
- Η ανάπτυξη του κακόβουλου λογισμικού, που εγκαταστάθηκε στον ηλεκτρονικό εξοπλισμό του δικτύου της εταιρείας, χαρακτηρίζεται από μεγάλη δυσκολία και πολυπλοκότητα. Η τεχνικά άρτια εκμετάλλευση των ιδιοτήτων του υπάρχον λογισμικού, επέτρεψε στους επιτιθέμενους να **δρουν απαρατήρητοι επί μήνες**.

3) Athens Affair – Επιπτώσεις

- Τα 100 πρόσωπα που είχαν γίνει στόχος αποτελούσαν μεταξύ άλλων **υψηλόβαθμα μέλη της κυβέρνησης, αξιωματούχοι του στρατού και του ναυτικού και όχι μόνο, διακινδυνεύοντας έτσι την διαρροή κρατικών πληροφοριών.**
- Για ακόμη μία φορά δεν είναι δυνατός ο πλήρης **προσδιορισμός των δεδομένων** που υποκλάπηκαν, ούτε και **ο σκοπός της παραβίασης.**
- Το γεγονός ότι τα άτομα ήταν συγκεκριμένα και κατείχαν **υψηλόβαθμα αξιώματα, δημιουργεί μεγάλες ανησυχίες για τους απώτερους σκοπούς των δραστών και τον αντίκτυπο, της διαρροής των προσωπικών πληροφοριών των συγκεκριμένων ατόμων, για την εθνική ασφάλεια.**



Σε όλες τις παραπάνω υποθέσεις που είδαμε αναμφίβολα διακυβεύονται θέματα εθνικής ασφάλειας.

Ο σκοπός μας στη συνέχεια είναι να αναλύσουμε το ελληνικό νομοθετικό πλαίσιο, βάσει του οποίου θα αντιμετωπίζονταν νομικά όλες οι παραπάνω επιθέσεις.

Θα αναφερθούμε σε νόμους και άρθρα τα οποία σχετίζονται με το Δίκαιο της Πληροφορίας και δεν θα αναφερθούμε σε όλες τις διατάξεις στις οποίες εμπίπτουν οι παραπάνω πράξεις.

Βάσει των άρθρων του Ποινικού Κώδικα

Άρθρο 292B - Παρακώλυση της λειτουργίας Πληροφοριακών Συστημάτων.

- ✓ Καλύπτονται επιθέσεις εις βάρος συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά.
- ✓ Καλύπτεται όποια περίπτωση σοβαρής παρεμπόδισης ή διακοπής χωρίς δικαίωμα συστήματος πληροφοριών. (με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά)

Άρθρο 293 - Παρακώλυση της λειτουργίας άλλων κοινωφελών εγκαταστάσεων.

- ✓ Καλύπτονται ειδικά επιθέσεις που οδήγησαν σε κατάσταση έκτακτης ανάγκης. (παρ. 3)

Άρθρο 292Γ

- ✓ Εμπίπτουν πράξεις διακίνησης, παραγωγής, κατοχής ειδικού λογισμικού και συσκευών που προορίζονται για την διάπραξη εγκλημάτων του 292B

Άρθρο 292Α - Εγκλήματα κατά της ασφάλειας τηλεφωνικών επικοινωνιών .

- ✓ Καλύπτονται ειδικά επιθέσεις σαν το Athens Affair, για την χωρίς δικαίωμα πρόσβαση σε σύστημα λογισμικού, που χρησιμοποιείται για την παροχή υπηρεσιών . (παρ. 3)

Βάσει των άρθρων του Ποινικού Κώδικα

Έπειτα από έγκληση η δίωξη μπορεί να γίνει και βάση των άρθρων:

Άρθρο 370B - Παράνομη πρόσβασης σε σύστημα πληροφοριών ή σε δεδομένα.

- ✓ Όταν αποκτάται πρόσβαση, «κατά παράβαση μέτρων προστασίας και χωρίς δικαίωμα» σε μέρος ή στο σύνολο συστήματος πληροφοριών και σε ηλεκτρονικά δεδομένα.

Άρθρο 370Δ

- ✓ Προστατεύεται το απόρρητο των πληροφοριακών συστημάτων και των δεδομένων αλλά χωρίς να έχει γίνει απαραίτητα ο χαρακτηρισμός τους ως απόρρητα, απ' τον νόμιμο κάτοχό τους (αρκεί ο αποκλεισμός τρίτων σε αυτά).

Άρθρο 370Γ

- ✓ Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών, τα οποία συνιστούν απόρρητα (κρατικά, επιχειρήσεων). Διαφυλάσσει οποιοδήποτε στοιχείο θεώρησε ο νόμιμος κάτοχός του ως εμπιστευτικό και έλαβε μέτρα προστασίας του από τρίτους.

Άρθρο 370Α - Παραβίαση απορρήτου τηλεφωνικής επικοινωνίας

- ✓ Καλύπτονται ειδικά επιθέσεις σαν το Athens Affair και το απόρρητο των τηλεφωνικών επικοινωνιών.

Βάσει της Οδηγίας NIS

Οδηγία 2016/1148/EE
& Νόμος 4577/2018

Άρθρο 11 – Ν.4577/2018

- ✓ Οι Εθνική Αρχή Κυβερνοασφάλειας, η αρμόδια CSIRT και οι άλλοι εμπλεκόμενοι φορείς, καθορίζουν απαιτήσεις ασφαλείας και απαιτούν απ' τους φορείς εκμετάλλευσης βασικών υπηρεσιών ή πάροχους ψηφιακών υπηρεσιών, να παρέχουν απαραίτητες πληροφορίες για την εκτίμηση της ασφάλειας των συστημάτων τους.
- ✓ Υπάρχουν διαδικασίες που πρέπει να ακολουθηθούν σε περίπτωση εντοπισμού μίας επικείμενης απειλής ή επίθεσης απ' τους φορείς υπηρεσιών.

Άρθρο 9 – υ.α. 1027/2019

- ✓ κάθε οργανισμός κοινοποιεί στο αρμόδιο CSIRT και την Εθνική Αρχή Κυβερνοασφάλειας χωρίς αδικαιολόγητη καθυστέρηση κάθε συμβάν που έχει αντίκτυπο στη συνεχή παροχή της υπηρεσίας που προσφέρει.

Άρθρο 11 – υ.α. 1027/2019

- ✓ υπάρχει και η πρόβλεψη για κοινοποίηση του συμβάντος στο κοινό, όταν αυτό κρίνεται απαραίτητο για να συμβάλλει στην καλύτερη αντιμετώπισή του.

Άρθρο 15 – Ν.4577/2018

- ✓ Κυρώσεις επιβάλλονται και για παραβιάσεις της διαδικασίας κοινοποίησης συμβάντων αλλά και για την παράλειψη των απαιτούμενων προληπτικών μέτρων απ' την πλευρά του φορέα.

Βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων & Νόμος 4624/2019

Όσον αφορά τον δράστη:

Άρθρο 38 – Ν.4624/2019

- ✓ Διώκεται όποιος χωρίς δικαίωμα επεμβαίνει σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα και προχωρά στην επεξεργασία αυτών, αντιγράφοντας, αφαιρώντας, αλλοιώνοντας, εάν τα μεταδίδει και γνωστοποιεί σε τρίτους.
- ✓ Σε ειδική περίπτωση εμπίπτουν δεδομένα με την παραβίαση των οποίων διακινδυνεύεται η «ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή η εθνική ασφάλεια»

Όσον αφορά τους φορείς και πιο συγκεκριμένα τους υπεύθυνους επεξεργασίας και εκτελούντες την επεξεργασία:

Άρθρο 32 – ΓΚΠΔ

- ✓ Οφείλουν να εφαρμόζουν τα κατάλληλα τεχνικά και οργανωτικά μέσα για την διασφάλιση ανάλογου επιπέδου ασφάλειας, έναντι κινδύνων.

Άρθρο 33 – ΓΚΠΔ

- ✓ Σε περίπτωση που ένα περιστατικό ενδέχεται να προκαλέσει κίνδυνο στα δικαιώματα και τις πληροφορίες των προσώπων στα οποία αφορά, οφείλουν να το γνωστοποιήσουν στην Αρχή Προστασίας Δεδομένων εντός 72 ωρών.

Άρθρο 34 – ΓΚΠΔ

- ✓ Προβλέπεται και η κοινοποίηση στα φυσικά πρόσωπα αν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες τους.

❖ Έχοντας κάνει λοιπόν, αυτή τη μελέτη, καταλήγουμε ότι με την υπάρχουσα νομοθεσία καλύπτονται επαρκώς τα παραπάνω εγκλήματα.

Λόγω όμως της φύσης των επιθέσεων που μελετήσαμε – εγκλήματα που υπονομεύουν την εθνική ασφάλεια μίας χώρας, αντιλαμβανόμαστε ότι ο εντοπισμός των δραστών είναι αρκετές φορές πολύ δύσκολος.

❖ Καταλήγουμε, λοιπόν, ότι η πιο αποτελεσματική αντιμετώπιση τέτοιων ζητημάτων είναι εφαρμόζοντας το νομοθετικό πλαίσιο των Οδηγιών της Ε.Ε. που δρα προληπτικά, υποχρεώνοντας τους φορείς να διατηρούν υψηλά επίπεδα ασφάλειας των συστημάτων τους.



Συμπεράσματα?