Στοιχεία Δικαίου της Πληροφορίας

Εαρινό Εξάμηνο 2020-2021

Δουραχαλής Φίλιππος, 3170045

Νικολάου Ελένη, 3170121

Γνωστές επιθέσεις σε πληροφοριακά συστήματα, που θίγουν θέματα εθνικής ασφάλειας και οι νομικές δυνατότητες αντιμετώπισής τους, με βάση το εθνικό νομοθετικό πλαίσιο.

Πίνακας Περιεχομένων

1. Εισαγωγή

Στη παρούσα εργασία θα παρουσιάσουμε ορισμένα **περιστατικά σημαντικών επιθέσεων** σε κράτη, οι οποίες έθεσαν σοβαρά ερωτήματα όσον αφορά την **ασφάλεια των κρατών** αυτών. Για κάθε περίπτωση θα αναφέρουμε τον **τρόπο** με τον οποίο πραγματοποιήθηκε η επίθεση, το **χρονικό πλαίσιο** στο οποίο εκτυλίχθηκε καθώς και τις υποδομές, τους οργανισμούς, τις κρατικές υπηρεσίες και ενδεχομένως τα πρόσωπα που **επηρέασε** σε μεγάλο βαθμό. Παράλληλα θα εξετάσουμε τις **επιπτώσεις** που είχε η επίθεση στην οικονομία, στις σχέσεις της χώρας με ξένα κράτη καθώς και στην εσωτερική οργάνωση της. Θεωρούμε ότι το συγκεκριμένο θέμα παρουσιάζει μεγάλο ενδιαφέρον, τόσο για τα κράτη, τα οποία πρέπει να εξασφαλίσουν την ασφάλεια των πληροφοριακών συστημάτων, σε κυβερνητικές υπηρεσίες και κρίσιμες υποδομές, όσο και για τους αναλυτές ασφαλείας που

εξετάζουν τις ευπάθειες των συστημάτων και πραγματοποιούν την αξιολόγηση των κινδύνων ώστε να καταγράψουν τους πιθανούς τρόπου αντιμετώπισης. Ιδιαίτερα τα τελευταία χρόνια, οι διαρκώς αυξανόμενες δυνατότητες του διαδικτύου έχουν φέρει στο προσκήνιο νέους τρόπους με τους οποίους μπορούν να διεξαχθούν οι κυβερνοεπιθέσεις (για παράδειγμα μέσω έξυπνων συσκευών) και έχουν προκαλέσει αύξηση στον ρυθμό εμφάνισής τους. Έχοντας λοιπόν αναλύσει όλα τα ανωτέρω θα μπορέσουμε να προσδιορίσουμε το **νόμους που εφαρμόζονται** σε κάθε διαφορετική περίπτωση επίθεσης βάσει του εθνικού νομοθετικού πλαισίου και να εξετάσουμε τις κυρώσεις που ορίζονται.

---

2. Σημαντικές Επιθέσεις

Η επίθεση στο ηλεκτρικό δίκτυο της Ουκρανίας

Περιγραφή

Το Δεκέμβριο του 2015, μια ομάδα Ρώσων χάκερ, γνωστή ως «*Sandworm*» ή «*Voodoo Bear*» εξαπέλυσε μια επίθεση που στόχευε το ηλεκτρικό δίκτυο, την κυβέρνηση και συστήματα βιομηχανικού ελέγχου και τηλεμετρίας (SCADA) της Ουκρανίας. Η επίθεση διεξήχθη χρησιμοποιώντας τα κακόβουλα λογισμικά *KillDisk*, σε συνδυασμό και *BlackEnergy 3*[1], το οποίο είναι η τρίτη έκδοση του δούρειου ίππου (Trojan) *BlackEnergy*[2], που ανακαλύφθηκε το 2007 και χρησιμοποιούταν κυρίως για επιθέσεις άρνησης υπηρεσιών (DoS). Το *BlackEnergy* 3 ενσωματώνει τεχνικές εξαπάτησης των χρηστών μέσω ηλεκτρονικού ταχυδρομείου (*Spear-Phising*[3]), παροτρύνοντάς τους να ανοίξουν ένα κακόβουλο αρχείο Word, Excel ή PDF. Όταν ο χρήστης ανοίξει το αρχείο που περιέχεται στο μήνυμα, το *BlackEnergy* 3 εγκαθίσταται στον υπολογιστή του χρήστη. Αυτό επιτρέπει στο κακόβουλο λογισμικό να εκτελέσει επιθέσεις DoS και επιπλέον να υποκλέπει προσωπικά δεδομένα και

---

[1] https://www.incibe-cert.es/en/blog/blackenergy-critical-systems (τελευταία πρόσβαση στις 07.05.2021)

[2] https://en.wikipedia.org/wiki/BlackEnergy (τελευταία πρόσβαση στις 06.05.2021)

[3] https://www.kaspersky.com/resource-center/definitions/spear-phishing (τελευταία πρόσβαση στις 06.05.2020)

σημαντικές πληροφορίες όπως τα διαπιστευτήρια του χρήστη, τα οποία και στέλνει στον επιτιθέμενο[4]. Μετά την επικοινωνία αυτή, πραγματοποιείται αυτόματα λήψη του λογισμικού *KillDisk*, το οποίο χρησιμοποιείται για τον τερματισμό υπηρεσιών και την καταστροφή σημαντικών αρχείων του συστήματος καθώς και την διαγραφή των αρχείων καταγραφής ώστε να καλυφθούν τα ίχνη της επίθεσης. Μέχρι στιγμής έχουν κατηγορηθεί έξι αξιωματικοί *Ρωσικής Υπηρεσίας Πληροφοριών* (GRU[5]) σύμφωνα με κατηγορητήριο που εξέδωσε παραπεμπτικό σώμα ενόρκων στις Η.Π.Α. Οι κατηγορούμενοι είναι ο Yuriy Sergeyevich Andrienko, ο Sergey Vladimirovich Detistov, ο Pavel Valeryevich Frolov, ο Anatoliy Sergeyevich Kovalev, ο Artem Valeryevich Ochichenko και ο Petr Nikolayevich Pliskin, οι οποίοι φαίνεται να έχουν παίξει κρίσιμο ρόλο και σε πολυάριθμες άλλες επιθέσεις, μεταξύ των οποίων και η γνωστή *NotPetya*[6].

Υποδομές που επηρεάστηκαν

Όπως αναφέρθηκε, η επίθεση είχε ως στόχο τις κρίσιμες υποδομές, και πιο συγκεκριμένα το ηλεκτρικό δίκτυο της Ουκρανίας, επηρεάζοντας τουλάχιστον 3 από τις εταιρίες παραγωγής ηλεκτρικού ρεύματος, σε διαφορετικές περιοχές του κράτους. Το λογισμικό *BlackEnergy* επέτρεψε στους επιτιθέμενους να ανιχνεύσουν τα δίκτυα των εταιριών και να εντοπίσουν τους σταθμούς εργασίας των χειριστών. Έτσι μπορούσαν να ελέγξουν το δίκτυο μέσω των διακοπτών των κυκλωμάτων όπως κάθε νόμιμος χειριστής. Υπολογίζεται ότι κατά τη διάρκεια της επίθεσης 225.000 πολίτες δεν είχαν ηλεκτρικό ρεύμα, ενώ η ταυτόχρονη επίθεση άρνησης υπηρεσιών στα τηλεφωνικά κέντρα των εταιριών τους απέτρεψε από το να λάβουν περισσότερες πληροφορίες και βοήθεια σχετικά με το συμβάν.

[4] https://marcusedmondson.com/2019/01/18/black-energy-analysis/ (τελευταία πρόσβαση στις 06.05.2021)

[5] https://en.wikipedia.org/wiki/GRU_(Russian_Federation) (τελευταία πρόσβαση στις 09.5.2020)

[6] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (τελευταία πρόσβαση στις 09.05.2020)

Επιπτώσεις στο κράτος και στην εθνική ασφάλεια

Η επίθεση αυτή, μεταξύ άλλων παρόμοιων επιθέσεων, θεωρείται από τους αναλυτές ως μια προσπάθεια αποσταθεροποίησης της Ουκρανίας, προκειμένου να ενισχυθεί η οικονομική της εξάρτηση από την Ρωσία[7]. Η εξάρτηση αυτή παρότι υφίσταται ακόμα και σήμερα, έχει αποδυναμωθεί εξαιτίας των ισχυρών εμπορικών σχέσεων της Ουκρανίας με την Ευρωπαϊκή Ένωση, καθώς οι εμπορικές συναλλαγές με την Ε.Ε. αντιστοιχούν, σύμφωνα με επίσημα στοιχεία, στο 40% του εμπορίου της Ουκρανίας με ξένα κράτη[8]. Η κατανόηση των σχέσεων εξάρτησης μεταξύ της Ουκρανίας και της Ρωσίας, αν και σημαντική για να γίνει πλήρως αντιληπτός ο αντίκτυπος της συγκεκριμένης επίθεσης, δεν θα αναλυθεί περαιτέρω διότι ξεφεύγει από τους σκοπούς αυτής της εργασίας. Επιπροσθέτως, μια κυβερνοεπίθεση τέτοιας έκτασης δύναται να κλονίσει την εμπιστοσύνη προς την κυβέρνηση, καθώς εκείνη δεν κατέχει τους απαραίτητους πόρους, εργαλεία και χρόνο για να αντεπιτεθεί. Με αυτόν τον τρόπο αποδεικνύεται παράλληλα η αδυναμία της Ουκρανίας να αντιμετωπίσει τις επιθέσεις αυτές, γεγονός που θέτει σοβαρά ζητήματα εθνικής ασφάλειας, καθώς είναι φανερό πως το κράτος δεν ήταν σε θέση να προστατέψει τα πληγέντα συστήματα και τα δεδομένα των μελών της κυβέρνησης.

Η επίθεση στις κρατικές υποδομές των Η.Π.Α.

Περιγραφή

Η επόμενη επίθεση στην οποία θα αναφερθούμε αφορά ένα από τα πιο σημαντικά περιστατικά ασφαλείας που καταγράφηκαν στις Η.Π.Α[9]. την τελευταία δεκαετία. Πρόκειται για μια *επίθεση αλυσίδας (Supply Chain Attack*) μεγάλης κλίμακας που διεξήχθη μέσω του λογισμικού που διακινεί η εταιρία *SolarWinds*. Η *SolarWinds* είναι μια εταιρία πληροφορικής με έδρα το Austin της πολιτείας του Texas, η οποία παράγει λογισμικό για την διαχείριση δικτύων και πληροφοριακών συστημάτων. Το πιο γνωστό από τα προϊόντα της είναι το λογισμικό «*Orion*», που χρησιμοποιείται

[7] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ (τελευταία πρόσβαση 06.05.2021)

[8] https://ec.europa.eu/trade/policy/countries-and-regions/countries/ukraine/ (τελευταία πρόσβαση 07.05.2021)

[9] https://www.bbc.com/news/technology-55321643 (τελευταία πρόσβαση 06.05.2021)

από πληθώρα εταιριών σε όλο το κόσμο, αλλά και από την ίδια την κυβέρνηση των Ηνωμένων Πολιτειών. Η επίθεση ξεκίνησε περίπου τον Μάρτιο του 2020. ωστόσο δεν έγινε αντιληπτή μέχρι 13 Δεκεμβρίου του ίδιου έτους. Σε μια επίθεση αλυσίδας, κάποιος αποκτά πρόσβαση σε ένα σύστημα παραβιάζοντας κάποιο από τα υποσυστήματα του, εκμεταλλευόμενος μια αδυναμία που έχει το συγκεκριμένο υποσύστημα. Με παρόμοιο τρόπο σε αυτή την υπόθεση, οι επιτιθέμενοι απέκτησαν πρόσβαση σε χιλιάδες μηχανήματα μέσω του λογισμικού *Orion*, μολύνοντας τις ενημερώσεις του λογισμικού χρησιμοποιώντας μια ευπάθεια (vulnerability) που οι ειδικοί ασφαλείας ονόμασαν «*SUNBURST*» και εισάγοντας σε αυτές κακόβουλο κώδικα υπό τη μορφή βιβλιοθηκών (αρχεία dll). Οι τροποποιημένες ενημερώσεις στη συνέχεια διανέμονταν επί μήνες στους πελάτες της *SolarWinds* ως γνήσιες, καθώς έφεραν ένα πλαστό πιστοποιητικό, με αποτέλεσμα να είναι σχεδόν αδύνατος ο εντοπισμός τους από συστήματα *IDS (Intrusion Detection Systems)* και λογισμικό αντιμετώπισης ιών (Antivirus). Ωστόσο η επιτυχία της επίθεσης συνίσταται επίσης στο γεγονός πως οι το λογισμικό ανίχνευε διαρκώς το σύστημα του χρήστη στο οποίο είχε εγκατασταθεί προκειμένου να ελέγξει αν παράλληλα με εκείνο ήταν ενεργές ορισμένες υπηρεσίες του συστήματος (System processes) που είναι υπεύθυνες για τον εντοπισμό και την αντιμετώπιση απειλών ή κάποιο πρόγραμμα παρακολούθησης δικτύων, όπως το *Wireshark*. Εάν ανίχνευε κάποια από αυτές τις υπηρεσίες ή προγράμματα, ο κακόβουλος κώδικας τερματιζόταν αυτόματα, αφήνοντας τα υπόλοιπα στοιχεία του συστήματος αναλλοίωτα, συμπεριλαμβανομένου και του λογισμικού *Orion* στο οποίο περιεχόταν. Σε κάθε άλλη περίπτωση, κατά τη διάρκεια εκτέλεσης του προγράμματος, ο κώδικας που είχε εισαχθεί παράνομα, έστελνε στους επιτιθέμενους πληροφορίες σχετικές με την τοπολογία του δικτύου στο οποίο βρισκόταν το μηχάνημα καθώς και δεδομένα όπως τις πληροφορίες σχετικά με το μηχάνημα, αρχεία και μηνύματα ηλεκτρονικού ταχυδρομείου που μπορεί να στέλνει ο χρήστης.

Υποδομές που επηρεάστηκαν

Η επίθεση *SUNBURST* επηρέασε σύμφωνα με επίσημες έρευνες χιλιάδες οργανισμούς και εταιρίες των Η.Π.Α, 400 από τις οποίες ανήκουν στη λίστα *FORTUNE* και οι οποίες είχαν εγκατεστημένο στις υποδομές τους λογισμικό της

SolarWinds. Ωστόσο ο λόγος που το περιστατικό αυτό αναφέρεται ως το πιο σοβαρό ζήτημα κυβερνοασφάλειας των τελευταίων χρόνων είναι επειδή εκτός από ιδιωτικές επιχειρήσεις, οι παράγοντες πίσω από την επίθεση απέκτησαν πρόσβαση σε κρατικές υπηρεσίες και υπουργεία της κυβέρνησης. Μεταξύ αυτών ήταν το *Στέιτ Ντιπάρτμεντ* (Υπουργείο Εξωτερικών), το Υπουργείο Άμυνας, το Υπουργείο Οικονομικών, η Εθνική Αρχή Τηλεπικοινωνιών και Πληροφορίας (*National Telecommunications and Information Administration*) και ακόμα 9 Υπουργεία[10].

Επιπτώσεις στην εθνική ασφάλεια

Το περιστατικό της *SolarWinds* δεν αποτελεί μια τυπική περίπτωση κυβερνοεπίθεσης, από την άποψη ότι ο χαρακτήρας της ήταν κυρίως παθητικός σε αντίθεση με την επίθεση που περιεγράφηκε προηγουμένως. Το γεγονός ότι οι παράγοντες πίσω από αυτήν δεν ζήτησαν κάποιο χρηματικό ποσό, κι ούτε προξένησαν ανεπανόρθωτες βλάβες στα μηχανήματα που προσέβαλε το κακόβουλο λογισμικό, αλλά και η ασυνήθιστα μακρά διάρκεια της επίθεσης αποδεικνύει σύμφωνα με αναλυτές ασφαλείας που εξέτασαν το περιστατικό πως πρόκειται περί κατασκοπείας. Διαφορετικές πηγές αναφέρουν ότι οι επιτιθέμενοι ενεργούσαν προς όφελος της Ρωσίας ή της Κίνας, χωρίς κάτι τέτοιο να έχει εξακριβωθεί. Παρότι είναι αδύνατο να προσδιοριστούν ακριβώς τα δεδομένα που διέρρευσαν κατά τη διάρκεια της επίθεσης, πράγμα που δυσχεραίνει τις έρευνες των ειδικών, γίνεται εύκολα αντιληπτός ο κίνδυνος που εγείρεται όταν επίσημα στοιχεία του κράτους, όπως απόρρητα έγγραφα και εμπορικές συμφωνίες αλλά και προσωπικά δεδομένα στελεχών της κυβέρνησης υποκλέπτονται από αντίπαλα κράτη. Το γεγονός πως οι Η.Π.Α. δεν είχαν δεχθεί ξανά στο παρελθόν μια επίθεση τέτοιας έκτασης προξένησε πολλές ανησυχίες[11] ως προς την αποτελεσματικότητα των υφιστάμενων μέτρων ασφαλείας στις κυβερνητικές υποδομές και το κατά πόσο ήταν δυνατή η πλήρης αντιμετώπιση του φαινομένου, δεδομένου πως το λογισμικό της *SolarWinds* βρισκόταν ήδη σε πολλούς και διαφορετικούς οργανισμούς και σε πολλές περιπτώσεις εκείνο ήταν κρίσιμο στοιχείο

[10] https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach#List_of_confirmed_connected_breaches (τελευταία πρόσβαση στις 08.05.2021)

[11] https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive-idUSKBN28N0PG (τελευταία πρόσβαση 09.05.2021)

της λειτουργίας τους, επομένως η απεγκατάστασή του δεν αποτελούσε επιλογή. Σε συνδυασμό με όλα τα ανωτέρω προέκυψε επίσης το ζήτημα σχετικά με τις επιπτώσεις της επίθεσης στον πραγματικό κόσμο, δηλαδή κατά πόσο το κράτος που υπέκλεψε πληροφορίες ζωτικής σημασίας θα μπορούσε να τις αξιοποιήσει για να προξενήσει ζημιά στην οικονομία των Η.Π.Α. ή ακόμα και φυσική ζημιά στις κρίσιμες υποδομές, σε μια επίθεση αντίστοιχη με αυτή που περιεγράφηκε προηγουμένως. Εν κατακλείδι, η επίθεση στη *SolarWinds* που έπληξε χιλιάδες ιδιωτικά και κρατικά πληροφοριακά συστήματα, δημιούργησε πολλές αμφιβολίες [12]σχετικά με την φύση των πληροφοριών που διέρρευσαν, τους παράγοντες που έλαβαν τις πληροφορίες αυτές και τους τρόπους που θα μπορούσαν να τις χρησιμοποιήσουν στο μέλλον για να πλήξουν περεταίρω το κράτος των Ηνωμένων Πολιτειών.

Athens Affair

Το σκάνδαλο τηλεφωνικών υποκλοπών στην Ελλάδα έλαβε χώρα τα έτη 2004-2005[13], ενώ αποκαλύφθηκε στο ευρύ κοινό τον επόμενο χρόνο. Το έγκλημα αφορά την «παγίδευση» τηλεφωνικών αριθμών και την υποκλοπή συνομιλιών 100 πελατών της εταιρείας κινητής τηλεφωνίας *Vodafone Greece*. Παρ' όλο που η παράνομη και ενίοτε, υπό προϋποθέσεις, σύννομη πράξη της υποκλοπής τηλεφωνικών συνομιλιών πραγματοποιείτο χρόνια και με αναλογικά μέσα, με τα σύγχρονα δεδομένα και την ψηφιοποίηση των τηλεπικοινωνιών, χρίζει πλέον ιδιαίτερου ενδιαφέροντος για τους επαγγελματίες της πληροφορικής, πόσο μάλλον εκείνους που ασχολούνται με την ασφάλεια πληροφοριακών συστημάτων. Παράλληλα, για τον ίδιο λόγο, τα ισχύοντα νομοθετικά πλαίσια και τα νομικά μέσα αντιμετώπισής τέτοιου είδους επιθέσεων θεωρούμε ότι μπορούν να θεωρηθούν αντικείμενο του Δικαίου της Πληροφορίας.

[12] https://statescoop.com/no-evidence-solarwinds-hack-touched-election-systems/ (τελευταία πρόσβαση στις 09.05.2021)

[13] https://en.wikipedia.org/wiki/Greek_wiretapping_case_2004%E2%80%9305 (τελευταία πρόσβαση στις 27.04.2021)

Περιγραφή

Με απλά λόγια[14], η επίθεση μπορεί να συνοψιστεί στα εξής: οι επιτιθέμενοι hackers μπήκαν στο τηλεφωνικό δίκτυο της Vodafone, υπονομεύοντας και χρησιμοποιώντας για δικούς τους σκοπούς, το ήδη υπάρχον σύστημα «νόμιμης συνακρόασης» - *Lawful Interception*. Το λογισμικό αυτό που εγκαταστάθηκε παράνομα στους μεταγωγείς (switches) της Vodafone, δημιουργούσε παράλληλες ροές της ψηφιακής συνομιλίας. Ενώ υπήρχε η κανονική γραμμή που συνέδεε τους δύο συνομιλητές, δημιουργούταν ακόμη μία, πανομοιότυπη, που κατευθυνόταν σε τηλέφωνα τρίτων, δίνοντάς τους τη δυνατότητα να ακούν αλλά και να καταγράφουν.

Το κακόβουλο λογισμικό τοποθετήθηκε στο μέρος του συστήματος που ονομάζεται *mobile switching center – switch*. Αποτελεί το κέντρο στο οποίο φτάνουν οι κλήσεις των συνδρομητών και ανακατευθύνονται στους παραλήπτες. Η Vodafone Greece χρησιμοποιούσε συσκευές switch της εταιρείας *Ericsson*. Τα συγκεκριμένα switches επιτρέπουν «νόμιμες συνακροάσεις» δηλαδή το να παγιδευτούν συγκεκριμένοι τηλεφωνικοί αριθμοί μέσω μίας νόμιμης διαδικασίας η οποία περιλαμβάνει την επίδειξη εντάλματος και απόφασης δικαστηρίου ή εισαγγελέα στην εταιρεία τηλεπικοινωνιών. Τα *Ericsson AXE switches*, υλοποιούν τη συγκεκριμένη λειτουργία μέσω ενός ειδικού λογισμικού το οποίο αντιγράφει τη συνομιλία σε μία δεύτερη γραμμή στην άκρη της οποίας βρίσκεται η Διωκτική Αρχή. Το λογισμικό αυτό ονομάζεται *RES – Remote-Control Equipment Subsystem* ενώ η κατασκευάστρια εταιρεία παρείχε και ένα σύστημα διαχείρισης του RES, μία διεπαφή αλλιώς, το *IMS – Interception Management System* – μέσω του οποίου δημιουργούνται και διαχειρίζονται οι συνομιλίες που παρακολουθούνται. Όταν αυτά τα δύο συστήματα είναι εγκατεστημένα, συνεργάζονται και πρέπει να συμφωνούν, δηλαδή μία γραμμή παρακολούθησης που είναι ανοικτή στο *RES*, χωρίς να έχει γίνει αντίστοιχο αίτημα στο *IMS* αποτελεί ένδειξη ότι κάτι έχει γίνει λάθος, ενώ για να εντοπιστεί αρκεί ένας τυπικός έλεγχος.

Στην περίπτωση όμως της Vodafone Greece, ενώ το σύστημα νόμιμης συνακρόασης δεν είχε αγοραστεί, έπειτα από μία αναβάθμιση, στις αρχές του 2003, έγινε εγκατάσταση του λογισμικού *RES* από την Ericsson, με αποτέλεσμα, τα switch να

[14] *Vassilis Prevelakis, Diomidis Spinellis (2007),* "The Athens Affair, how some extremely smart hackers pulled off the most audacious cell-network break-in ever", *IEEE Spectrum*. Available from: https://spectrum.ieee.org/telecom/security/the-athens-affair (τελευταία πρόσβαση στις 28.04.2021)

περιείχαν το λογισμικό που υποστήριζε την ύπαρξη γραμμών παρακολούθησης αλλά όχι την διεπαφή *IMS* που διαχειρίζεται τα αιτήματα και επιτρέπει τέτοιου είδους νόμιμες υποκλοπές. Οι hackers εκμεταλλευόμενοι και επιπρόσθετες ιδιαιτερότητες τον συστημάτων της Ericsson, εγκατέστησαν ένα αρκετά πολύπλοκο λογισμικό και σε συνδυασμό με την απουσία της διεπαφής που θα τους έκανε ορατούς, κατάφεραν να περνούν απαρατήρητοι από τους διαχειριστές συστήματος (system administrators) της Vodafone αλλά και της Ericsson.[15]

Στις 24 Ιανουαρίου του 2005, οι δράστες πραγματοποίησαν ένα update στο κακόβουλο λογισμικό, που επηρέασε την προώθηση γραπτών μηνυμάτων (SMS) - τα οποία έπαψαν να παραδίδονται – γεγονός, που με τη σειρά του, πυροδότησε μία αυτόματη αναφορά σφάλματος. Έπειτα από έρευνα που έγινε από την εταιρεία Ericsson και την ανακάλυψη του κακόβουλου λογισμικού, οι υπεύθυνοι ήταν σε θέση να εντοπίσουν τη χρονική στιγμή της εγκατάστασής του και ως αποτέλεσμα την χρονική διάρκεια της επίθεσης. Επιπλέον, είχαν στα χέρια τους τη λίστα με τους τηλεφωνικούς αριθμούς που είχαν παγιδευτεί.

Επιπτώσεις στην Εθνική Ασφάλεια

Τι είναι όμως αυτό που κάνει τη συγκεκριμένη υπόθεση τόσο ξεχωριστή από άλλες επιθέσεις και της προσδίδει τόση σημασία? Αρχικά, αποτελεί μία υψίστης σημασίας επίθεση καθώς φαίνεται να θίγει θέματα εθνικής ασφαλείας. Τα πρόσωπα που είχαν γίνει στόχος από τους επιτιθέμενους ήταν συγκεκριμένα και αποτελούσαν κυρίως υψηλόβαθμα μέλη της κυβέρνησης αλλά και του ελληνικού στρατού, διακινδυνεύοντας έτσι την διαρροή κρατικών πληροφοριών και μυστικών που πιθανόν να περιείχαν αυτές οι κλήσεις. Τα άτομα, των οποίων οι τηλεφωνικοί αριθμοί βρέθηκαν στη λίστα των παγιδευμένων, αποτελούσαν ο τότε Έλληνας Πρωθυπουργός και τα μέλη της οικογένειάς του, η δήμαρχος Αθηναίων, τα περισσότερα ανώτερα στελέχη του Υπουργείου Εθνικής Άμυνας, του Υπουργείου Εξωτερικών, του Υπουργείου Δημοσίας Τάξης, μέλη του κυβερνώντος κόμματος, της αξιωματικής

[15] Να σημειωθεί ότι στα περισσότερα δίκτυα τηλεπικοινωνιών εφαρμόζεται κρυπτογράφηση, από τα κινητά έως τους σταθμούς. Στο εσωτερικό όμως του δικτύου του παρόχου (στον πυρήνα του συστήματος, στον οποίο βρίσκονταν τα switch που υπονόμευσαν οι επιτιθέμενοι), δεν υπήρχε κρυπτογράφηση, γιατί θα καθίστατο δύσκολη και η διενέργεια νόμιμης παρακολούθησης.

αντιπολίτευσης, το Γενικό Επιτελείο του Πολεμικού Ναυτικού και ο πρώην υπουργός Εθνικής Άμυνας. Σε αυτή την περίπτωση, και σε αντίθεση με προηγούμενες, είναι η φύση των δεδομένων που κατά τη γνώμη μας την κάνουν να ξεχωρίζει. Δεν πρόκειται για κλοπή μόνο απόρρητων κρατικών πληροφοριών, αλλά προσωπικών συζητήσεων υψηλόβαθμων στελεχών, που δύναται να περιέχουν, εκτός από απόρρητες κρατικές πληροφορίες, και προσωπικά ευαίσθητα δεδομένα. Όπως και να έχει η συγκεκριμένη υποκλοπή με την έκταση που έλαβε αποτελεί ιδιαίτερη περίπτωση που όμοιά της δεν έχει αποκαλυφθεί.

Δυστυχώς, πλέον, είναι αρκετά δύσκολο να εντοπιστούν οι δράστες, διότι, στοιχεία κλειδιά στην υπόθεση χάθηκαν, καταστράφηκαν ή δεν συλλέχθηκαν ποτέ. Όταν τα στελέχη της Vodafone πληροφορήθηκαν για το κακόβουλο λογισμικό ο τότε Διευθύνων Σύμβουλος της εταιρείας έδωσε εντολή να διαγραφεί από τα συστήματα, δίνοντας έτσι ένα ξεκάθαρο μήνυμα στους δράστες ότι έχουν αποκαλυφθεί και ότι πρέπει να εξαφανίσουν κάθε ίχνος της δράσης τους. Η εταιρεία, λοιπόν, παρέλειψε να ακολουθήσει τις υπάρχουσες διαδικασίες, όπως το να γνωστοποιήσει στις ανεξάρτητες αρχές την επίθεση σε συγκεκριμένο χρονικό διάστημα. Αντ΄ αυτού αποδεικτικά στοιχεία καταστράφηκαν. Οι αρχές απ’ την πλευρά τους, όταν ειδοποιήθηκαν, αρκέστηκαν σε στοιχεία που η ίδια η εταιρεία τους παρείχε και σε ανακρίσεις υπαλλήλων της.

---

3. Νομοθετικό Πλαίσιο

Θα εξετάσουμε την παραπάνω επίθεση και όλες τις επιθέσεις που αναφέραμε στα πλαίσια του κοινού δικαίου και δεν θα αναλύσουμε ενδεχόμενα ανάμειξης άλλων κρατών, κατασκοπείας και άμυνας, θέματα του επονομαζόμενου δικαίου του πολέμου.

Ας θεωρήσουμε το παράδειγμα της πρώτης επίθεσης, στις υποδομές παροχής ενέργειας της Ουκρανίας. Αρχικά, μέσω της συγκεκριμένης επίθεσης, οι δράστες παρακωλύουν την ομαλή λειτουργία πληροφοριακών συστημάτων και ειδικότερα συστημάτων «που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες». Κάθε πράξη, λοιπόν, αυτής της μορφής, υπάγεται στις διατάξεις του άρθρου **292Β του Ποινικού Κώδικα** (Νόμος 4619/2019)

περί **Παρακώλυσης της λειτουργίας Πληροφοριακών Συστημάτων** αλλά και του άρθρου **293 του Ποινικού Κώδικα** (Νόμος 4619/2019) περί **Παρακώλυσης της λειτουργίας άλλων κοινωφελών εγκαταστάσεων**. Σύμφωνα με το άρθρο 292Β του ποινικού κώδικα «ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια» και όπως είδαμε τα πληροφοριακά συστήματα που επηρεάστηκαν ανήκουν επί τω πλείστων, αν όχι εξ' ολοκλήρου, στην τελευταία κατηγορία. Πιο αναλυτικά, οι συγκεκριμένες παραβάσεις αντιστοιχούν στην περίπτωση (γ) της δεύτερης (2) παραγράφου του άρθρου 292Β, για επίθεση κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά και υπηρεσίες όπου η ποινή είναι αυξημένη σε σύγκριση με τις προηγούμενες περιπτώσεις, με φυλάκιση τουλάχιστον τριών (3) ετών και χρηματική ποινή. Επιπλέον, αν, βάσει της τρίτης (3) παραγράφου του άρθρου 293, μιλάμε για την περίπτωση που η τέλεση μίας αντίστοιχης πράξης προκαλέσει κατάσταση «κοινής ανάγκης» η ποινή φυλάκισης ενδέχεται να αυξηθεί έως και 10 έτη. Ακόμη και αν η επίθεση δεν στοχεύει τέτοιου είδους υποδομές αλλά ωστόσο, στις περιπτώσεις άλλων θυμάτων, βλάπτει σε μεγάλο βαθμό (σε έκταση και χρονικά) τις παρεχόμενες υπηρεσίες του πληροφοριακού συστήματος, προξενώντας μεγάλη οικονομική ζημία και σημαντική καταστροφή δεδομένων, ο νόμος (περίπτωση (β) της παρ.2, του αρ.292Β ΠΚ) προβλέπει κι εκεί ποινή φυλάκισης τουλάχιστον 2 ετών και χρηματική ποινή.

Οι επιτιθέμενοι δύναται να διωχθούν και λόγω της παραγωγής, πώλησης, προμήθειας προς χρήση, κατοχής, εισαγωγής και γενικά διακίνησης συσκευών ή λογισμικού σχεδιασμένου ή προσαρμοσμένου για την παράνομη πρόσβαση σε πληροφοριακά συστήματα και παρακώλυση της λειτουργίας τους. Παράλληλα διώκονται και για την διακίνηση, κατοχή κ.α. δεδομένων που δύναται να συμβάλλουν στην απόκτηση πρόσβασης σε τέτοια συστήματα. Οι παραπάνω πράξεις εμπίπτουν στο άρθρο **292Γ του ΠΚ** περί **Προπαρασκευαστικών Ενεργειών Παρακώλυσης Λειτουργίας Πληροφοριακών Συστημάτων**.

Στην περίπτωση της τελευταίας επίθεσης, του Athens Affair, θα μπορούσαμε να πούμε ότι ποινικές διώξεις θα μπορούσαν να γίνουν βάσει του άρθρου **292Α** του Ποινικού Κώδικα περί Εγκλημάτων κατά της ασφάλειας τηλεφωνικών επικοινωνιών.

Στα άρθρα των προηγούμενων περιπτώσεων οι διώξεις γίνονται αυτεπαγγέλτως, ενώ στη συνέχεια θα δούμε και διατάξεις άρθρων κατά τις οποίες οι διώξεις γίνονται έπειτα από έγκληση.

Μία επίθεση σε πληροφοριακό σύστημα μπορεί να διωχθεί και σύμφωνα με το άρθρο **370Β του Ποινικού Κώδικα** (Νόμος 4619/2019) περί **παράνομης πρόσβασης σε σύστημα πληροφοριών ή σε δεδομένα**, το άρθρο **370Γ** και το άρθρο **370Δ** του Ποινικού Κώδικα (Νόμος 4619/2019). Για παράδειγμα, καλύπτεται η επίθεση της *SolarWinds* κατά την οποία οι επιτιθέμενοι δεν παρακώλυσαν σημαντικά την λειτουργία των πληροφοριακών συστημάτων αλλά ωστόσο είχαν παράνομη πρόσβαση σε αυτά. Πιο συγκεκριμένα η πράξη στην οποία αναφερόμαστε αντιστοιχεί στην παράγραφο 1 του 370Β καθώς αποκτάται πρόσβαση, «κατά **παράβαση μέτρων προστασίας και χωρίς δικαίωμα**» σε μέρος ή στο σύνολο συστήματος πληροφοριών και σε ηλεκτρονικά δεδομένα. Επίσης βάσει του άρθρου 370Γ, προστατεύονται τα διάφορα **απόρρητα** στοιχεία ή προγράμματα Η/Υ, τα οποία συνιστούν κρατικά, επιστημονικά, επαγγελματικά ή απόρρητα επιχειρήσεων του δημοσίου ή ιδιωτικού τομέα και ποινικοποιείται η κατά οποιονδήποτε τρόπο παραβίαση τους. Παρ' όλο που σε κάποιες περιπτώσεις δεν έχει αποδειχθεί – και ενδεχομένως να μην γίνεται να αποδειχθεί, ότι είχαμε αντιγραφή, χρησιμοποίηση ή αποκάλυψη σε τρίτους έχουμε ωστόσο ξεκάθαρη παραβίαση των δεδομένων και το συγκεκριμένο άρθρο διαφυλάσσει οποιοδήποτε στοιχείο θεώρησε ο νόμιμος κάτοχός του ως **εμπιστευτικό** και **έλαβε μέτρα προστασίας** του από τρίτους. Τέλος, στο άρθρο 370Δ προστατεύεται για ακόμη μία φορά το απόρρητο των πληροφοριακών συστημάτων και των δεδομένων αλλά αυτή τη φορά με την τυπική του έννοια, δηλαδή, προστατεύεται το δικαίωμα του νόμιμου κατόχου να **αποκλείει την πρόσβαση** τρίτων σε αυτά χωρίς να γίνει ο ειδικός χαρακτηρισμός τους όπως στο άρθρο 370Γ ως απόρρητα[16]. Η πρόσβαση σε τέτοια συστήματα και δεδομένα λοιπόν, βάσει και αυτών των άρθρων διώκεται έπειτα από έγκληση του φορέα, και τιμωρείται τουλάχιστον με 1 και έως 3 έτη φυλάκισης και χρηματική ποινή.

[16] *Ιωάννης Θ. Δαλακούρας* (2020), Η προστασία των απορρήτων, κατά τα άρθρα 370Β –370Ε Ποινικού Κώδικα. Ουσιαστική και Δικονομική προσέγγιση, Διπλωματική Εργασία, Θεσσαλονίκη: Πανεπιστήμιο Μακεδονίας, Δημοκρίτειο Πανεπιστήμιο Θράκης. Διαθέσιμο: https://dspace.lib.uom.gr/bitstream/2159/24455/1/DalakourasIoannisMsc2020.pdf (τελευταία πρόσβαση 08.05.2021)

Για ακόμη μία φορά, η τελευταία περίπτωση επίθεσης της υποκλοπής των τηλεφωνικών συνομιλιών, εμπίπτει στην παραβίαση απορρήτου τηλεφωνικής επικοινωνίας και στο αντίστοιχο άρθρο **370Α του Ποινικού Κώδικα περί** Παραβίασης απορρήτου τηλεφωνικής επικοινωνίας**,** όπως και στο άρθρο **370Ε** για την παρακολούθηση και αποτύπωση μη δημόσιων διαβιβάσεων δεδομένων**.**

Οδηγία NIS – Ευθύνες των φορέων.

Παρ' όλο που στις περιπτώσεις επιθέσεων που αναφέραμε δεν υπάρχουν σαφή δεδομένα για μη τήρηση υποχρεώσεών, απ' την πλευρά των φορέων, αξίζει να αναφερθούμε στα πλαίσια που ορίζει η ισχύουσα νομοθεσία και τους κανονισμούς που επιβάλλει. Με την ενσωμάτωση της υπ' αριθμόν 2016/1148/ΕΕ Οδηγίας του Ευρωπαϊκού Κοινοβουλίου, γνωστής και ως NIS – *Network and Information Systems,* στην ελληνική νομοθεσία με τον νόμο 4577/2018, θέτονται βασικές **απαιτήσεις ασφάλειας** των συστημάτων δικτύων και δεδομένων, προσδιορίζεται η **διαδικασία κοινοποίησης συμβάντων** και παροχής πληροφοριών στις αρμόδιες Αρχές, όπως και η μεθοδολογία αξιολόγησης και **ελέγχου των μέτρων** Ασφαλείας που λαμβάνονται απ' τους εκάστοτε φορείς[17]. Όλα τα παραπάνω έχουν ως στόχο την επίτευξης ενός ενιαίου υψηλού επιπέδου ασφάλειας συστημάτων δικτύων και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση.

Βάσει του άρθρου 11 και 12 του νόμου **4577/2018 περί Απαιτήσεων ασφάλειας και κοινοποίησης συμβάντων,** η Εθνική Αρχή Κυβερνοασφάλειας[18]. σε συνεργασία με την αρμόδια CSIRT[19] και τους άλλους εμπλεκόμενους φορείς, καθορίζουν, όπως προαναφέραμε απαιτήσεις ασφάλειας (αρ.11), απαιτούν απ' τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών καθώς και Πάροχοι Ψηφιακών Υπηρεσιών - οι

[17] βλ. Εθνική Στρατηγική Κυβερνοαφάλειας 2020 – 2025 (https://mindigital.gr/wp-content/uploads/2020/12/ΕΘΝΙΚΗ-ΣΤΡΑΤΗΓΙΚΗ-ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ-2020-2025.pdf)

[18] βάσει του αρ.7 του ν. 4577/2018 ως **Εθνική Αρχή Κυβερνοασφάλειας** έχει οριστεί η Γενική Διεύθυνση Κυβερνοασφάλειας που υπάγεται στη Γενική Γραμματεία Τηλεπικοινωνιών & Ταχυδρομείων του υπουργείου Ψηφιακής Διακυβέρνησης.

[19] Βάσει του αρ. 8, ν.4577/2019. **Αρμόδια Ομάδα Απόκρισης** για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team - CSIRT εφεξής «αρμόδια CSIRT») και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας, είναι η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ.

υποδομές των οποίων θεωρούνται κρίσιμες[20],να παρέχουν απαραίτητες πληροφορίες για την εκτίμηση της ασφάλειας των συστημάτων τους και οφείλουν να αξιολογούν και να επιβάλλουν σε περιπτώσεις που αποδεικνύεται ότι οι φορείς δεν συμμορφώνονται εποπτικά μέτρα[21]. Με όλα τα παραπάνω επιτυγχάνεται ο συνεχής έλεγχος και η διατήρηση υψηλού επιπέδου ασφάλειας στα συστήματα αυτά. Παράλληλα, η νομοθεσία προβλέπει και διαδικασίες που πρέπει να ακολουθηθούν σε περίπτωση εντοπισμού μίας επικείμενης απειλής ή επίθεσης. Οι παραπάνω αρμόδιοι φορείς οφείλουν να καθορίσουν μία διαδικασία κοινοποίησης των συμβάντων (τα μέσα επικοινωνίας και η λεπτομερής διαδικασία περιγράφονται στην Εθνική Στρατηγική Κυβερνοαφάλειας). Σύμφωνα με το άρθρο 9 της **υπ. αποφ. υπ. αρ. 1027/2019** - Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α΄ 199), 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. Αυτό έχει την υποχρέωση να το κάνει χωρίς αδικαιολόγητη καθυστέρηση και εντός 24 ωρών απ' τη στιγμή που ενημερώνεται για το συμβάν. Επιπλέον αν το συμβάν κρίνεται ως «σοβαρή διατάραξη[22]» ο οργανισμός είναι υποχρεωμένος να υποβάλλει μία αρχική αναφορά χωρίς αδικαιολόγητες καθυστερήσεις. Και στις δύο προηγούμενες περιπτώσεις, οι αναφορές θα πρέπει να περιέχουν όποιες πληροφορίες για το περιστατικό θα διευκολύνουν τις αρμόδιες αρχές να εκτιμήσουν τον αντίκτυπο, όπως και δίνεται η δυνατότητα σε περίπτωση που τα στοιχεία μεταβληθούν να υποβληθεί νέα επικαιροποιημένη αναφορά. Στη νομοθεσία υπάρχει και η πρόβλεψη για κοινοποίηση του συμβάντος στο κοινό, όταν αυτό κρίνεται απαραίτητο για να συμβάλλει στην καλύτερη αντιμετώπισή του (παρ.

[20] Με την ενσωμάτωση της υπ' αρ. 2016/1148/ΕΕ Οδηγίας του Ευρωπαϊκού Κοινοβουλίου, γνωστής και ως NIS – Network and Information Systems, στον νόμο 4577/2018 ορίζονται οι **φορείς εκμετάλλευσης βασικών υπηρεσιών** ως δημόσιες ή ιδιωτικές οντότητες που δραστηριοποιούνται στους τομείς της ενέργειας, των μεταφορών, των τραπεζών, των χρηματοπιστωτικών αγορών, της υγείας, του νερού και των ψηφιακών υποδομών. Περαιτέρω κριτήρια για τον προσδιορισμό ορίζονται στην υπ. Αποφ. Υπ. Αρ. 1027. Ως **πάροχοι ψηφιακών υπηρεσιών** ορίζονται νομικά πρόσωπα που παρέχουν ψηφιακές υπηρεσίες, όπως αυτές ορίζονται στο αρ. 3 του ν.4577/2018.

[21] βάσει του αρ. 1, παρ. 2, του ν. 4577/2018 οι απαιτήσεις ασφάλειας και κοινοποίησης που προβλέπονται **δεν εφαρμόζονται** σε επιχειρήσεις που παρέχουν δημόσια δίκτυα ή δημόσιες υπηρεσίες ηλεκτρονικών επικοινωνιών και έχουν ειδικά ή αποκλειστικά δικαιώματα παροχής υπηρεσιών σε άλλες αγορές πλην των αγορών δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (παρ. 1 του άρθρου 33 του ν. 4070/2012 (Α΄ 82)) ή σε παρόχους υπηρεσιών εμπιστοσύνης (εμπίπτουν στο άρθρο 19 του Κανονισμού (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 (ΕΕ L 257).

[22] όπως ορίζεται στο άρθρο 7 και 8 της υ.α. υπ. αρ. 1027/2019 - Θέματα εφαρμογής και διαδικασιών του ν. 4577/ 2018 (Α΄ 199))

5, αρ. 11, ν. 4577/2018 και αρ. 11, υπ. αποφ. υπ. αρ. 1027/2019). Σε περίπτωση τώρα που διαπιστωθεί ότι ο φορέας εκμετάλλευσης βασικών υπηρεσιών ή φορέας παροχής ψηφιακών υπηρεσιών δεν κοινοποιεί ή κοινοποιεί με αδικαιολόγητη καθυστέρηση συμβάν, που όπως αναφέραμε και προηγουμένως, έχει σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών του, του επιβάλλονται κυρώσεις βάσει του άρθρου 15 του ν. 4577/2018, από τον Υπουργό Ψηφιακής διακυβέρνησης ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας. Οι κυρώσεις αυτές αποτελούν πρόστιμο έως και 15,000 ευρώ με σύσταση για συμμόρφωση και προειδοποίηση για επιβολή περαιτέρω κυρώσεων, ενώ σε περίπτωση υποτροπής το πρόστιμο αυξάνεται στα 200,000 ευρώ. Αν κατά τη διάρκεια των ερευνών, φυσικό ή νομικό πρόσωπο διαπιστωθεί ότι δεν παρέχει ή παρέχει με αδικαιολόγητη καθυστέρηση πληροφορίες σχετικές με το συμβάν, του αναλογεί πρόστιμο έως 50,000 ευρώ και σύσταση για συμμόρφωση ενώ σε περίπτωση υποτροπής το πρόστιμο δύναται να αυξηθεί και έως 200,000 ευρώ. Τέλος, κυρώσεις προβλέπονται και σε περίπτωση που ο φορέας υπηρεσιών δεν λαμβάνει «κατάλληλα και αναλογικά τεχνικά και οργανωτικά, προληπτικά μέτρα» σχετικά με την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων που χρησιμοποιεί, τα οποία πρόστιμα ταυτίζονται με την προηγούμενη περίπτωση.

Είδαμε λοιπόν, πώς με το παρόν νομοθετικό πλαίσιο της χώρας, συγκεκριμένοι φορείς, όπως πάροχοι ενέργειας (ηλεκτρική ενέργεια, πετρέλαιο και αέριο), νερού, μεταφορών (αεροπορικών, σιδηροδρομικών, πλωτών και οδικών), υγείας, τράπεζες, κ.α. που εμπλέκονται και στα παραδείγματα επιθέσεων, είναι υποχρεωμένοι να τηρούν συγκεκριμένα standards ως προς την ασφάλεια των συστημάτων τους αλλά και να ακολουθούν σαφώς ορισμένες διαδικασίες για την αποτελεσματικότερη αντιμετώπιση τέτοιων συμβάντων.

Προσωπικά Δεδομένα

Μέχρι στιγμής έχουμε αναφερθεί στο νομοθετικό πλαίσιο και τα άρθρα στα οποία εμπίπτουν τα εγκλήματα που περιγράψαμε, εξετάζοντάς τα επί τω πλείστων ως προς την υπονόμευση της ασφάλειας πληροφοριακών συστημάτων, της παράνομης εισόδου σε αυτά και της παρακώλυσης της λειτουργίας τους. Είδαμε την ποινική αντιμετώπιση παραβίασης απορρήτου των δεδομένων, αλλά δεν έχουμε εξετάσει την

επίδραση μίας επικείμενης επίθεσης σε δεδομένα προσωπικού χαρακτήρα. Η προστασία τέτοιων δεδομένων ρυθμίζεται από τον **Γενικό Κανονισμό Προστασίας Δεδομένων** (GDPR) και τον **νόμο 4624/2019** που ενσωματώνει και εξειδικεύει την προηγούμενη οδηγία στην ελληνική νομοθεσία.

Ο δράστης που χωρίς δικαίωμα επεμβαίνει σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα και προχωρά στην επεξεργασία αυτών, αντιγράφοντας, αφαιρώντας, αλλοιώνοντας κ.α. (παρ.1, αρ. 38, ν.4624/2019) του επιβάλλεται φυλάκιση έως 1 έτους, ενώ εάν μεταδίδει και γνωστοποιεί σε τρίτους τα ίδια δεδομένα (παρ.2 του ίδιου άρθρου) τιμωρείται επίσης με φυλάκιση. Ιδιαίτερα αν αυτά τα δεδομένα εμπίπτουν σε ειδικές κατηγορίες ή που αφορούν ποινικές καταδίκες και αδικήματα (παρ.3 του ίδιου άρθρου) η ποινή αυξάνεται σε φυλάκιση τουλάχιστον 1 έτους και χρηματική ποινή 100,000 ευρώ. Πιο σχετικά με τις δικές μας περιπτώσεις, στην παράγραφο 5 του ίδιου άρθρου, προβλέπεται στην περίπτωση που μέσω της παραβίασης των δεδομένων, προκλήθηκε κίνδυνος για την «ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια», κάθειρξη και χρηματική ποινή, στον δράστη, έως τριακόσιες χιλιάδες (300.000) ευρώ.

Όταν σε μία επίθεση διακυβεύεται η ασφάλεια προσωπικών δεδομένων, όπως έγινε σε όλες τις περιπτώσεις των επιθέσεων που αναφέραμε, τότε υπάρχουν υποχρεώσεις απ' την πλευρά των φορέων η μη τήρηση των οποίων επιφυλάσσει κυρώσεις. Ο υπεύθυνος επεξεργασίας[23] και ο εκτελών την επεξεργασία[24] αναλαμβάνουν, μεταξύ άλλων, να εφαρμόσουν τα κατάλληλα τεχνικά και οργανωτικά μέσα για την διασφάλιση ανάλογου επιπέδου ασφάλειας έναντι κινδύνων (αρ. 32 του Γενικού Κανονισμού Προστασίας Δεδομένων), όπως και υποχρεούνται να κοινοποιούν συμβάντα στα οποία παραβιάζονται προσωπικά δεδομένα. Συγκεκριμένα ως προς την κοινοποίηση, βάσει του άρθρου 33, του Γενικού Κανονισμού Προστασίας Δεδομένων, ο υπεύθυνος επεξεργασίας δεδομένων, σε περίπτωση που από το

[23] **Υπεύθυνος επεξεργασίας**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

[24] **Εκτελών την επεξεργασία**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

περιστατικό ενδέχεται να προκαλέσει κίνδυνο στα δικαιώματα και τις πληροφορίες των προσώπων στα οποία αφορά, οφείλει να γνωστοποιήσει το περιστατικό στην Αρχή Προστασίας Δεδομένων[25]. Η γνωστοποίηση αυτή, οφείλει να γίνει «αμελλητί» εντός 72 ωρών από τη στιγμή που ο υπεύθυνος επεξεργασίας ενημερώνεται για το συμβάν. Προβλέπεται επίσης, ότι ο εκτελών την επεξεργασία έχει κι εκείνος υποχρέωση να ενημερώσει, άμεσα μόλις αντιληφθεί την παραβίαση, τον υπεύθυνο επεξεργασίας έτσι ώστε να προβεί εκείνος στα παραπάνω βήματα. Η γνωστοποίηση, παρ' όλο που είναι υποχρεωτικό να περιέχει κάποιες βασικές πληροφορίες, αν εκείνες δεν είναι δυνατόν να συλλεχθούν μέχρι και την λήξη της προθεσμίας (72 ώρες), δύναται να παρέχονται σταδιακά, έπειτα από αυτή, χωρίς καθυστερήσεις. Ακόμη σύμφωνα με το άρθρο 34 του ίδιου κανονισμού, αν η παραβίαση ενδέχεται να θέσει σε **υψηλό κίνδυνο** τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, τότε ο υπεύθυνος επεξεργασίας «οφείλει να ανακοινώνει αμελλητί την παραβίαση και στα πρόσωπα αυτά». Τα παραπάνω εμπίπτουν και στα άρθρα 63, 64 του νόμου 4624/2019. Περαιτέρω, όταν παραβιάζονται οι παραπάνω υποχρεώσεις του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία (αρ. 33 και 34 του ΓΚΠΔ) επιβάλλονται διοικητικά πρόστιμα έως 10,000,000 ευρώ και σε περίπτωση επιχειρήσεων έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους. Τέλος, όπως έχει οριστεί από την ελληνική νομοθεσία σύμφωνα με το άρθρο 82, ν. 4624/2019, οι κυρώσεις, που επιβάλλονται σε **δημόσιες αρχές** με χρέη υπευθύνων επεξεργασίας όταν γίνεται παραβίαση των ίδιων άρθρων, είναι διοικητικό πρόστιμο έως και 1,000,000 ευρώ.

4. Τελικά συμπεράσματα/Επίλογος

Κλείνοντας την ανάλυση μας επί του θέματος που παρουσιάστηκε, είναι σημαντικό να εστιάσουμε στα εξής σημεία. Αρχικά παρατηρούμε πως το ισχύον νομοθετικό πλαίσιο της χώρας είναι ικανό να καλύψει όλες τις ανωτέρω περιπτώσεις κυβερνοεγκλημάτων που είδαμε και τα άρθρα του ποινικού κώδικα που αναφέρθηκαν είναι διατυπωμένα με τρόπο τέτοιο ώστε να λαμβάνουν υπόψιν κάθε δυνατή μορφή μιας επίθεσης σε κάποιο πληροφοριακό σύστημα. Παρ' όλα αυτά, σε τέτοιου είδους

[25] https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis, (τελευταία πρόσβαση 09.05.2021)

επιθέσεις η διαδικασία απόδοσης ευθυνών παρουσιάζει δυσκολίες, διότι συχνά είναι αδύνατη η ανεύρεση των δραστών. Για τους λόγους αυτούς καταλήγουμε στο συμπέρασμα πως είναι σωστή η τάση που υπάρχει να επιβάλλονται υψηλά πρόστιμα στους φορείς τηλεπικοινωνιών που δεν τηρούν τις αυστηρές απαιτήσεις ασφαλείας, καθώς η τήρηση αυτή είναι ουσιώδης, όπως προαναφέραμε, για την προστασία της ασφάλειας ενός κράτους.

---

5. Παράρτημα: Συνοπτικός πίνακας ισχύουσας νομοθεσίας ανά επίθεση.

Επίθεση	**Άρθρα που εφαρμόζονται**
Επίθεση στο Ηλεκτρικό Δίκτυο της Ουκρανίας	αρ. 292Β ΠΚ (Νόμος 4619/2019)
	αρ. 293 ΠΚ (Νόμος 4619/2019)
	αρ. 292Γ ΠΚ
	αρ. 370Β ΠΚ
	αρ. 370Γ ΠΚ
	αρ. 370Δ ΠΚ
Η επίθεση στις κρατικές υποδομές των Η.Π.Α.	αρ. 292Γ ΠΚ
	αρ. 370Β ΠΚ
	αρ. 370Γ ΠΚ
	αρ. 370Δ ΠΚ
	αρ. 38 Ν. 4624/2019
Athens Affair	αρ. 292Α ΠΚ
	αρ. 292Γ ΠΚ
	αρ. 370Α ΠΚ
	αρ. 370Β ΠΚ
	αρ. 370Δ ΠΚ
	αρ. 370Ε ΠΚ
	αρ. 38 Ν. 4624/2019
	αρ. 33 Γ.Κ.Π.Δ.

Περίληψη

Στην εργασία παρουσιάζονται τρεις γνωστές περιπτώσεις επιθέσεων που έγιναν εις βάρος κρατικών πληροφοριακών συστημάτων και κρίσιμων υποδομών: η επίθεση στο ηλεκτρικό δίκτυο της Ουκρανίας, η επίθεση στη SolarWinds και το Athens Affair, που περιγράφει την επίθεση στο τηλεφωνικό δίκτυο της εταιρίας τηλεπικοινωνιών Vodafone. Σε μια εποχή όπου η ψηφιοποίηση των δεδομένων και ο αυτοματισμός των διαδικασιών βρίσκεται σε κάθε φάσμα της ζωής των πολιτών και αποτελεί απαραίτητο στοιχείο για την λειτουργία των περισσότερων χωρών, η προστασία των δεδομένων και των συστημάτων που τα φιλοξενούν αποτελεί ένα σημαντικό και καίριο ζήτημα για την ασφάλεια και την ευημερία των κρατών. Για το λόγο αυτό, μέσω της ανάλυσης των επιθέσεων αυτών, ευελπιστούμε ότι θα γίνει κατανοητό το μέγεθος και η κρισιμότητα που είχε καθεμιά από αυτές, καθώς και οι πιθανές συνέπειες για την εθνική ασφάλεια των χωρών τις οποίες έπληξαν. Επιπλέον θα στηριχθούμε στο ισχύον νομοθετικό πλαίσιο της χώρας ώστε να παρουσιάσουμε τους νόμους που ισχύουν για τα κυβερνοεγκλήματα που αναφέρουμε καθώς και τις κυρώσεις που δύνανται να υποστούν τα πρόσωπα πίσω από αυτά.