ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΜΗΜΑ ΝΟΜΙΚΗΣ
ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΥΠΟΛΟΓΙΣΤΙΚΗ ΝΕΦΟΥΣ ΚΑΙ ΑΠΟΡΡΗΤΟ(370Β,370Γ)

Διπλωματική Εργασία
Της
Κανάτα Μαριάνθης

Θεσσαλονίκη 2019

ΥΠΟΛΟΓΙΣΤΙΚΗ ΝΕΦΟΥΣ ΚΑΙ ΑΠΟΡΡΗΤΟ(370Β,370Γ)

Κανάτα Μαριάνθη

Πτυχίο Νομικής , ΑΠΘ , 2017

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές
Ψάννης Κωνσταντίνος
Δαλακούρας Θεοχάρης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ηη/μμ/εεεε

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
.....	.....	.....

ΠΡΟΛΟΓΟΣ

Το Υπολογιστικό Νέφος εμφανίζεται στη βιβλιογραφία με πληθώρα ορισμών χωρίς κάποιος να έχει καθιερωθεί και να είναι κοινά αποδεκτός. Το cloud computing δεν είναι ένας μικρός, μη αναπτυχθείς κλάδος της τεχνολογίας των πληροφοριών.

Μεγάλα ονόματα εταιρειών πληροφόρησης που ξέρουμε όπως η Amazon, η Google και η Microsoft παλεύουν για μια θέση στο «σύννεφο». Με το «σύννεφο» μπορούμε να κάνουμε πολλά ή ακόμη μπορούμε να κάνουμε τα πάντα. Από το να τρέχουμε εφαρμογές για να αποθηκεύουμε δεδομένα εκτός εταιρείας μέχρι να τρέχουμε ολόκληρα λειτουργικά συστήματα στο «σύννεφο».

Τα προϊόντα τα οποία παρέχονται μέσω υποδομών σαν Υπηρεσία μπορεί να είναι υπολογιστικές μηχανές, εξυπηρετητές, αποθηκευτικά μέσα και γενικά μία πλήρης υπολογιστική υποδομή. Στην περίπτωση της πλατφόρμας σαν Υπηρεσία, παρέχεται ότι χρειάζεται μια εφαρμογή για να εκτελεστεί, δηλαδή το υλικό, το λειτουργικό σύστημα, η βάση δεδομένων, οι εξυπηρετητές και το λογισμικό.

Η ασφάλεια έχει τόσο βάρος στο σύννεφο όσο και οπουδήποτε αλλού. Ο κόσμος θέλει να μάθει για το cloud computing από διαφορετικές σκοπιές. Μερικοί θεωρούν το «σύννεφο» ένα ανασφαλές μέρος. Δηλαδή μόλις σταλούν τα δεδομένα στο «σύννεφο» χάνεται ο πλήρης έλεγχος επάνω τους και υπάρχει μεγαλύτερος κίνδυνος διάρρηξης. Αλλά η άλλη πλευρά αυτού του νομίσματος είναι ότι οι προμηθευτές «σύννεφου» κάνουν πάρα πολλά για να εξασφαλίσουν την ασφάλεια. Πολλοί προμηθευτές «σύννεφου» αφιερώνουν ομάδες στην ασφάλεια ώστε να εξασφαλίσουν ότι τα σύννεφά τους είναι ασφαλή. Αυτό έχει έννοια διότι το μόνο που χρειάζεται είναι να συμβεί μια παραβίαση για να εξαφανιστούν οι πελάτες.

Όλες οι επιχειρήσεις μεγάλες ή μικρές που προσφέρουν υπηρεσίες «σύννεφου», προσπαθούν να προσφέρουν καινοτόμες λύσεις αιχμής που είναι ελκυστικές αρκετά για να σκεφτούμε να μετακινηθούμε προς το «σύννεφο». Στα πλαίσια μιας γενικότερης θεώρησης ασφάλεια θεωρείται η επιτυχής εξουδετέρωση απειλών όπως κλοπή, απάτη, κατασκοπεία, εκβιασμός, τρομοκρατία.

Με βάση το κίνητρο της επίθεσης που μπορεί να είναι απλή επιθυμία απόκτησης πρόσβασης σε απαγορευμένους πόρους, μέχρι την ανορθόδοξη επίτευξη πολιτικών και οικονομικών στόχων, διακρίνονται διάφορες κατηγορίες εισβολέων όπως Hackers, κατάσκοποι, επαγγελματίες εγκληματίες, βάνδαλοι, τρομοκράτες, βιομηχανικοί κατάσκοποι.

Ανεξάρτητα από την κατηγοριοποίηση των επιτιθέμενων σε ένα σύστημα κύριο πρόβλημα, που πρέπει να αντιμετωπισθεί, είναι ο έγκαιρος

προσδιορισμός των τρωτών και η βελτίωση της ασφάλειας των συστημάτων πριν από τους επιτιθέμενους.
Το διαδίκτυο προσφέρει ένα νέο μαγικό κόσμο που τείνει να κυριαρχήσει στη ζωή μας καθ'ότι το διαδίκτυο είναι ο σύγχρονος τρόπος επικοινωνίας, ανταλλαγής ιδεών και απόψεων, συνομιλίας, ενημέρωσης, συλλογής και επεξεργασίας πληροφοριών, ψυχαγωγίας και συνάμα η νέα ανοικτή ηλεκτρονική αγορά προϊόντων και υπηρεσιών.
Μέσα στο ραγδαία εξελισσόμενο τεχνολογικό γίγνεσθαι, στο πλαίσιο του Διαδικτύου, τίθεται το ερώτημα εάν είναι δυνατή η επέμβαση του νομοθέτη και σε ποιο στάδιο αλλά και πως πρέπει να ενεργεί.
Παράλληλα όμως με την ανάπτυξη των τεχνολογικών μέσων αναπτύσσονται και νέες μορφές εγκληματικότητας οι οποίες επωφελούνται από τη σύγχρονη τεχνολογία, προκειμένου να προκαλέσουν βλάβες ή να αλλοιώσουν τα ίδια τα συστήματα. Η εγκληματικότητα αυτή λαμβάνει διάφορες μορφές όπως επιθέσεις κατά συστημάτων πληροφοριών, διάδοση παιδικής πορνογραφίας, παραβιάσεις πνευματικής ιδιοκτησίας, προσβολές της ιδιωτικότητας, απάτες μέσω διαδικτύου, διακίνηση πειρατείας λογισμικού, διακίνηση ναρκωτικών ουσιών και όπλων, υφαρπαγή προσωπικών δεδομένων, σωματεμπορία. Ο χαρακτήρας της σημερινής κοινωνίας της πληροφορίας είναι ιδιαίτερα ευάλωτος. Η οικονομία, η διοίκηση και η κοινωνία είναι σε πολύ μεγάλο βαθμό εξαρτημένες από την αποτελεσματικότητα και την ασφάλεια των πληροφοριακών συστημάτων.
Μπροστά στα παραπάνω δεδομένα τόσο η διεθνής και Ευρωπαϊκή νομοθεσία, όσο και ο Έλληνας νομοθέτης στα πλαίσια των επιταγών του ενωσιακού δικαίου, προσπαθούν να προσαρμοστούν στα νέα δεδομένα εισάγοντας νέες μορφές αξιόποινων συμπεριφορών, προκειμένου να μπορέσουν να σταθούν στο ύψος των περιστάσεων και στις επιταγές της σύγχρονης κοινωνίας για να αντιμετωπίσουν τις νέες πρωτόγνωρες εγκληματικές συμπεριφορές. Το ηλεκτρονικό έγκλημα διαφέρει και υπερέχει από το κοινό έγκλημα κυρίως σε ταχύτητα, προσβασιμότητα και ευκολία.
Η ηλεκτρονική εγκληματικότητα η οποία ενέσκηψε τα τελευταία χρόνια, παράλληλα με την εξέλιξη της τεχνολογίας, προκαλεί νέα προβλήματα στην επιστήμη του ποινικού δικαίου. Τα προβλήματα αυτά αντιμετωπίστηκαν, έως έναν βαθμό με την εισαγωγή ειδικής νομοθεσίας στο Ελληνικό Ποινικό δίκαιο και πιο συγκεκριμένα, με το Ν.1805/1988, ο οποίος προσέθεσε τέσσερα εμβόλιμα άρθρα στον ΠΚ(εδ β' στο άρθρο 13 περ. γ' και 386Α) ως και τα άρθρα 370Β και 370Γ που παρατίθενται και αναλύονται στην παρούσα εργασία. Με τις διατάξεις αυτές και κυρίως με τη διάταξη του άρθρου 370Γ παρ 2 του Ποινικού Κώδικα η οποία έχει χαρακτηρισθεί ως «ο πυρήνας του Ελληνικού ποινικού δικαίου πληροφορικής» επιχειρείται να αντιμετωπισθούν ορισμένες

μορφές εγκληματικότητας που συνδέονται με την πληροφορική και τους η/υ, οι οποίες είναι καινοφανείς.
Με τις διατάξεις του Ν 4619/11 -6- 2019 «Κύρωση Ποινικού Κώδικα» επέρχονται, μεταξύ των άλλων, αλλαγές και στα άρθρα 370Β και 370Γ. Έτσι στο άρθρο 370Γ έχει ενταχθεί το έγκλημα που τυποποιείται σήμερα στο άρθρο 370Β και στο άρθρο 370Δ, έχει ενταχθεί το έγκλημα που τυποποιείται σήμερα στο άρθρο 370Γ Ποινικού Κώδικα.
Η Ελληνική νομοθεσία αρχίζει σταδιακά να προσαρμόζεται στη νέα πραγματικότητα και νέες διατάξεις θεσπίζονται για την κύρωση των αδικημάτων που τελούνται στο Διαδίκτυο το οποίο έχει αναδειχθεί ως ένα νέο μέσο επικοινωνίας με παγκόσμια εμβέλεια και που εξαιτίας αυτού ανέκυψαν νέες προκλήσεις για την επιστήμη του ποινικού δικαίου.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΚ	**Αστικός Κώδικας**
ΑΕΠ	**Ακαθάριστο Εθνικό Προϊόν**
ΑΠ	**Άρειος Πάγος**
αρ	**Άρθρο**
Αιτ	**Αιτιολογική**
ΔΣ	**Διοικητικό Συμβούλιο**
δηλ	**Δηλαδή**
ΔΕΥ	**Συμβούλιο Δικαιοσύνης και Εσωτερικών Υποθέσεων**
ΕΕ	**Ευρωπαϊκή Ένωση**
ΕΟΧ	**Ευρωπαϊκό Οικονομικό Χώρο**
εδ	**εδάφιο**
Εκθ	**Έκθεση**
Εκδ	**Εκδόσεις**
Η/Υ	**Ηλεκτρονικός Υπολογιστής**
ΗΠΑ	**Ηνωμένες Πολιτείες Αμερικής**
κλπ	**και λοιπά**
λχ	**Λόγου Χάριν**
Ν	**Νόμος**
Ναυτ	**Ναυτοδικείο**
ΝΤ	**Νέες Τεχνολογίες**
ΟΟΣΑ	**Οργανισμός για την Οικονομική συνεργασία και Ανάπτυξη**

ΠΚ	**Ποινικός Κώδικας**
Παρ	**Παράγραφος**
περ	**περίπτωση**
ΠΟΕ	**Παγκόσμιος Οργανισμός Εμπορίου**
Π.χ	**Παραδείγματος Χάριν**
Ποιν. Χρ	**Ποινικά Χρονικά (περιοδικό)**
Ποιν. Δικ	**Ποινική Δικαιοσύνη (περιοδικό)**
Πειρ.	**Πειραιά**
Σχ	**Σχέδιο**
Σ	**Σύνταγμα**
ΤΠ	**Τεχνολογία Πληροφοριών**
ΦΕΚ	**Φύλλο Εφημερίδας Κυβερνήσεως**
DaaS	**Data as a Service**
DoS	**Denial of Service**
ECP	**Λειτουργία Ευρωπαϊκής Σύμπραξης για το υπολογιστικό νέφος**
IDC	**International Data Corporation**
IP	**Internet Protocol**
IaaS	**Infrastructure as a Service**
OS	**Τύπος Εκτελέσιμου αρχείου**
PaaS	**Platform as a Service**
SaaS	**Software as a Service**
VM	**Virtual Machine**
VNC	**Virtual Network Computing**

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΜΕΡΟΣ ΠΡΩΤΟ

ΚΕΦΑΛΑΙΟ 1^{Ο}

1.ΥΠΗΡΕΣΙΕΣ CLOUD COMPUTING

ΚΕΦΑΛΑΙΟ 2^{Ο}

ΚΕΦΑΛΑΙΟ 5^{Ο}

5. ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΩΝ ΔΥΝΑΤΟΤΗΤΩΝ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ (CLOUD COMPUTING) ΣΤΗΝ ΕΥΡΩΠΗ

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

ΑΠΟΡΡΗΤΑ (ΑΡΘΡΑ 370Β, 370Γ ΠΚ)

ΚΕΦΑΛΑΙΟ 6^{Ο}

ΚΕΦΑΛΑΙΟ 7^{Ο}

7. ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

ΚΕΦΑΛΑΙΟ 8^{Ο}

ΚΕΦΑΛΑΙΟ 9^{Ο}

ΚΕΦΑΛΑΙΟ 10^{Ο}

ΠΙΝΑΚΕΣ

ΕΙΣΑΓΩΓΗ

Η παρούσα εργασία εξετάζει τον κλάδο της τεχνολογίας των πληροφοριών, την «υπολογιστική νέφους» ως και τα μέτρα που λαμβάνονται στην Ελλάδα με τις διατάξεις των Νόμων 370Β και 370Γ Ποινικού Κώδικα για την νομική προστασία της ιδιωτικής σφαίρας του ατόμου, από την κατηγορία εγκλημάτων που προέκυψαν με την ανάπτυξη των ηλεκτρονικών υπολογιστών και του Διαδικτύου.
Στο πρώτο μέρος της εργασίας αναπτύσσεται α)η έννοια του υπολογιστικού νέφους β) τα πλεονεκτήματα του Cloud Computing γ) τα μειονεκτήματα του συστήματος δ) οι επιθέσεις και τα είδη των επιθέσεων στην ασφάλεια του δικτύου ε)η ασφάλεια στο υπολογιστικό νέφος και οι προβληματισμοί στ) η ιδιωτικότητα, εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του νέφους ζ)τα οφέλη ασφάλειας από τη χρήση των υπηρεσιών cloud η)εκμετάλλευση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη και θ) πως μπορεί να εξελιχθεί το cloud computing.
Το δεύτερο μέρος της εργασίας περιλαμβάνει τα μέτρα που λαμβάνονται στην Ελλάδα και Διεθνώς για την αντιμετώπιση των νέων μορφών εγκληματικότητας που παρουσιάστηκαν με την ανάπτυξη των τεχνολογικών μέσων και του διαδικτύου και κυρίως αναλύονται τα άρθρα 370Β και 370Γ του Ποινικού Δικαίου που θεσπίσθηκαν για να αντιμετωπιστεί στη χώρα μας η ηλεκτρονική εγκληματικότητα στο διαδίκτυο και το απόρρητο των επικοινωνιών. Στο μέρος αυτό καταγράφονται και αναλύονται α) Η προστασία της ιδιωτικής σφαίρας του ατόμου β) Το Διεθνές και Ευρωπαϊκό Νομοθετικό πλαίσιο γ) Οι εθνικές νομοθετικές παρεμβάσεις με το Ν 4411/2016 δ) Οι ειδικότερες διατάξεις της σύμβασης για το έγκλημα στον Κυβερνοχώρο ε) Το Ελληνικό πλαίσιο προστασίας του απορρήτου των επικοινωνιών στ) Το άρθρο 370Β ΠΚ (νομοτυπική μορφή – έννοια του όρου αθέμιτα – έννοια του απορρήτου – προστατευόμενο έννομο αγαθό άρθρου 370Β ΠΚ – αντικειμενική υπόσταση του άρθρου 370Β ΠΚ– Υπαλλακτικοί τρόποι τέλεσης του εγκλήματος – Υποκειμενική υπόσταση – Η διακεκριμένη μορφή της παρ2 του άρθρου 370Β ΠΚ – Η παραβίαση στρατιωτικών – διπλωματικών απορρήτων, άρθρο 370Β παρ 3.) ζ) Βασικά στοιχεία του άρθρου 370Γ(370Γ παρ1 ΠΚ – άρθρο 370Γ παρ2 διακρίσεις και χαρακτηρισμοί – Η αντικειμενική υπόσταση του άρθρου 370Γ παρ2 – Χωρίς δικαίωμα – η έννοια "παραβιάζοντας απαγορεύσεις ή μέτρα ασφάλειας").
Η εργασία μας όπως είναι διατυπωμένη πιστεύουμε ότι, αφ'ενός μεν βοηθά στην ανάδειξη του μεγέθους των δυνατοτήτων και των κινδύνων που περικλείουν οι νέες τεχνολογίες του Διαδικτύου ως η υπολογιστική νέφους, αφετέρου δε παραθέτει τα νομικά μέτρα τα οποία λαμβάνει η

χώρα μας για την προστασία της προσωπικότητας του ατόμου και των απορρήτων από κακόβουλες επιθέσεις, ως και για την θωράκιση από την εγκληματικότητα που συνδέεται με την πληροφορική και τους ηλεκτρονικούς υπολογιστές.

Επίσης πιστεύουμε ότι βοηθά στην ανάδειξη της εξέλιξης της τεχνολογίας του Διαδικτύου με τα μειονεκτήματα και πλεονεκτήματα αυτού ως και τον νομικό τρόπο αντιμετώπισης των διαφόρων μορφών εγκληματικής συμπεριφοράς εκείνων που επωφελούνται από τη σύγχρονη τεχνολογία και επιτίθενται κατά του ατόμου και των επιτευγμάτων αυτού.

Η ραγδαία εξέλιξη της τεχνολογίας και η ανάπτυξη της πληροφορικής, που επέφερε πρωτοφανή επανάσταση στην επικοινωνία, έχει αλλάξει τη μορφή του κόσμου, τα προβλήματα δε που συνόδευσαν την ως άνω ενωσιακή εξέλιξη και αφορούν την εγκληματικότητα, μπορούν να αντιμετωπισθούν μόνο με διεθνείς κοινές νομοθετικές πρακτικές προσαρμοσμένες πάντα στα εθνικά ποινικά δίκαια.

ΜΕΡΟΣ ΠΡΩΤΟ

ΚΕΦΑΛΑΙΟ 1ο

1. ΥΠΗΡΕΣΙΕΣ CLOUD COMPUTING

1.1 Ιστορική και εννοιολογική προσέγγιση της έννοιας Cloud Computing

Η έννοια του Υπολογιστικού Νέφους (Cloud Computing) πρωτοεμφανίστηκε τη δεκαετία του 1950 σε εκπαιδευτικά ινστιτούτα και εταιρείες, και η χρήση του πραγματοποιούταν από κεντρικούς υπολογιστές μεγάλων υπολογιστικών και αποθηκευτικών δυνατοτήτων.[1] Οι χρήστες είχαν πρόσβαση σε αυτούς τους υπολογιστές μέσω τερματικών (dumb terminals), οι οποίοι δεν είχαν ούτε υπολογιστική ισχύ ούτε αποθηκευτικές ικανότητες. Ο όρος του Υπολογιστικού Νέφους έγινε ευρύτερα γνωστός τη δεκαετία του 1970, όταν η IBM και η Google αποφάσισαν να συνεργαστούν στο συγκεκριμένο τεχνολογικό πεδίο. Αρχικά η IBM παρουσίασε το λειτουργικό σύστημα εικονικών μηχανών (VM operating system), το οποίο παρείχε τη δυνατότητα να εργάζονται πολλές εικονικές μηχανές(virtual machines) στο ίδιο μηχάνημα. Κάθε εικονική μηχανή είναι – ήταν μία αυτοτελής οντότητα που εκτελεί το δικό της λειτουργικό σύστημα και παρέχει υπολογιστικούς πόρους, όπως τη – μια κεντρική μονάδα επεξεργασίας, μνήμης και μονάδες εισόδου-εξόδου.

Τη δεκαετία του 1980, η πρώτη τακτική χρήση των προσωπικών υπολογιστών συνοδεύτηκε από την υπόσχεση ότι οι χρήστες θα ήταν σε θέση να αποφασίζουν οι ίδιοι για το υπολογιστικό τους περιβάλλον. Η εμφάνιση του Διαδικτύου και του Παγκόσμιου Ιστού, εκτόξευσε τη φήμη του Υπολογιστικού Νέφους. Τη δεκαετία του 1990 εμφανίστηκαν τα Εικονικά Ιδιωτικά Δίκτυα(Virtual Private Networks).Μέχρι τότε ,οι εταιρείες τηλεπικοινωνιών υποστήριζαν τα κυκλώματα δεδομένων σημείο προς σημείο(point-to-point data circuits). Μέχρι το 2000, κολοσσοί της Πληροφορικής όπως η Amazon, η Microsoft και η Google, ασχολήθηκαν με την ανάπτυξη και την παροχή υπηρεσιών

[1] "Υπολογιστικό νέφος- Ιστορία", https://el.wikipedia.org, σελ 1

Υπολογιστικού Νέφους. Ακολούθησαν κάποια γεγονότα που θεωρούνται ευρέως ως ορόσημα στην ιστορία του Υπολογιστικού Νέφους. Το 2006, η Amazon παρουσίασε το Ελαστικό Υπολογιστικό Νέφος(Elastic Compute Cloud(EC2)). Μία εμπορική υπηρεσία βασισμένη στο Παγκόσμιο Ιστό, που παρείχε στο χρήστη τη δυνατότητα να υλοποιεί εφαρμογές σε ενοικιασμένα-ενοικιαζόμενα μηχανήματα. Το 2008, προωθήθηκε στην αγορά το Eucalyptus, η πρώτη πλατφόρμα ανοικτού κώδικα για ανάπτυξη ιδιωτικών σύννεφων(private clouds). Την ίδια χρόνια, η Google κυκλοφόρησε το Google App Engine, μια πλατφόρμα που υποστήριζε διάφορες υπηρεσίες του Υπολογιστικού Νέφους. Στην συνέχεια των εξελίξεων το 2011, η IBM SmartCloud ενώ το 2012 κυκλοφόρησε το Oracle Cloud. Τέλος η Microsoft ανακοίνωσε επίσης ότι θα εισαγάγει το cloud computing στην επόμενη μεγάλη ενημέρωση λύσεων Dynamics ERP και θα λειτουργούν μέσω πλατφόρμας Windows Azure.

1.2 Υπολογιστικό Νέφος - Ορισμός

Αν και στην βιβλιογραφία εμφανίζεται πληθώρα ορισμών για το Υπολογιστικό Νέφος, δεν υπάρχει κάποιος ο οποίος να έχει καθιερωθεί και να είναι κοινά αποδεκτός. Ένας ορισμός που χρησιμοποιείται συχνά είναι πως: "Το υπολογιστικό νέφος[2] είναι η αποθήκευση, η επεξεργασία και η χρήση δεδομένων από απομακρυσμένους υπολογιστές στους οποίους εξασφαλίζεται πρόσβαση μέσω του διαδικτύου." Πολλοί άνθρωποι χρησιμοποιούν σήμερα το υπολογιστικό νέφος δίχως καν να το συνειδητοποιούν. Υπηρεσίες όπως το διαδικτυακό ηλεκτρονικό ταχυδρομείο ή τα κοινωνικά δίκτυα συχνά βασίζονται στην τεχνολογία του υπολογιστικού νέφους. Για τους επαγγελματίες χρήστες της τεχνολογίας των πληροφοριών το υπολογιστικό νέφος σημαίνει μεγάλη ευελιξία όσον αφορά τις ανάγκες υπολογιστικής ισχύος. Για παράδειγμα όποτε διαπιστώνεται αυξημένη χρήση μιας υπηρεσίας, μέσω του υπολογιστικού νέφους είναι πολύ απλό να προστεθεί επιπλέον δυναμικό σε αυτή, κάτι για το οποίο θα απαιτείτο πολύ περισσότερος χρόνος εάν μια εταιρία υποχρεωνόταν να εγκαταστήσει νέες μηχανές στο δικό της κέντρο δεδομένων. Κάποιοι ορισμοί του Υπολογιστικού Νέφους εμφανίζονται στενότεροι λ.χ. εκείνοι που αναφέρουν ότι:

[2] http://europa.eu/rapid/press-release:Ευρωπαϊκή Επιτροπή,2013,σελ 1

"Το Υπολογιστικός νέφος (cloud computing)[3] αναφέρεται στις υπηρεσίες τεχνολογιών πληροφόρησης και επικοινωνίας που χρησιμοποιούνται μέσω διαδικτύου για την πρόσβαση σε λογισμικό, υπολογιστική δύναμη, χωρητικότητα αποθήκευσης κλπ" ή ότι: "Υπολογιστικό Νέφος[4] ονομάζεται η κατ'αίτηση διαδικτυακή κεντρική διάθεση υπολογιστικών πόρων(όπως δίκτυο, εξυπηρετητές, εφαρμογές και υπηρεσίες) με υψηλή ευελιξία , ελάχιστη προσπάθεια από τον χρήστη και υψηλή αυτοματοποίηση." Στο Υπολογιστικό Νέφος η αποθήκευση, η επεξεργασία και η χρήση δεδομένων, λογισμικού και υπηρεσιών γίνεται διαδικτυακά, μέσω απομακρυσμένων υπολογιστών σε κεντρικά Datacenter. Υπηρεσίες όπως η κατ'αίτηση παροχή εικονικών μηχανών, το διαδικτυακό ηλεκτρονικό ταχυδρομείο ή τα κοινωνικά δίκτυα συχνά βασίζονται στην τεχνολογία του Υπολογιστικού Νέφους. Από την παράθεση και ανάλυση των ως άνω ορισμών δεν νομίζουμε πως υπάρχουν ουσιαστικές διαφορές στις διάφορες «κατηγορίες» ορισμών του Υπολογιστικού Νέφους, αφού τελικά στο ίδιο αποτέλεσμα καταλήγουν.

1.3 Λειτουργία υπολογιστικού νέφους

Ο χρήστης συνδέει τον υπολογιστή του στην πλατφόρμα του υπολογιστικού νέφους μέσω εξειδικευμένου λογισμικού. Στο υπολογιστικό νέφος, η επεξεργαστική ισχύς εξασφαλίζεται από μεγάλα κέντρα δεδομένων, με εκατοντάδες εξυπηρετητές και συστήματα αποθήκευσης δεδομένων, που στην πράξη είναι σε θέση να χειριστούν σχεδόν οιοδήποτε λογισμικό υπολογιστή(από την επεξεργασία δεδομένων μέχρι τα βιντεοπαιχνίδια που ενδέχεται να χρειαστούν οι πελάτες). Ενίοτε οι αντίστοιχες υπηρεσίες προσφέρονται δωρεάν(π.χ. διαδικτυακό ηλεκτρονικό ταχυδρομείο), αλλά οι περισσότεροι πελάτες έχουν τη δυνατότητα να χρησιμοποιήσουν ένα ευέλικτο σύστημα για πληρωμές ανάλογα με τις χρησιμοποιούμενες υπηρεσίες ή με την καταβολή μηνιαίου παγίου.

1.4 Αποθήκευση δεδομένων υπολογιστικού νέφους

Τα δεδομένα όταν χρησιμοποιώ το υπολογιστικό νέφος αποθηκεύονται σε ένα κέντρο δεδομένων κάπου στον πλανήτη. Στις περιπτώσεις που η

[3] https://cyberalert.gr/ypiresies-ypologistikoy-nefous/
[4] https://www.epset.gr/el/content/yplogistiko-nefos-cloud-computing

φυσική τοποθεσία των εγκαταστάσεων είναι σημαντική, οι χρήστες μπορούν να αιτούνται ώστε αυτή να διευκρινίζεται στις συμβάσεις που έχουν συνάψει για εξυπηρέτηση μέσω του υπολογιστικού νέφους. Όσον αφορά τα προσωπικά δεδομένα τρίτων, η οδηγία για την προστασία των δεδομένων επιβάλλει τα δεδομένα να αποθηκεύονται είτε στον Ευρωπαϊκό Οικονομικό Χώρο(ΕΟΧ) ή σε επικράτεια διεπόμενη από ισοδύναμους νόμους περί ιδιωτικότητας.

1.5 Αρχιτεκτονική του υπολογιστικού νέφους

Η αρχιτεκτονική υπολογιστικού νέφους ορίζει[5] τα στοιχεία και τις επιμέρους συνιστώσες που απαιτούνται για το υπολογιστικό νέφος. Στην απλή μορφή του, τα θεμέλια του υπολογιστικού νέφους μπορεί να ταξινομηθούν σε δύο τμήματα: front – end και back – end, τα οποία είναι συνδεδεμένα μεταξύ τους μέσω ενός εικονικού δικτύου ή του διαδικτύου. Το υπολογιστικό νέφος συντελείται από τις ακόλουθες βασικές δυνατότητες και λειτουργίες:

1. Front end platform (fat client, thin client, mobile device). Οι αρχές του υπολογιστικού νέφους(η front- end πλατφόρμα) ονομάζονται επίσης πελάτες ή cloud clients. Αυτοί οι πελάτες είναι διακομιστές, fat(or thick) clients, zero or ultra-thin client, τα ταμπλέτς και τις κινητές συσκευές. Αυτές οι πλατφόρμες πελατών αλληλοεπιδρούν με την αποθήκευση δεδομένων cloud μέσω μιας εφαρμογής(middleware) και μέσω ενός προγράμματος περιήγησης ιστού ή μέσω μιας εικονικής περιόδου σύνδεσης. Ένας zero or ultra-thin client προετοιμάζει το δίκτυο ώστε να συγκεντρώσει τα απαιτούμενα αρχεία ρυθμίσεων όπου είναι αποθηκευμένα τα εκτελέσιμα OS της.
2. Back end platforms (servers, αποθήκευσης). Μια ηλεκτρονική αποθήκευση δικτύου, όπου τα δεδομένα αποθηκεύονται και είναι προσβάσιμα σε πολλούς πελάτες.
3. Η παράδοση με βάση το υπολογιστικό νέφος όπως(IaaS – Infrastructure as a Service), οι πλατφόρμες με περιβάλλον προγραμματισμού(PaaS – Platform as a Service) και το λογισμικό(SaaS – Λογισμικό ως Υπηρεσία), και

[5] https://el.wikipedia.org: Υπολογιστικό νέφος, σελ 2

4. Ένα δίκτυο(Internet, Intranet, Intercloud). Τα μοντέλα ανάπτυξης είναι είτε ιδιωτικά(private) είτε δημόσια(internet) είτε σε συνδυασμό των δύο(hybric/intercloud).

1.6 Μορφές υπολογιστικού νέφους

Υπάρχουν τέσσερις βασικές κατηγορίες μοντέλων "υπηρεσιών σύννεφου":[6]

1. **Software-as-a-Service (SaaS):** Αντί να εγκατασταθεί λογισμικό στο μηχάνημα και στον υπολογιστή του πελάτη επιβαρύνοντάς τον με τακτικές επιδιορθώσεις, συχνές εκδόσεις κτλ., εφαρμογές όπως το Word, CRM (Διαχείριση Σχέσεων Πελατών), ERP (Enterprise Resource) Προγραμματισμός) διατίθενται (φιλοξενούνται) μέσω του διαδικτύου για την κατανάλωση του τελικού χρήστη.
2. **Platform-as-a-Service (PaaS):** Αντί ο πελάτης να χρειαστεί να αγοράσει – πληρώσει τις άδειες λογισμικού για πλατφόρμες όπως και τα λειτουργικά συστήματα, τις βάσεις δεδομένων και το ενδιάμεσο λογισμικό, μπορεί να το κάνει χρησιμοποιώντας την πλατφόρμα και τα εργαλεία(όπως το java, το .NET, Python, Ruby on Rails).
3. **Infrastructure-as-a-Service (IaaS):** Πρόκειται για τις απλές-βασικές υλικές συσκευές(raw υπολογιστές)όπως είναι οι εικονικοί υπολογιστές, οι διακομιστές, οι συσκευές αποθήκευσης, η μεταφορά μέσω του δικτύου, οι οποίες βρίσκονται φυσικά σε ένα κεντρικό σημείο(κέντρο δεδομένων). Υπάρχει η δυνατότητα να προσπεραστούν και να χρησιμοποιηθούν από το διαδίκτυο χρησιμοποιώντας τα συστήματα ελέγχου ταυτότητας σύνδεσης και τους κωδικούς πρόσβασης από οποιοδήποτε dumb τερματικό ή συσκευή.
4. **Desktop-as-a-Service (DaaS):** Η υπηρεσία επιφάνεια εργασίας προσφέρει μια υποδομή εικονικής επιφάνειας εργασίας (Virtual Desktop Ifranstructure – VDI) που φιλοξενείται από έναν πάροχο λύσεων λογισμικού cloud και βασίζεται συνήθως σε ένα μοντέλο μηνιαίας συνδρομής. Το DaaS χρησιμοποιεί μια αρχιτεκτονική πολλαπλών μισθώσεων, πράγμα που σημαίνει ότι μια μοναδική

[6] https://el.wikipedia.org, Υπολογιστικό νέφος, σελ 2

εμφάνιση μιας εφαρμογής εξυπηρετείται σε πολλούς χρήστες, που αναφέρονται ως "ενοικιαστές". Ο πάροχος λύσεων λογισμικού cloud είναι υπεύθυνος για τη διαχείριση του cloud και της υποκείμενης υποδομής και το επίπεδο εξυπηρέτησης μπορεί να διαφέρει ανάλογα με τις ανάγκες των χρηστών. Το τελικό αποτέλεσμα αυτής της υποδομής είναι ότι οι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα και τις εφαρμογές τους από σχεδόν οποιαδήποτε συσκευή, οπουδήποτε.

1.7 Πλεονεκτήματα του Cloud Computing

Το Cloud Computing διαθέτει πλεονεκτήματα σημαντικά για το χρήστη. Συγκεκριμένα διαθέτει:[7] [8] [9] [10] [11] [12]

1.7.1 Πρόσβαση από παντού: Ο χρήστης μπορεί να μπει από το διαδίκτυο στα δεδομένα που έχουν αποθηκευτεί από οποιοδήποτε σημείο του κόσμου με ασφάλεια. Όταν η σύνδεση με το διαδίκτυο δεν είναι εφικτή, μπορούν να ικανοποιηθούν οι απαιτήσεις και μέσω του mobile internet.

1.7.2 Ευελιξία: Σε περίπτωση που μια εταιρεία χρειαστεί να μετακινηθεί ολόκληρη είτε κάποιο συγκεκριμένο τμήμα της, ο χρόνος που θα παραμείνει χωρίς πληροφορίες είτε ο κίνδυνος απώλειας των στοιχείων είναι μηδενικός καθώς όλα τα συστήματα και το λογισμικό παραμένουν διαθέσιμα.

Για την συγκεκριμένη κατηγοριοποίηση, οι επιχειρήσεις κλήθηκαν να απαντήσουν σε ποιο βαθμό επωφελήθηκαν από τη χρήση του Cloud

[7] Τσεσμελής Βασίλειος : Ασφάλεια και εφαρμογές Cloud Computing, 2018, σελ 23

[8] Kostas E, Psannis, Christos Stergiou, and B. B. Gupta, Advanced Media-based Smart Data on Intelligent Cloud Systems, IEEE Transactions on Sustainable Computing (T-SUSC), June 2018

[9] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, Secure integration of IoT and Cloud Computing, Elsevier, Future Generation Computer Systems, December 2016

[10] Christos Stergiou and Kostas E.Psannis, Efficient and Secure BIG Data Delivery in Cloud Computing, Multimedia Tools and Applications, 2017

[11] Christos Stergiou, Kostas E. Psannis, B.B. Gupta, and Yutaka Ishibashi, Security, Privacy & Efficiency of Sustainable Cloud Computing, Informatics and Systems, Elsevier, June 2018

[12] C. Stergiou, Kostas. E. Psannis, A. P. Plageras, Y. Ishibashi, B.-G. Kim, "Algorithms for efficient digital media transmission over IoT and cloud networking", Journal of Multimedia Information System, vol. 5, no. 1, pp. 1-10, March 2018

Computing, με την ανάλυση «υψηλό βαθμό», «κάποιο βαθμό», «περιορισμένο βαθμό», «καθόλου».[13]

Πίνακας 1:Ευελιξία λόγω της δυνατότητας αναπροσαρμογής των υπηρεσιών υπολογιστικού νέφους(Ά Τρίμηνο 2014)

Σε υψηλό βαθμό	24,81 %
Σε κάποιο βαθμό	53,68 %
Σε περιορισμένο βαθμό	12,35 %
Καθόλου	9,15 %

1.7.3 Συνεργασία: Καθώς υπάρχουν τα δεδομένα αποθηκευμένα και υπάρχει διαθέσιμη πρόσβαση στο διαδίκτυο, οι εργαζόμενοι μιας επιχείρησης , μπορούν να συνεργαστούν ακόμα και στην περίπτωση που βρίσκονται και εκτός του χώρου εργασίας.

1.7.4 Αποθηκευτικός χώρος: Ο αποθηκευτικός χώρος είναι απεριόριστος κάτι που είναι πλεονέκτημα για την επιχείρηση καθώς την αποδεσμεύει από συνεχείς αναβαθμίσεις με στόχο την εξοικονόμηση χώρου.

1.7.5 Βέλτιστη χρήση πόρων: Παλαιότερα οι επιχειρήσεις σπαταλούσαν χρόνο για την προετοιμασία υπηρεσιών και πολλές φορές χωρίς αποτέλεσμα καθώς δεν ανταποκρίνονταν στις προσδοκίες τους. Με το Cloud Computing μειώνονται οι δαπάνες και αυξάνεται η χωρητικότητα καθώς οι πόροι διατίθενται μόνο όταν είναι απαραίτητοι.

1.7.6 Disaster Recovery: Σε περίπτωση καταστροφής της μηχανοργάνωσης μιας επιχείρησης, μέσω των υπηρεσιών σύννεφων μπορούν να ενεργοποιηθούν οι διαδικασίες αποκατάστασης της ζημιάς και μέσω των αντιγράφων ασφαλείας που υπάρχουν να επέλθει η λύση.

1.7.7 Οικονομικά Οφέλη: Η οικονομία είναι από τα βασικότερα οφέλη του cloud computing. Το κόστος που μπορεί να έχει ένα λογισμικό ίσως να είναι πολύ μεγάλο για μια μικρή εταιρία. Με το «cloud» τα δεδομένα αυτά αλλάζουν καθώς η εταιρία δεν πληρώνει την εφαρμογή αλλά πληρώνει την χρήση της. Συνήθως σε δίκτυα cloud υπάρχουν πολλές δυνατότητες και τρόποι για την πληρωμή της χρήσης κάποιας

[13] https://cyberalert.gr/ypiresies-ypologistikou-nefous/

εφαρμογής.
Για την συγκεκριμένη κατηγοριοποίηση[14] , οι επιχειρήσεις κλήθηκαν να απαντήσουν σε ποιο βαθμό επωφελήθηκαν από τη χρήση του cloud computing, με την ανάλυση «υψηλό βαθμό», «κάποιο βαθμό», «περιορισμένο βαθμό», «καθόλου».

Πίνακας 2: Μείωση του κόστους που σχετίζεται με τις τεχνολογίες πληροφόρησης και επικοινωνίας(Ά Τρίμηνο 2014)

Σε υψηλό βαθμό	18,12 %
Σε κάποιο βαθμό	43,75 %
Σε περιορισμένο βαθμό	27,75 %
Καθόλου	10,38 %

1.7.8 Απλότητα: Το ότι δεν χρειάζεται η επιχείρηση να αγοράσει και να διαμορφώσει νέο εξοπλισμό επιτρέπει στην επιχείρηση και το προσωπικό της μηχανογράφησής της να ασχοληθούν με τα σημαντικά πράγματα της επιχείρησης. Η λύση «σύννεφου» κάνει δυνατόν να ξεκινήσει την εφαρμογή της αμέσως και κοστίζει πολύ λιγότερο απ'ότι θα κόστιζε η υλοποίηση μιας λύσης τοπικά.[15]

1.7.9 Λογισμικό: Το λογισμικό που συνδέεται με ένα διακομιστή σύννεφου ο οποίος ενημερώνεται αυτόματα με αποτέλεσμα να βοηθά με τη σειρά του την επιχείρηση να ασχολείται μόνο με τα θέματα που την απασχολούν.

1.7.10 Πολλαπλές τοποθεσίες: Για την αναπαραγωγή περιεχομένου, οι πάροχοι συντηρούν κάποιους οικονομικούς πόρους κάνοντας έτσι δυνατή την αποφυγή αποτυχιών. Με αυτό τον τρόπο απορρίπτεται οποιαδήποτε ζημιά.

1.7.11 Διαχείριση απειλών: Ένας απλός καταναλωτής είτε μια μικρή επιχείρηση δεν έχει τα μέσα και τους τρόπους για να αντιμετωπίσει πιθανές απειλές. Οι πάροχοι των υπηρεσιών cloud παρόλα αυτά διαθέτουν και μπορούν να βρουν τρόπους ακόμα και να αναπτύξουν στρατηγικές διαχείρισης των απειλών.

[14] https://cyberalert.gr/yphresies-ypologistikou-nefous/σελ 4
[15] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter: Cloud Computing. Μια πρακτική προσέγγιση, 2010, σελ 30

1.7.12 Άμεση ανταπόκριση σε οποιαδήποτε πρόκληση: Οι πάροχοι των υπηρεσιών Cloud μπορούν να αντιληφθούν άμεσα ένα κακόβουλο λογισμικό λόγω της εφαρμογής συστημάτων που τους επιτρέπουν την άμεση ανταπόκριση.

1.7.13 Δίκτυα αιχμής: Οι υπηρεσίες Cloud διαθέτουν δυνατότητες αποθήκευσης και επεξεργασίας πληροφοριών μέσω εξελιγμένων τεχνολογιών, προσφέροντας στους χρήστες αξιοπιστία, βελτιωμένη ποιότητα και λιγότερα προβλήματα δικτύου.

1.7.14 Γρήγορη επέκταση των πόρων: Οι πόροι που υποστηρίζονται από τις υπηρεσίες Cloud (αποθήκευση, επεξεργασία δεδομένων, μνήμη, χρήση εικονικών μηνυμάτων, υπηρεσίες δικτύου), έχουν τη δυνατότητα να επεκταθούν γρήγορα με τη βοήθεια και από τη συνεχόμενη εξέλιξη της τεχνολογίας. Οι πάροχοι διαθέτουν αρκετούς πόρους και δυνατότητα αναδιανομής τους, προκειμένου να μεγιστοποιήσουν τα μέτρα ασφαλείας όταν πρόκειται να πραγματοποιηθεί πιθανή «επίθεση». Με αυτό τον τρόπο μπορούν να περιοριστούν οι επιθέσεις και οι επιπτώσεις που αυτές επιφέρουν, χρησιμοποιώντας συνδυαστικά την ευέλικτη αναδιανομή των πόρων και την κατάλληλη μέθοδο βελτιστοποίησης των πόρων.

1.7.15 Συγκέντρωση των πόρων: Η συγκέντρωση των πόρων έχει αρκετά οφέλη εκτός από κάποια μειονεκτήματα. Θεωρώντας την ύπαρξη ικανοποιητικών μέτρων ασφαλείας δεδομένη, η συγκέντρωση των πόρων πλεονεκτεί στη φθηνότερη παραμετροποίηση και στο φθηνότερο έλεγχο πρόσβασης ανά μονάδα πόρου, στη φθηνότερη εφαρμογή ολοκληρωμένης πολιτικής ασφάλειας και ελέγχου πάνω στη διαχείριση δεδομένων και στη διαχείριση περιστατικών, όπως επίσης και φθηνότερες διαδικασίες συντήρησης.

Αναβαθμίσεις και προεπιλογές στο Cloud Computing οι εικόνες των εικονικών μηχανών και το λογισμικό που χρησιμοποιείται από τους πελάτες μπορεί να αναβαθμιστεί με τις τελευταίες εκδόσεις και ρυθμίσεις ασφαλείας. Επίσης, οι υπηρεσίες IaaS προσφέρουν περιβάλλοντα προγραμμάτων τα οποία παρέχουν τη δυνατότητα λήψης φωτογραφίας από το εικονικό περιβάλλον και να συγκρίνεται με το αρχικό. Οι αναβαθμίσεις πολλές φορές λαμβάνουν χώρα πιο γρήγορα πάνω στη πλατφόρμα. Αυτά είναι όλα τα οφέλη που αφορούν τη βελτίωση της ασφάλειας.

1.7.16 Πεπειραμένοι προμηθευτές: Γενικά, όταν κάποια νέα τεχνολογία γίνεται δημοφιλής, υπάρχει αφθονία προμηθευτών που προσφέρουν την δική τους έκδοση αυτής της τεχνολογίας. Αυτό δεν είναι πάντα καλό, επειδή πολλοί από αυτούς τους προμηθευτές τείνουν να προσφέρουν μη χρήσιμες τεχνολογίες. Σε αντίθεση οι πρώτοι προμηθευτές που εμφανίστηκαν στο cloud computing είναι πραγματικά πολύ αξιόπιστες επιχειρήσεις. Εταιρείες όπως οι Amazon, Google, Microsoft, IBM και Yahoo είναι καλοί προμηθευτές, επειδή προσφέρουν αξιόπιστες υπηρεσίες και πολύ χωρητικότητα.[16]

1.8 Μειονεκτήματα του Cloud Computing

Παρά τα πλεονεκτήματα που χαρακτηρίζουν το Cloud Computing προκύπτουν κάποια μειονεκτήματα[17] τα οποία συνδέονται κυρίως με την διαθέσιμη συνδεσιμότητα με το διαδίκτυο και με την λειτουργικότητα του διακομιστή. Η κοινή χρήση δεδομένων μπορεί εύκολα να γίνει μειονέκτημα, καθώς προκύπτουν θέματα νομικής φύσεως, θέματα ασφάλειας, κόστους, πολυπλοκότητα και αβεβαιότητα.

1.8.1 Ασφάλεια: Αποτελεί ένα από τα κύρια μειονεκτήματα καθώς συχνά ο διακομιστής δέχεται επιθέσεις από Hackers. Πιο συγκεκριμένα, ο χρήστης αποθηκεύει τα δεδομένα του στο διακομιστή ο οποίος σε περίπτωση που δεχτεί την επίθεση μπορεί να χάσει τα δεδομένα. Υπάρχουν πολλοί κίνδυνοι[18] όταν χρησιμοποιείται ένας παροχέας «σύννεφου» αλλά σε αξιόπιστες επιχειρήσεις προσπαθούν σκληρά να διατηρήσουν τους προμηθευτές ασφαλείς. Οι προμηθευτές έχουν αυστηρές πολιτικές μυστικότητας και υιοθετούν αυστηρά μέτρα ασφάλειας όπως αποδεδειγμένες κρυπτογραφικές μεθόδους για να επικυρώνουν τους χρήστες.

1.8.2 Πρόσβαση στο διαδίκτυο: Βασικός συντελεστής για την χρήση των υπηρεσιών Cloud είναι η σύνδεση με το διαδίκτυο. Σε περίπτωση

[16] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter: Cloud Computing. Μια πρακτική προσέγγιση, 2010, σελ 30
[17] Τσεσμελής Βασίλειος: Ασφάλεια και εφαρμογές Cloud Computing,2018,σελ 26
[18] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter: Cloud Computing. Μια πρακτική προσέγγιση, 2010, σελ 31

που δεν υπάρχει σύνδεση στο διαδίκτυο δεν μπορεί ο χρήστης να κάνει χρήση των υπηρεσιών.

1.8.3 Κόστος: Το χρονικό διάστημα το οποίο απαιτείται για να πραγματοποιηθεί η μετάβαση από τη συμβατική τεχνολογία ίσως δημιουργεί κόστος το οποίο να αποτρέπει το χρήστη να συνεχίσει τη διαδικασία.

1.8.4 Προβληματισμοί Νομικής Φύσεως: Ένας άλλος προβληματισμός αφορά θέματα νομικού περιεχομένου, αφορά την προστασία προσωπικών δεδομένων όταν ένας χρήστης χρησιμοποιεί περιβάλλον σύννεφου. Οι προβληματισμοί χρήζουν ουσιαστικής προσοχής όταν υπάρχει συνδυασμός θεμάτων ασφάλειας και ιδιωτικότητας. Ο χρήστης θα πρέπει να γνωρίζει ποια από τα προσωπικά στοιχεία καταγράφηκαν και σε περίπτωση που δεν συμφωνεί με αυτό να ζητήσει διακοπή της διαδικασίας.

1.8.5 Αυξημένη πολυπλοκότητα: Όταν έχουμε μία εφαρμογή αποθηκευμένη κάπου τοπικά, σε ένα δικό μας διακομιστή και προσπαθούμε να την κάνουμε να επικοινωνήσει με μία άλλη στο σύννεφο “cloud”.

1.8.6 Μη χρήση υπολογιστικού νέφους(cloud computing)

Από τις 20.578 επιχειρήσεις που απάντησαν ότι έχουν πρόσβαση στο διαδίκτυο, οι 18.822 απάντησαν ότι δεν αγόρασαν υπηρεσίες υπολογιστικού νέφους, ποσοστό δηλαδή που ανέρχεται σε 91,46%. Σε σχετική ερώτηση για τους λόγους που εμπόδισαν την επιχείρηση από το να κάνει χρήση του cloud computing το μεγαλύτερο ποσοστό, 43,1%, ήταν η μη επαρκής γνώση του υπολογιστικού νέφους.[19]

ΠΙΝΑΚΑΣ 3:Λόγοι μη χρήσης υπολογιστικού νέφους (Ά Τρίμηνο 2014)

Το ρίσκο παραβίασης ασφάλειας	26,26%
Η αβεβαιότητα για την τοποθεσία των δεδομένων	21,83%
Το υψηλό κόστος αγοράς των υπηρεσιών	28,53%

[19] https://cyberalert.gr/ypiresies-ypologistikou-nefous/σελ 5

Η μη επαρκής γνώση	43,10%

ΚΕΦΑΛΑΙΟ 2ο

2. ΕΠΙΘΕΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΔΙΚΤΥΟΥ[20]

Είναι ίσως προφανές ότι ο όρος «εισβολέας» σημαίνει διαφορετικά πράγματα για διαφορετικούς ανθρώπους. Μερικές φορές υποδηλώνει τον ασυγκράτητο προγραμματιστή που είναι έτοιμος να αναλώσει ακόμη και το χρόνο του ύπνου του, για να δουλέψει με τη μηχανή, να ξεδιαλύνει το ένα ή το άλλο πράγμα του προγράμματος ή να καλύψει κάποια «ατέλεια». Αυτές οι δραστηριότητες, αν και συνιστούν μια νοσηρή κατάσταση, δεν είναι απαραίτητα απαγορευμένες ή παράνομες.

Κατά μια άλλη έννοια, η εισβολή υποδηλώνει μια αξιόποινη πράξη, την επιδέξια χρησιμοποίηση του υπολογιστή για τη διάπραξη αξιόποινων πράξεων διαφόρων ειδών.

Το πρώτο σημαντικό περιστατικό ασφάλειας παρουσιάστηκε στο διαδίκτυο το 1988.[21] Ονομάστηκε Morris Worm, από το όνομα του φοιτητή του Cornell University, Robert Morris, που έγραψε ένα πρόγραμμα που μπορούσε να συνδεθεί σε έναν άλλο υπολογιστή, να αντιγραφεί σε αυτόν και να αρχίσει να κάνει το ίδιο με τον επόμενο υπολογιστή στο δίκτυο. Αυτό το αυτόματα αναπαραγόμενο πρόγραμμα προκάλεσε μια γεωμετρική έκρηξη επιθέσεων στο διαδίκτυο. Το πρόγραμμα χρησιμοποίησε τόσους πολλούς πόρους από το σύστημα που βρισκόταν, ώστε τελικά έπαυσε να είναι λειτουργικό. Το αποτέλεσμα ήταν το 10% των υπολογιστών που ήταν συνδεδεμένοι στο ARPANET (σε σύνολο 88,000) να σταματήσουν τη λειτουργία τους την ίδια ώρα. Το δίκτυο που θα μπορούσε να ήταν το μέσο που θα βοηθούσε στην επίλυση του προβλήματος, είχε πάψει να είναι λειτουργικό. Επιπλέον οι διαχειριστές πολλών sites από φόβο μήπως «μολυνθούν» τα συστήματά τους, σταματούσαν την επικοινωνία τους με το δίκτυο για να

[20] R. Doswell, G.L.Simons: Πληροφορική και Εγκληματικότητα, Αθήνα 1990, σελ 69
[21] Κομνηνός Θόδωρος, Σπυράκος Παύλος, Ασφάλεια δικτύων υπολογιστικών συστημάτων, Αθήνα 2002, σελ 47

αντιμετωπίσουν την κατάσταση, με αποτέλεσμα να γίνονται περισσότεροι οι κόμβοι που δεν ήταν συνδεδεμένοι.

Από την πρώτη σημαντική εμφάνιση μαζικής επίθεσης, μέχρι σήμερα η ίδια η εξέλιξη του internet είναι τέτοια που το έχει κάνει ένα μέσο διακίνησης τεράστιων ποσοτήτων πληροφορίας σχετικές με τα τρωτά του. Έχει καταφέρει να ενώσει ανθρώπους σε ομάδες που δεν γνωρίζονται προσωπικά, αλλά έχουν κοινά ενδιαφέροντα και επιδιώξεις. Η διακίνηση της πληροφορίας είναι ελεύθερη και φθάνει ταχύτατα σε κάθε σημείο του πλανήτη. Οι νέοι μαθαίνουν από τους γνώστες νέους τρόπους επιθέσεων, τροφοδοτούνται με εργαλεία, εκπαιδεύονται σε μεθόδους, γίνονται έμπειροι στην αποκάλυψη νέων τρωτών σημείων και όλοι μαζί προσπαθούν να γίνουν γνωστοί στην ομάδα κρυμμένοι πίσω από το ψευδώνυμό τους κάνοντας όμως αισθητή την παρουσία τους στον κόσμο.

2.1 Είδη επιθέσεων και τεχνικές[22]

2.1.1 Επίθεση στις ιστοσελίδες

Τα sites με σελίδες του διαδικτύου ήταν πάντα ο αγαπημένος στόχος των hackers, ίσως γιατί δεν προσφέρουν ικανοποιητική ασφάλεια και τις σελίδες τους επισκέπτονται πολλοί άνθρωποι κάθε μέρα. Η αλλαγή της κεντρικής σελίδας αυτών των sites γίνεται συνήθως για να διαβαστούν από πολλούς πολιτικά ή αντικυβερνητικά μηνύματα. Δεν είναι λίγες οι περιπτώσεις που οργανισμοί έχουν δει την φήμη τους να πληγώνεται από τέτοιες επιθέσεις. Μεγάλες εταιρίες, κυβερνητικοί οργανισμοί, στρατιωτικά προγράμματα είναι οι κύριοι στόχοι.

2.1.2 Επίθεση με Δούρειους Ίππους

Οι Δούρειοι Ίπποι(Trojan horses) είναι προγράμματα που προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Κρύβονται συνήθως σε άλλα προγράμματα, αλλά μπορούν να βρίσκονται και μεμονωμένα. Παράδειγμα Δούρειου Ίππου είναι ο Happy99.exe. Αυτοί αντιπροσωπεύουν ποσοστό 58% του συνόλου των Εργαλείων.

[22] Κομνηνός Θόδωρος, Σπυράκης Παύλος: Ασφάλεια δικτύων και υπολογιστικών συστημάτων, Αθήνα 2002, σελ 50

Ενδεικτικά, αναφέρονται κάποια ποσοστά για Δούρειους Ίππους από έρευνα που έγινε από το CERT/CC: login(56%), telnet(16%), ps(12%).

2.1.3 Επίθεση με «σκουλήκια»

Προγράμματα που δρουν αυτόνομα και «σέρνονται»(έτσι προκύπτει το όνομα «σκουλήκι») σε site εκμεταλλευόμενα τρύπες του συστήματος είναι τα «σκουλήκια» (worms). Σε κάθε site το σκουλήκι δρα αυτόνομα και ανεξάρτητα από τα υπόλοιπα sites που προσπαθεί να «συρθεί». Το πιο χαρακτηριστικό σκουλήκι είναι το Internet Worm που το βράδυ της 2ας Νοεμβρίου 1988, κατάφερε να διασπάσει το Διαδίκτυο στην Αμερική, προκαλώντας αντιδράσεις πανικού σε όλο τον κόσμο.

2.1.4 Επίθεση με Ιούς

Τα γνωστά προγράμματα που προσπαθούν(με πονηρές και συνήθως δόλιες τεχνικές) να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα του συστήματος με διάφορους τρόπους(από τους πιο ανώδυνους, αφήνοντας μία υπογραφή- ίχνος της παρουσίας τους ή πιο επώδυνους, με απώλεια δεδομένων, καταστροφή της διαμόρφωσης- configuration του συστήματος) είναι οι ιοί(viruses). Ένα από τα πιο έγκυρα αντί-ιοικά προγράμματα(το Symantec Norton Antivirus) στην ανανέωση του Μάιου 1999 περιείχε υπογραφές 21753 ιών.

2.1.5 Επίθεση με «Ανιχνευτές»

Οι ανιχνευτές (scanners) δικτυακής κίνησης είναι προγράμματα που χρησιμοποιούνται για τον έλεγχο της ασφάλειας των συστημάτων. Ονομάζονται ανιχνευτές γιατί γνωρίζουν όλα τα πιθανά εξωτερικά σημεία που θα μπορούσε να εκμεταλλευτεί ένας επίδοξος hacker για να προσβάλει την ασφάλεια του συστήματος. Αν και αρχικά δημιουργήθηκαν για χρήση από τους διαχειριστές των συστημάτων, σύντομα έγιναν εργαλεία των hackers για να βρίσκουν πιθανούς στόχους. Τέτοια προγράμματα είναι το ISS, το TCPdump, το Nmap, το SATAN και πολλά άλλα. Το ποσοστό της χρήσης τους είναι 14.3% του συνολικού των εργαλείων.

2.1.6 Επίθεση στο πρωτόκολλο TFTP

Το πρωτόκολλο TFTP(Trivial File Transfer Protocol) σχεδιάστηκε ως πρωτόκολλο για την χωρίς δίσκο εκκίνηση «πελατών»(diskless clients). Ωστόσο, δεν είχε δοθεί αρκετή προσοχή στην πρόσβαση σε συγκεκριμένους καταλόγους του συστήματος με αποτέλεσμα να μπορεί κανείς να αντιγράψει κι άλλα αρχεία, όπως για παράδειγμα, το αρχείο κωδικών πρόσβασης.

2.1.7 Επίθεση στη Δικτυακή Υπηρεσία Πληροφοριών (NIS)

Πρόκειται για την υλοποίηση της Sun Microsystems «Κίτρινων Σελίδων»(Yellow Pages) για κατανεμημένη διαχείριση δικτυακών πληροφοριών(όπως αρχεία κωδικών πρόσβασης, χάρτες του δικτύου κλπ.). Ωστόσο, οι πληροφορίες αυτές περνούσαν πάνω από το δίκτυο και μπορούσε οποιοσδήποτε να τα παρακολουθήσει και να τα υποκλέψει. Το NIS(Network Information Service) αντικαταστάθηκε από το NIS+ (από την Sun Microsystems και πάλι) το οποίο χρησιμοποιεί κρυπτογραφικές μεθόδους για την μεταφορά κάθε είδους ευαίσθητης πληροφορίας.

2.1.8 Επίθεση στο ηλεκτρονικό ταχυδρομείο

Στην κατηγορία αυτή εμπίπτουν προβλήματα που προκύπτουν από την προβληματική χρήση του SMTP. Τέτοια είναι το mail spoofing(απόκρυψη αποστολέα ή αλλαγή διεύθυνσής του), mail bombs(μεγάλος όγκος μηνυμάτων σε συγκεκριμένο παραλήπτη), binmail, mailrace, mail abuse. Μία πιο πρόσφατη τρωτότητα που μπορεί να κατηγοριοποιηθεί κάτω από τον ευρύτερο όρο “mail” είναι και το spamming, η παράνομη χρήση mail relays για την αποστολή μηνυμάτων ακατάλληλου ή αδιάφορου περιεχομένου, σε ένα μεγάλο αριθμό χρηστών.

2.1.9 Επίθεση με «έμπιστους υπολογιστές»

Η υπηρεσία των «έμπιστων υπολογιστών»(trusted hosts) δημιουργήθηκε αρχικά για την ευκολία των χρηστών που είχαν πολλούς λογαριασμούς σε συστήματα και χρειάζονταν άμεση πρόσβαση χωρίς την καθυστέρηση για ταυτοποίηση μέσω κωδικών πρόσβασης. Το πρόβλημα αυτό παρουσιάζεται σε UNIX συστήματα και συγκεκριμένα στα αρχεία

hosts.equiv (πλήρης πρόσβαση από άλλα συστήματα) και .rhosts (πρόσβαση σε λογαριασμό χρήστη που ορίζεται από τον ίδιο το χρήστη).

2.1.10 Επίθεση μέσω διαμόρφωσης (weak configuration)

Επιθέσεις που έχουν καταγραφεί σε αυτή τη κατηγορία οφείλονται σε λάθη και παραλείψεις στη διαμόρφωση του συστήματος και κυρίως στη δικτυακή διαμόρφωση. Σε αυτές τις περιπτώσεις παραμένουν τα αρχικά συνθηματικά(passwords) που δημιουργούνται κατά την εγκατάσταση ενός λογισμικού ή συστήματος και ο διαχειριστής δεν τα αλλάζει. Επίσης μπορεί να παραμείνουν τα αρχικά δικαιώματα προσπέλασης που δεν είναι κατά ανάγκη ασφαλή.

2.1.11 Επίθεση από εύρεση των κωδικών πρόσβασης

Η εύρεση του κωδικού πρόσβασης ενός χρήστη μπορεί να γίνει με αρκετούς τρόπους: (i) αντιγραφή του αρχείου κωδικών (password file) και μετέπειτα επεξεργασία αυτού(14 %), (ii) «σπάσιμο» κωδικών πρόσβασης (password cracking) με χρήση προγραμμάτων που προσπαθούν να μαντέψουν passwords κωδικοποιώντας συνήθεις λέξεις(10%), (iii) «αδύνατοι κωδικοί» (weak passwords) που μπορεί εύκολα να βρει κανείς γνωρίζοντας το πρόσωπο στο οποίο ανήκει ο λογαριασμός(χρήση του ονόματος, διεύθυνσης, τηλεφώνου κλπ.)(4%). Η τρωτότητα των κωδικών πρόσβασης(password vulnerabilities) είναι η πιο συχνή μορφή παραβίασης της πρόσβασης(ποσοστό 22%).

2.1.12 Επίθεση με «σπαστήρια» κωδικών

Τα «σπαστήρια κωδικών» (password cracks) είναι προγράμματα τα οποία με είσοδο ένα αρχείο κωδικών πρόσβασης(password file) και με χρήση ενός λεξικού συνηθισμένων λέξεων που χρησιμοποιούνται για κωδικοί, προσπαθούν να ανακαλύψουν όσο το δυνατό περισσότερους κωδικούς για πρόσβαση σε κάποιο σύστημα. Ενδεικτικά αναφέρεται ότι σε ένα UNIX σύστημα 1000 περίπου χρηστών, και υποθέτοντας ότι οι χρήστες δεν έχουν συμβουλευτεί να επιλέγουν δύσκολους κωδικούς(συνήθως συνδυασμό γραμμάτων, αριθμών και σημείων στίξης), ένα «σπαστήρι» μπορεί να ανακαλύψει εύκολα ένα ποσοστό 40% των συνολικών κωδικών. Τα προγράμματα αυτά χρησιμοποιούν και οι διαχειριστές συστημάτων για να προλάβουν παρόμοιες ενέργειες από hackers.

2.1.13 Επίθεση με «ωτακουστές»

Οι «Ωτακουστές» πακέτων(packet sniffers) είναι προγράμματα που μπορούν να παρακολουθούν(«ακούν», ή «μυρίζουν» - sniff) την κίνηση του δικτύου σε επίπεδο IP πακέτων. Με κατάλληλες τεχνικές, έχουν την δυνατότητα να ανακατασκευάσουν τα μηνύματα και να κάνουν αναγνώριση των πρωτοκόλλων που περνούν πάνω από το δίκτυο. Οι sniffers τρέχουν συνήθως σε τοπικά δίκτυα(Ethernet) και «κλέβουν» κωδικούς πρόσβασης ή παρακολουθούν τις πληκτρολογήσεις από συγκεκριμένους σταθμούς εργασίας. Με κατάλληλους μηχανισμούς ανασυνθέτουν τα πακέτα που μπορεί να έχουν χρήσιμη πληροφορία(κωδικούς πρόσβασης, αρχεία, κλπ) χωρίς όμως να επηρεάζουν το περιεχόμενό τους(ανάγνωση μόνο). Τα γεγονότα που αφορούν sniffers ανταποκρίνονται σε ένα ποσοστό 31% του συνόλου των εργαλείων. Ο τρόπος επίθεσης με αυτούς δείχνει μία κλιμάκωση στον τρόπο δράσης: ξεκινά από απλή ανίχνευση του στόχου κι αφού εντοπίσει παραλείψεις στην ασφάλεια, εισβάλλει, σβήνει τα ίχνη, αποδυναμώνει την άμυνα του συστήματος(NIS, FTP, sendmail) και εγκαθιστά Trojans για την εξάπλωσή του. Η χρήση των sniffers αν και μπορεί να έχει θετικά αποτελέσματα για την διαχείριση δικτύου και υπολογιστικών συστημάτων(εντοπισμός bottlenecks, άχρηστης πληροφορίας που μεταδίδεται κλπ.) στα χέρια των hackers μπορεί να έχει καταστροφικά αποτελέσματα. Η χρήση ενός sniffer απαιτεί προνόμια διαχειριστή(superuser privileges), αλλά σήμερα, ο καθένας είναι «διαχειριστής» του προσωπικού του συστήματος και μάλιστα με σύνδεση στο διαδίκτυο. Για τον λόγο αυτό, η ασφάλεια από τα sniffers θα πρέπει να εξασφαλίζεται στο επίπεδο παρόχου υπηρεσιών δικτύου(ISP).

2.1.14 Επίθεση με πλαστογράφηση της IP διεύθυνσης

Η τεχνική αυτή βασίζεται στη δυνατότητα την οποία μπορεί να έχει ένας κόμβος να ισχυρίζεται πως έχει την IP διεύθυνση ενός άλλου. Από την στιγμή που πολλά συστήματα(όπως για παράδειγμα οι access lists σε δρομολογητές) ορίζουν ποια πακέτα επιτρέπονται και ποια όχι να εισέλθουν σε ένα δίκτυο ανάλογα με την IP διεύθυνση του αποστολέα, αυτή είναι μία χρήσιμη τεχνική σε έναν hacker. Με τον τρόπο αυτό είναι δυνατό να διασφαλίσει την προσπέλαση σε υπηρεσίες που επιτρέπονται σε κόμβους με συγκεκριμένες IP διευθύνσεις. Επίσης μπορεί να σταλεί

από ένα εξωτερικό δίκτυο ένα πακέτο δεδομένων που να φαίνεται πως έχει σταλεί από εσωτερικό κόμβο ενός προφυλαγμένου δικτύου, δίνοντας έτσι την δυνατότητα να εκτελεστούν εντολές, που επιτρέπονται να εκτελεστούν μόνο από εσωτερικούς κόμβους.

Η πλαστογράφηση της IP διεύθυνσης(IP spoofing) είναι μία νέα (σχετικά) τεχνική επίθεσης σε δικτυωμένους υπολογιστές. Αν και η πιθανότητα τέτοιας επίθεσης είχε προβλεφθεί από το 1989 από τον Steve Bellovin, μόνο από τις αρχές του 1995 άρχισε να χρησιμοποιείται από τους hackers.

Προκειμένου να αποκτήσουν πρόσβαση, οι εισβολείς δημιουργούν πακέτα με ψεύτικες IP διευθύνσεις. Αυτό εκμεταλλεύεται τις εφαρμογές που χρησιμοποιούν ταυτοποίηση(authentication)που βασίζεται στην IP διεύθυνση του αποστολέα και μπορεί να οδηγήσει ακόμα και στην απόκτηση πρόσβασης διαχειριστή στο σύστημα στόχο(για παράδειγμα στις περιπτώσεις χρήσης του/etc/hosts.equiv ή .rhosts). Οι επιθέσεις αυτές μπορούν να αποτραπούν από firewalls που ελέγχουν τις διευθύνσεις πριν μπουν στο τοπικό, έμπιστο(trusted) δίκτυο.

Οι επιθέσεις τύπου “IP spoofing” είναι γενικά δύσκολο να εντοπιστούν, αφού η πρώτη εντύπωση είναι ότι η επίθεση έχει προέλθει από την πλαστή διεύθυνση. Η επαλήθευση συνήθως αργεί, επιτρέποντας στον hacker να δρα ανενόχλητος για κάποιο διάστημα. Η πιο επαρκής «θεραπεία» είναι η χρήση δρομολογητών που έχουν κατάλληλα διαμορφωθεί ώστε να αποτρέπουν είσοδο πακέτων από το εξωτερικό interface με εσωτερικές διευθύνσεις του δικτύου του(δρώντας ως φίλτρο εισόδου).

2.1.15 Επίθεση με «πειρατεία» IP σύνδεσης

Με αυτή την επίθεση που είναι σύνθετη και που περιγράφηκε πρώτα από τον Steve Bellovin, ένας hacker μπορεί να καταλάβει την σύνδεση ενός χρήστη με έναν εξυπηρετητή(γνωστή και σαν man in the middle) και να εκτελεί εντολές που έχει δικαίωμα ο χρήστης. Επιπλέον μπορεί να βλέπει τι γράφει ο χρήστης. Για παράδειγμα αν ο χρήστης γράφει ένα mail τότε ο hacker μπορεί να διαβάσει το mail του, ενώ αν στέλνει στοιχεία της πιστωτικής του κάρτας μπορεί να τα δει. Αρχική Αντιμετώπιση: Με την δημιουργία κωδικοποιημένης σύνδεσης του χρήστη με τον εξυπηρετητή,

μπορούμε να εμποδίσουμε το διάβασμα των στοιχείων, δεδομένων ή εντολών καθώς και την χρήση της σύνδεσης από τον hacker που μη έχοντας το κλειδί κρυπτογράφησης του χρήστη βλέπει μόνο «σκουπίδια».

2.1.16 Επίθεση με υπερχείλιση προσωρινής μνήμης

Μερικές φορές οι hackers εισβάλουν σε συστήματα χωρίς να χρειάζεται να κάνουν login σε αυτά. Αντίθετα χρησιμοποιούν ένα πρόγραμμα που ήδη υπάρχει στον υπολογιστή και τρέχει στο σύστημα και του δίνουν να εκτελέσει ένα κομμάτι εντολών. Για να το πετύχουν αυτό φτιάχνουν ένα μεγάλο τμήμα από χαρακτήρες που περιέχει τις εντολές που θέλουν να εκτελεστούν, και το εισάγουν σαν παράμετρο εισόδου στο πρόγραμμα. Κανονικά το πρόγραμμα δεν εκτελεί τον κώδικα που περνά σαν παράμετρος. Αν όμως το μήκος του κειμένου της παραμέτρου είναι μεγαλύτερο από το μήκος που έχει δοθεί σαν χώρος(buffer) για το πέρασμα της παραμέτρου, τότε μέρος του περνά στον χώρο του εκτελέσιμου προγράμματος και εκτελείται(Buffer overflow).

2.1.17 Επίθεση μέσω άρνησης παροχής υπηρεσιών (DoS)

Οι επιθέσεις αυτού του τύπου είναι οι πιο μοχθηρές και πιο δύσκολο να αντιμετωπισθούν. Είναι οι πιο μοχθηρές γιατί είναι εύκολο να γίνουν, δύσκολο(μερικές φορές αδύνατο) να εντοπισθούν και το χειρότερο δεν μπορείς να αρνηθείς την υπηρεσία στον επιτιθέμενο χωρίς να κάνεις το ίδιο στις γνήσιες αιτήσεις για την υπηρεσία, από κανονικούς χρήστες. Η μεθοδολογία της DoS(Denial of Service) επίθεσης είναι απλή: αν σταλούν σε έναν εξυπηρετητή, περισσότερες αιτήσεις από όσες μπορεί να εξυπηρετήσει τότε οι λειτουργίες που επιβάλλουν οι αιτήσεις αυτές, δεσμεύουν πόρους του συστήματος με αποτέλεσμα, μετά από κάποιο σύντομο χρονικό διάστημα, το σύστημα να μην είναι σε θέση να εξυπηρετήσει τους χρήστες και να μη μπορεί να παρέχει αρκετούς πόρους για την εκτέλεση διεργασιών. Παράδειγμα αποτελεί το mail spam, η επαναλαμβανόμενη δηλαδή αποστολή μηνυμάτων προκειμένου να φτάσει το σύστημα στα όρια της χωρητικότητάς του.

2.1.18 Επίθεση με «μοχθηρό κώδικα» (Malicious Code)

Πρόκειται για εντολές οι οποίες δείχνουν να ξεκινούν διαδικασίες χρηστών, αλλά στην πραγματικότητα προσπαθούν να μαζέψουν ή να εκμεταλλευτούν ευαίσθητα δεδομένα(password files). Για παράδειγμα

στην κατηγορία αυτή μπορούν να ενταχθούν οι προσπάθειες για σύνδεση μέσω του προγράμματος login, μέσω συνδέσεων http και telnet.

2.1.19 Επίθεση με εκμετάλλευση κοινωνικών σχέσεων

Οι hackers πολλές φορές προσπαθούν να βρουν στοιχεία που θα τους επιτρέψουν να εισβάλουν στο σύστημα χρησιμοποιώντας τις κοινωνικές σχέσεις και παριστάνοντας πως είναι κάποιοι άλλοι(Social Engineering).Αυτό το είδος της αναζήτησης πληροφοριών μπορεί να γίνει σε μεγάλους οργανισμούς που οι υπάλληλοι δεν γνωρίζονται μεταξύ τους. Για παράδειγμα μπορούν να παραστήσουν πως είναι νέοι τεχνικοί ή σύμβουλοι ασφάλειας που χρειάζονται ένα password για να φτιάξουν κάτι. Υπολογίζεται πως το 20% των εισβολών προέρχεται από πληροφορίες από social engineering. Σε μία περίπτωση έχει αναφερθεί πως ο hacker κατάφερε να πάρει πληροφορίες και Passwords, μοιράζοντας leaflets σε μία εταιρία για την αλλαγή του τηλεφώνου του help desk. Μόνο που το τηλέφωνο ήταν του σπιτιού του!

2.1.20 Άλλα είδη επιθέσεων είναι:

α**.** Επίθεση στο πρωτόκολλο μεταφοράς αρχείων (FTP)

β. Επίθεση στο σύστημα Δικτυακής αρχειοθέτησης (NFS)

γ. Επίθεση στο πρωτόκολλο ηλεκτρονικού ταχυδρομείου(SMTP)

δ. Επίθεση στην υπηρεσία ονοματολογίας(DNS)

ε. Επίθεση με παραποίηση IP διεύθυνσης

στ. Κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών(DDoS)

ΚΕΦΑΛΑΙΟ 3^{ο}

3. ΑΣΦΑΛΕΙΑ ΣΤΟ CLOUD COMPUTING ΚΑΙ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ

Οι κίνδυνοι που προσιδιάζουν στο υπολογιστικό νέφος σχετίζονται με τα θέματα πολυμίσθωσης και κοινόχρηστου χαρακτήρα των πόρων του υπολογιστικού νέφους(αυτό σημαίνει ότι η ίδια φυσική υποδομή θα εξυπηρετεί πολλούς διαφορετικούς πελάτες ενός παρόχου υπηρεσιών

υπολογιστικού νέφους). Στο υπολογιστικό νέφος ο πελάτης εκχωρεί σε κάποιο βαθμό τον έλεγχο της ασφάλειας στον φορέα παροχής υπηρεσιών πράγμα που καθιστά σημαντικό να είναι σε θέση να εκτιμήσει εάν ο πάροχος των υπηρεσιών υπολογιστικού νέφους συμμορφώνεται με τις απαιτήσεις ασφαλείας. Αυτό καταδεικνύει ότι τα συστήματα πιστοποίησης θα διαδραματίσουν σημαντικό ρόλο επειδή θα βοηθήσουν τους παρόχους να δώσουν αξιόπιστο σήμα ότι συμμορφώνονται προς τα προβλεπόμενα στους μελλοντικούς χρήστες. Από την άλλη πλευρά, για όσους δεν είναι εμπειρογνώμονες ΤΠ σε θέματα ασφάλειας, το να αφεθούν τα θέματα ασφάλειας στα χέρια των επαγγελματιών που εργάζονται για τον πάροχο υπηρεσιών υπολογιστικού νέφους θα μπορούσε να έχει ως αποτέλεσμα να αυξηθεί στην πραγματικότητα η ασφάλεια.[23]

Οι περισσότερες επιχειρήσεις, όπως έχει αποδειχθεί κάνουν χρήση των cloud υπηρεσιών με στόχο το ελάχιστο κόστος.[24] Αυτό πραγματοποιείται κατά κύριο λόγο μέσω της χρονικής μίσθωσης. Οι επιχειρήσεις χρησιμοποιώντας τις cloud υπηρεσίες επιτυγχάνουν τη φθηνότερη λύση για αποθήκευση, ωστόσο προκύπτουν προβληματισμοί οι οποίοι εστιάζουν στο κατά πόσο η αποθήκευση δεδομένων σε μια υπηρεσία cloud είναι εξίσου ασφαλής με την αποθήκευση δεδομένων και πληροφοριών στο εσωτερικό των επιχειρήσεων.[25]

Οι περισσότεροι προβληματισμοί γύρω από το θέμα της ασφάλειας είναι απόρροια της έλλειψης δομής του χρήστη ή της επιχείρησης. Πολλές από τις επιχειρήσεις που κάνουν χρήση των υπηρεσιών Cloud δεν γνωρίζουν ούτε τον χώρο που αποθηκεύουν τις πληροφορίες τους, ούτε με ποιο τρόπο αυτά τα δεδομένα προστατεύονται.

Σημαντικό επίσης ζήτημα θεωρείται το κατά πόσο παρέχουν ασφάλεια τα προγράμματα περιήγησης. Σε ένα Υπολογιστικό Νέφος οι υπολογισμοί γίνονται σε απομακρυσμένους servers και ο περιφερειακός υπολογιστής χρησιμοποιείται αποκλειστικά για την μεταβίβαση των πληροφοριών(I/O) και την πιστοποίηση των εντολών που εκτελούνται

[23] http://europa.eu/rapid/press-release: Ευρωπαϊκή Επιτροπή, 2013, σελ 3
[24] Ηλιοπούλου Σοφία:Cloud Computing,2014,σελ 43
[25] http://www.economist.com/topics/cloud computing

στο Νέφος. Επομένως τα τυπικά προγράμματα περιήγησης είχαν την ανάγκη να στείλουν I/O και αυτοί χρησιμοποιήθηκαν με διάφορα ονόματα όπως:εφαρμογές δικτύου, «web 2.0» ή SaaS. Παρόλα αυτά η χρήση των προγραμμάτων περιήγησης δημιούργησαν την αμφιβολία της ασφάλειας. Το TLS(Transport Layer Security – Ασφάλεια Μεταφοράς σε Επίπεδα) είναι σημαντικό σε αυτό το ζήτημα μιας και χρησιμοποιείται ευρέως για πιστοποίηση και κρυπτογράφηση δεδομένων.

Το θέμα ασφάλειας στις Cloud υπηρεσίες για να γίνει κατανοητό θα πρέπει να γίνει ιδιαίτερη νύξη στη σχέση και την αλληλοεξάρτηση μεταξύ των μοντέλων του Cloud.

Ο έλεγχος της ασφάλειας στις υπηρεσίες Cloud και σε ένα πληροφοριακό σύστημα πραγματοποιείται με τον ίδιο τρόπο. Λόγω όμως της διαφορετικής τεχνολογίας, των διαφορετικών μοντέλων υπηρεσίας και των λειτουργικών μοντέλων, προκύπτουν διαφορετικά ρίσκα για την επιχείρηση ή έναν οργανισμό κάνοντας χρήση των υπηρεσιών cloud(Cloud Security Alliance, 2009).

Επίσης, εξίσου σημαντικοί παράγοντες για την ασφάλεια ενός «Νέφους» είναι εκείνοι που αφορούν τον τομέα της Διακυβέρνησης και τον τομέα των Επιχειρήσεων.

3.1.Τομέας Διακυβέρνησης

α. Νομική και ηλεκτρονική κάλυψη

Αφορά νομικά ζητήματα όπως: προστασία πληροφοριών και υπολογιστικών συστημάτων, παραβιάσεις ασφάλειας, απαιτήσεις απορρήτου, διεθνείς νόμους κλπ.

β. Συμβατότητα και Λογιστικός Έλεγχος

Παρέχει συμβατότητα όταν η επιχείρηση μεταβαίνει σε cloud υπηρεσίες

γ. Φορητότητα και Διαλειτουργικότητα

Αφορά τη μεταφορά δεδομένων από έναν πάροχο σε έναν άλλο και την επιστροφή αυτών στην επιχείρηση

3.2.Τομέας επιχειρηματικός

α. Ασφάλεια εφαρμογών

Το κομμάτι αυτό εστιάζει στην ασφάλιση του λογισμικού εφαρμογών που τρέχουν ή αναπτύσσονται εντός του Νέφους. Αυτό περιλαμβάνει την επιλογή αν μια επιχείρηση θα μεταβεί σε υπηρεσίες Νέφους και, αν ναι, το πιο μοντέλο να υιοθετήσει(IaaS, PaaS ή SaaS).

β. Παραδοσιακή ασφάλεια, επιχειρησιακή συνοχή και ανάκτηση πληροφοριών

Λαμβάνει υπόψη του τον τρόπο που οι χρησιμοποιούμενες λειτουργικές διαδικασίες στην εφαρμογή ασφάλειας επηρεάζονται από το Cloud Computing. Αυτό το κομμάτι επίσης εστιάζει στα ρίσκα που λαμβάνονται από τις υπηρεσίες Νέφους συναρτήσει με τις προσδοκίες της επιχείρησης για καλύτερη διαχείριση του ρίσκου.

3.3 Μελέτη περίπτωσης

Η παρούσα αναφορά[26] σχετική με το θέμα που θα αναπτυχθεί εκτενώς παρακάτω στην εργασία μου ,κάνει λόγο για το ότι τα Big Data είναι μια τεχνολογία που αναπτύσσεται με ταχύ ρυθμό στον τομέα των τηλεπικοινωνιών, και ειδικά στον σύγχρονο τομέα των ασύρματων τηλεπικοινωνιών. Μια ακόμη τεχνολογία που αναπτύσσεται ταχύτατα στον τομέα των ασύρματων τηλεπικοινωνιών και εξετάζεται στην εργασία είναι η «Υπολογιστική Νέφους» ή, όπως είναι ευρέως γνωστή, Cloud Computing(CC).Εξετάζοντας εν συντομία τι είναι Big Data, διαπιστώνουμε πως είναι ένας νέος δημοφιλής όρος, που χρησιμοποιείται για να περιγράψει την εκπληκτικά ταχεία αύξηση του όγκου των δεδομένων. Ειδικότερα, είναι ένας ευρύς όρος που αναφέρεται σε σύνολα δεδομένων τόσο μεγάλα ή πολύπλοκα που οι παραδοσιακές εφαρμογές επεξεργασίας των δεδομένων είναι ανεπαρκείς. Η ακρίβεια της τεχνολογίας των Big Data μπορεί έτσι να οδηγήσει σε πιο σίγουρη λήψη αποφάσεων και οι καλύτερες αποφάσεις μπορούν να οδηγήσουν σε μεγαλύτερη λειτουργική αποτελεσματικότητα, μείωση του κόστους καθώς και μειωμένο κίνδυνο στη διαχείριση των δεδομένων. Τα Big Data είναι πλέον σημαντικά για τις επιχειρήσεις αλλά και για το διαδίκτυο

[26] www.researchgate.gr- Ψάννης Κωνσταντίνος , Χρήστος Στεργίου, Αποτελεσματική και Ασφαλής μεταφορά Big Data στο Cloud Computing με έναν αλγόριθμο(=Ιούλιος 2018)

γενικότερα, και αυτό γιατί οι περισσότερες πληροφορίες οδηγούν σε πιο ακριβείς αναλύσεις. Όσον αφορά το Cloud Computing που μας απασχολεί και εν προκειμένω αποτελεί μία νέα γενιά υπηρεσιών που έκανε την εμφάνισή της τα τελευταία χρόνια με σκοπό να προσφέρει τη δυνατότητα παροχής πρόσβασης σε πληροφορίες και δεδομένα από οποιοδήποτε μέρος και οποιαδήποτε ώρα, περιορίζοντας ή εξαλείφοντας έτσι την ανάγκη για υλικοτεχνικό εξοπλισμό. Όπως έχω αναφέρει ήδη και στην εισαγωγή και στον ορισμό της εργασίας το Cloud Computing(=Υπολογιστική Νέφους) ορίζεται ως η χρήση υπολογιστικών πόρων υλικοτεχνικής υποστήριξης, καθώς και λογισμικού μέσω της χρήσης υπηρεσιών που παρέχονται μέσω διαδικτύου. Σήμερα, οι υπηρεσίες του Cloud Computing απαρτίζουν ένα από τα μεγαλύτερα πεδία ανταγωνισμού στον κόσμο μεταξύ κολοσσιαίων εταιρειών στον τομέα της Πληροφορικής, όπως η Google, η Amazon και η Microsoft,οι οποίες αγωνίζονται να πάρουν μία πλεονεκτική θέση, σε αυτήν την ταχέως αναπτυσσόμενη βιομηχανία. Οι δύο τεχνολογίες που προαναφέρθηκαν και οι περισσότερες νέες τεχνολογίες και δη αυτές που σχετίζονται με την αποθήκευση και μεταφορά δεδομένων, αντιμετωπίζουν προβλήματα ασφάλειας και ιδιωτικότητας στη λειτουργία τους. Ο σκοπός της έρευνας που έγινε ήταν η βελτίωση και βελτιστοποίηση των ζητημάτων ιδιωτικότητας και ασφάλειας στη λειτουργία των τεχνολογιών αυτών. Στην εν λόγω έρευνα επιδιώκεται να εξετασθούν οι δύο προαναφερόμενες τεχνολογίες και τα βασικά τους χαρακτηριστικά εστιάζοντας στο κομμάτι της ασφάλειας και προστασίας της ιδιωτικότητας και πιο συγκεκριμένα γίνεται μια προσπάθεια συνδυασμού της λειτουργίας αυτών για την ανακάλυψη των κοινών τους χαρακτηριστικών και οφελών που σχετίζονται με θέματα ασφάλειας κατά την ενοποίηση των τεχνολογιών αυτών. Συνοπτικά η έρευνα αυτή παρουσιάζει μία νέα μέθοδο ενός αλγόριθμου που μπορεί να χρησιμοποιηθεί για τη βελτίωση της ασφάλειας του Cloud Computing μέσω της χρήσης αλγορίθμων που μπορούν να παρέχουν περισσότερη προστασία της ιδιωτικότητας και της ασφάλειας στα δεδομένα που σχετίζονται με την τεχνολογία του Big Data.

3.4 Cloud Security

Η δεύτερη αναφορά[27] στο βιβλίο Cloud Security- second edition(Theory and Practice) ορίζει ότι το σύννεφο υπολογιστών είναι ένα περιβάλλον στόχος για επιθέσεις στα προσωπικά δεδομένα και εγκληματικές οργανώσεις. Η ασφάλεια αποτελεί μείζων θέμα ανησυχίας για τους υπάρχοντες αλλά και για τους πιθανούς νέους χρήστες των υπηρεσιών του Cloud Computing. Το ενδέκατο κεφάλαιο ξεκινά με μία συζήτηση σχετικά με τις ανησυχίες των χρηστών του cloud, οι απειλές της ασφάλειας γίνονται αντιληπτές από τους χρήστες του cloud, και για την ασφάλεια και την εμπιστευτικότητα. Η κρυπτογράφηση προστατεύει τα δεδομένα αποθήκευσης στο cloud και τους παρόχους υπηρεσιών cloud που προσφέρουν υπηρεσίες κρυπτογράφησης. Τα προσωπικά δεδομένα πρέπει να αποκρυπτογραφούνται για επεξεργασία και αυτό προσφέρει ένα παράθυρο ευπάθειας. Οι απειλές στη διάρκεια της επεξεργασίας προερχόμενες από ελαττώματα στους επόπτες (=λογισμικά ελέγχου), στους απατεώνες των VMS ή σε ένα VMBR συζητούνται στη συνέχεια. Μία ανάλυση της ασφάλειας των υπηρεσιών δεδομένων ακολουθείται από μία παρουσίαση της ασφάλειας του λειτουργικού συστήματος, ασφάλειας VM, ασφάλειας της εικονικοποίησης, και μια ανάλυση των κινδύνων για την ασφάλεια που τίθενται από κοινόχρηστες εικόνες και από τη διαχείριση OS. Ο επόπτης Xoar είναι μια εκδοχή Xen σπάζοντας το Μονολιθικό Σχέδιο του TCB(= της αξιόπιστης βάσης υπολογιστών). Ένας αξιόπιστος επόπτης και μία κινητή συσκευή ασφαλείας είναι τα τελευταία θέματα που συζητούνται σε αυτό το Κεφάλαιο.

3.5 Πακέτο λογισμικού που είναι καλύτερο στον τομέα της ασφάλειας

Δυστυχώς το ερώτημα ποιο πακέτο λογισμικού είναι καλύτερο στον τομέα της ασφάλειας, δεν μπορεί να απαντηθεί εύκολα. Κάθε προϊόν έχει τις δυνατότητες και τις αδυναμίες του. Το ιδανικό προϊόν θα έπρεπε να συνδυάζει τις λειτουργίες πολλών διαφορετικών προγραμμάτων. Με όλες τις επιλογές που υπάρχουν σήμερα, είναι διαθέσιμα άφθονα πακέτα προς επιλογή. Ακολουθεί μια συνοπτική περιγραφή των βασικότερων προϊόντων λογισμικού στον τομέα του απομακρυσμένου ελέγχου.[28]

3.5.1 Το pcAnywhere

[27] www.sciencedirect.com- Cloud Security-Second edition-Theory and Practice(Dan C. Marinescu),2018, σελ 405 - 437

[28] Joel Scambray, Stuart McClure, George Kurtz:Χάκερ Επίθεση και Άμυνα, Αθήνα 2001,σελ 515

Το pcAnywhere της Symantec[29] υπήρξε ένα από τα δημοφιλέστερα προγράμματα απομακρυσμένου ελέγχου που κυκλοφορούν στην αγορά, και μεγάλο μέρος της ελκυστικότητάς του οφείλεται στην ασφάλεια. Αν και όλες οι εφαρμογές έχουν τα προβλήματά τους, το pcAnywhere έχει τις πιο ισχυρές λειτουργίες ασφάλειας σε σύγκριση με τα άλλα προϊόντα που κυκλοφορούν στην αγορά. Μεταξύ των λειτουργιών ασφάλειας που διαθέτει το pcAnywhere συγκαταλέγονται οι ακόλουθες:επιβολή "ισχυρών" κωδικών πρόσβασης, εναλλακτικό σχήμα πιστοποίησης, προστατευόμενα με κωδικούς αρχεία διαμόρφωσης/προφίλ, αποσύνδεση των χρηστών με την ολοκλήρωση της κλήσης, κρυπτογράφηση της κυκλοφορίας, περιορισμός των προσπαθειών σύνδεσης και καταγραφή των αποτυχημένων προσπαθειών. Δυστυχώς, όπως και πολλά άλλα προγράμματα, το pcAnywhwere είναι τρωτό στο πρόβλημα της αποκάλυψης κωδικών πρόσβασης.

3.5.2 Το ReachOut

Το ReachOut της Star Electronics[30] είναι ένα ακόμη εύρωστο πρόγραμμα απομακρυσμένου ελέγχου, αλλά έχει λιγότερες λειτουργίες ασφάλειας. Συγκεκριμένα, δε διαθέτει λειτουργίες για την επιβολή ισχυρών κωδικών πρόσβασης, εναλλακτικού σχήματος πιστοποίησης και προστασίας των αρχείων διαμόρφωσης/προφίλ με κωδικούς πρόσβασης. Η απλότητά του δεν είναι καθόλου κακή, δεδομένου ότι το ReachOut ανοίγει μόνο μία θύρα TCP/UDP, την 43188. Η ύπαρξη μόνο μιας ανοικτής θύρας περιορίζει σημαντικά τα σημεία εισόδου πιθανών εισβολέων.

3.5.3 Το Remotely Anywhere

Το Remotely Anywhere[31] είναι νέος παίχτης στην ομάδα, αλλά σίγουρα ο πιο υποσχόμενος. Το πρόγραμμα αυτό παρέχει τις τυπικές λειτουργίες απομακρυσμένου ελέγχου της επιφάνειας εργασίας, αλλά εκεί που πραγματικά υπερέχει είναι η συνολική διαχείριση συστήματος (πέρα από τον απλό απομακρυσμένο έλεγχο).Μεταξύ των τυπικών λειτουργιών απομακρυσμένου ελέγχου, διαθέτει σχεδόν όλες τις διαχειριστικές λειτουργίες των NT μέσω ενός web browser.
Οι χρήστες, οι ομάδες, τα registries, τα αρχεία καταγραφής συμβάντων,

[29] http://www.symantec.com
[30] http://www.stac.com
[31] http://www.remotelyanywhere.com

οι διεργασίες, το εργαλείο προγραμματισμού εργασιών, η λίστα διεργασιών, το λογισμικό διαχείρισης αρχείων, οι μονάδες δίσκων και οι υπηρεσίες είναι στοιχεία τα οποία είναι διαθέσιμα για διαμόρφωση και διαχείριση μέσω web browser. Αυτό σημαίνει ότι δε χρειάζεται καν να καταφύγει κάποιος στο γραφικό περιβάλλον του λειτουργικού συστήματος για να διαχειριστεί ένα σύστημα με NT. Αυτό μπορεί να είναι πολύ καλό ή πολύ κακό, ανάλογα με την θέση από την οποία βλέπει κάποιος τα πράγματα. Το αρνητικό για το Remotely Anywhere είναι ότι όταν οι εισβολείς αναλαμβάνουν τον έλεγχο του συστήματος, δε χρειάζεται πλέον να περιμένουν μέχρι να πάνε στα σπίτια τους οι χρήστες για να εκτελέσουν λειτουργίες στο γραφικό περιβάλλον. Αντίθετα, φορτώνουν απλώς τον δαίμονα και αρχίζουν τη δουλειά τους. Δυστυχώς για το Remotely Anywhere, επί του παρόντος δε διαθέτει μία εναλλακτική μορφή πιστοποίησης από αυτή που χρησιμοποιούν τα NT – πράγμα το οποίο το καθιστά τρωτό στις επιθέσεις, αφού παραβιαστεί το σύστημα. Για να είναι ασφαλής κάποιος όταν χρησιμοποιεί το Remote Anywhere στα συστήματά του μπορεί να ενεργοποιήσει ορισμένες επιλογές ασφάλειας, όπως το κλείδωμα, διευθύνσεων IP .Η λειτουργία αυτή δεν είναι εξαρχής ενεργοποιημένη, αλλά επιτρέπει στο χρήστη να μπλοκάρει τους εισβολείς μετά από έναν συγκεκριμένο αριθμό αποτυχημένων προσπαθειών.

Από την άποψη της διαχείρισης, το Remotely Anywhere είναι ακόμη καλύτερο από τα τυπικά βοηθήματα του γραφικού συστήματος επικοινωνίας με τον χρήστη, όπως και τα User Manager, Event Viewer και REGEDT32, επειδή τα βοηθήματα αυτά λειτουργούν σαν να ήταν τοπικά, απαιτώντας ελάχιστο χρόνο για να ολοκληρωθούν.

Για παράδειγμα, μπορεί να προστεθεί ένας χρήστης και μία ομάδα μέσω της εφαρμογής browser και να τεθούν σε ισχύ άμεσα, αντί να περιμένει το γραφικό περιβάλλον να στείλει εντολές ελέγχου στο σύστημα. Το θετικό είναι ότι το Remotely Anywhere υποστηρίζει πολλές λειτουργίες ασφάλειας και θα πρέπει να χρησιμοποιηθούν όλες:

- Δυνατότητα κρυπτογραφημένης μετάδοσης μέσω SSL στη θύρα 2001
- Φιλτράρισμα διευθύνσεων IP

- Κλείδωμα διευθύνσεων IP
- Ασφαλής πιστοποίηση NTLM

3.5.4 Remotely Possible/ControlIT

Το ControlIT της Computer Associates[32]είναι ένα πολύ γνωστό και συχνά χρησιμοποιούμενο προϊόν, αλλά στον τομέα της ασφάλειας παρέχει τις λιγότερες δυνατότητες. Πέρα από τα αρχικά προβλήματα του προϊόντος (μη κρυπτογραφημένα ονόματα χρήστη/ κωδικοί πρόσβασης), ακόμη και η πιο πρόσφατη έκδοση χρησιμοποιεί ένα αδύναμο σχήμα κρυπτογράφησης για τους κωδικούς πρόσβασης, αφήνοντάς τους ανοικτούς σε επιθέσεις. Δε διαθέτει δυνατότητες επιβολής "ισχυρών" κωδικών πρόσβασης και προστασίας των αρχείων διαμόρφωσης/προφίλ με κωδικούς πρόσβασης, και δε διαθέτει επίσης λειτουργία καταγραφής των αποτυχημένων προσπαθειών σύνδεσης. Τέλος, είναι επίσης τρωτό στο πρόβλημα αποκάλυψης κωδικών πρόσβασης.

3.5.5 Το Timbuktu

Μαζί με το pcAnywhere, το Timbuktu Pro 32 της Netopia[33] είναι ένα ακόμη συχνά χρησιμοποιούμενο πρόγραμμα απομακρυσμένου ελέγχου σε περιβάλλοντα μεγάλων εταιρειών. Παρόμοια με πολλά άλλα προϊόντα της κατηγορίας του, το Timbuktu παρέχει όλες τις γνωστές λειτουργίες απομακρυσμένου ελέγχου, μαζί με ορισμένες επιπλέον. Υποστηρίζει κοινή χρήση οθόνης μεταξύ πολλαπλών χρηστών ταυτόχρονα και ορισμένες ισχυρές λειτουργίες ασφάλειας, όπως ο καθορισμός ελάχιστου μεγέθους για τους κωδικούς πρόσβασης, ο περιορισμός της επαναχρησιμοποίησης των κωδικών πρόσβασης, εναλλακτικό σχήμα πιστοποίησης και λήξη των κωδικών πρόσβασης μετά από ένα καθοριζόμενο χρονικό διάστημα. Αλλά το καλύτερο απ'όλα τα χαρακτηριστικά του είναι ότι το Timbuktu δεν είναι τρωτό στο γνωστό πρόβλημα αποκάλυψης κωδικών πρόσβασης. Συνολικά, το Timbuktu είναι ένα εξαιρετικό πρόγραμμα απομακρυσμένου ελέγχου.

[32] http://www.cai.com
[33] https://www.netopia.com

3.5.6 Το Virtual Network Computing (VNC)

Το Virtual Network Computing αναπτύχθηκε στα εργαστήρια της AT & T (AT & Τα Research Labs, Cambridge, England) και βρίσκεται στη διεύθυνση[34]. Το VNC έχει ορισμένα μοναδικά χαρακτηριστικά, πρώτο εκ των οποίων είναι η ανεξαρτησία του από την πλατφόρμα του υπολογιστή. Το server συστατικό του προϊόντος μπορεί να εγκατασταθεί στα Windows, σε Linux, Solaris, Macintosh και ναι, ακόμη και από συσκευές με τα Windows! Το VNC έχει επίσης ένα σύστημα επικοινωνίας βασιζόμενο στην java, το οποίο μπορεί να εμφανίζεται σε οποιαδήποτε εφαρμογή browser υποστηρίζει την java, όπως το Netscape Communicator και ο Microsoft Internet Explorer. Και το πιο θετικό από όλα αυτά είναι ότι το VNC είναι δωρεάν!

Λόγω της πληθώρας και της ισχύος των λειτουργιών του, δεν αποτελεί έκπληξη το γεγονός ότι η χρήση του VNC θέτει ορισμένες σοβαρές επιπλοκές για την ασφάλεια. Το VNC πέφτει θύμα του προβλήματος αποκάλυψης κωδικών πρόσβασης. Διαπιστώθηκε επίσης το πόσο εύκολο είναι να εγκατασταθεί το VNC στα Windows NT μέσω απομακρυσμένης σύνδεσης δικτύου – το μόνο που χρειάζεται να γίνει είναι η εγκατάσταση της υπηρεσίας VNC μέσω της γραμμής εντολής, αφού γίνει μία και μόνη αλλαγή στο Registry του απομακρυσμένου συστήματος για να διασφαλιστεί ότι η υπηρεσία θα εκκινεί αόρατα.

Φυσικά, το WinVNC.EXE εμφανίζεται στη λίστα διεργασιών, ανεξάρτητα από την έκδοση ή την κατάσταση λειτουργίας. Ωστόσο, το πιο σημαντικό είναι ότι το VNC είναι τρωτό στις ακόλουθες επιθέσεις:

- **Χρήση μεθόδων ωμής δύναμης για την εξεύρεση κωδικών πρόσβασης στο VNC.**Οι αδύναμοι κωδικοί πρόσβασης μπορούν να δώσουν σε έναν εισβολέα τη δυνατότητα να αποκτήσει ολοκληρωτικό έλεγχο του συστήματος στο οποίο τρέχει το server συστατικό του VNC.
- **Υποκλοπή μέσω δικτύου.** Εξ ορισμού , το VNC δε χρησιμοποιεί κάποια μορφή κρυπτογράφησης αφού πιστοποιηθεί ένας χρήστης στο VNC server.

[34] https://www.uk.research.att.com/vnc.

- **Αδύναμο σχήμα κρυπτογράφησης του κωδικού πρόσβασης του WinVNC.** Το WinVnc αποθηκεύει τον κωδικό πρόσβασης του server με ένα αδύνατο σχήμα κρυπτογράφησης, πράγμα το οποίο μπορεί να επιτρέψει σε έναν εισβολέα να αποκαλύψει τον κωδικό πρόσβασης.

ΚΕΦΑΛΑΙΟ 4ο

4. ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

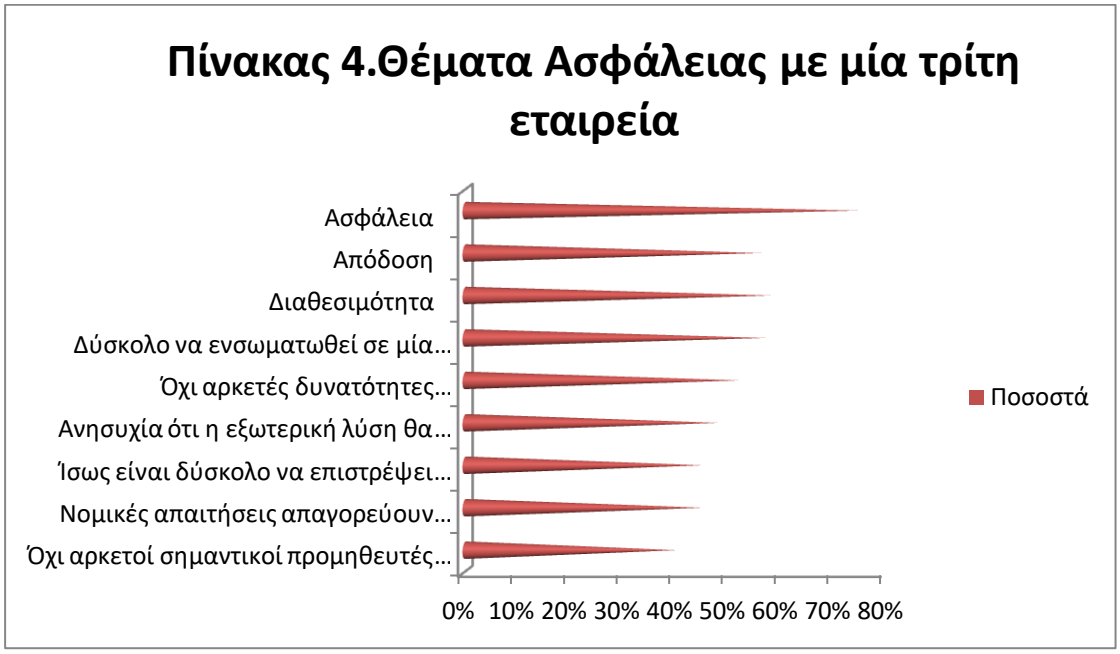
4.1 Ασφάλεια και Προστασία δεδομένων γενικά

Τα δυο από τα μεγαλύτερα και σημαντικότερα θέματα σχετικά με το Υπολογιστικό Νέφος αποτελούν η Ασφάλεια και η Προστασία Δεδομένων. Η ασφάλεια των πληροφοριών είναι ένα πολύπλοκο σύνολο που αποτελείται από τεχνολογίες, κανονισμούς, τεχνικές και συμπεριφορές που προστατεύουν την ακεραιότητα και την πρόσβαση σε συστήματα υπολογιστών και δεδομένων και που στοχεύουν στην υπεράσπιση έναντι των παρεμβολών που προκύπτουν: Από κακόβουλη πρόθεση και εισβολείς όπως για παράδειγμα οι χάκερς αλλά και από ακούσια λάθη του χρήστη. Όταν τα δεδομένα ενός δημόσιου οργανισμού ή μιας εταιρίας αποθηκεύονται στο Νέφος και η ανταλλαγή τους γίνεται μέσω του ιντερνέτ οι υπηρεσίες που στηρίζονται είναι εκτεθειμένες σε εξωτερικές απειλές και διασκορπίζονται σε διάφορες τοποθεσίες. Αυτός είναι και ο λόγος που κάποιες εταιρίες διστάζουν να επωφεληθούν από την χρήση της τεχνολογίας του Υπολογιστικού Νέφους γιατί δεν μπορούν να διατηρούν τις πληροφορίες της εταιρίας τους κάτω από πλήρη έλεγχο. Ο χρήστης παραχωρεί τα δεδομένα και τις πληροφορίες που μπορεί να είναι προσωπικές, απόρρητες και ευαίσθητες και ο πάροχος του Νέφους πρέπει να είναι αξιόπιστος για την συντήρηση και την προστασία αυτών. Δηλαδή οι μηχανισμοί ασφάλειας ανάμεσα στον χρήστη και τον πάροχο πρέπει να είναι ισχυροί και προσεκτικά σχεδιασμένοι.

Οι δύο μεγάλες κατηγορίες που αφορούν θέματα ανησυχίας – ασφάλειας που σχετίζονται με το Υπολογιστικό Νέφος είναι τα ζητήματα ασφάλειας που αντιμετωπίζουν οι πάροχοι του Νέφους και τα θέματα ασφάλειας

που αντιμετωπίζουν οι χρήστες τους. Αυτό γίνεται με δυο τρόπους: Ο πρώτος είναι να εξασφαλίσει ο πάροχος ότι οι υποδομές του είναι ασφαλείς και ότι τα δεδομένα και οι εφαρμογές των πελατών του προστατεύονται και ο δεύτερος είναι ο χρήστης να διασφαλίσει ότι ο πάροχος έχει λάβει τα κατάλληλα μέτρα ασφάλειας για την προστασία των πληροφοριών χρησιμοποιώντας ισχυρούς κωδικούς πρόσβασης και μέτρα ελέγχου ταυτότητας.

Το IDC Μία πραγματοποίησε έρευνα σε 244 ανώτερους υπαλλήλους μηχανογράφησης σχετικά με τις υπηρεσίες «σύννεφου». Όπως δείχνει ο (πίνακας 4) η ασφάλεια με 74,5% είναι η κύρια ανησυχία για το «σύννεφο»[35]



[35] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter: Cloud Computing. Μια πρακτική προσέγγιση, 2010, σελ 35

4.2 Βασικές αρχές της ασφάλειας δεδομένων

Υπάρχουν κάποιες βασικές αρχές ασφάλειας πληροφοριών. Αυτές είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

4.2.1 Εμπιστευτικότητα

Η εμπιστευτικότητα αναφέρεται στην εκούσια ή ακούσια μη εξιουσιοδοτημένη αποκάλυψη περιεχομένου. Ακόμα σχετίζεται και με τις περιοχές των δικαιωμάτων πνευματικής ιδιοκτησίας, ανάλυση κίνησης, διεπαφή , κρυπτογράφηση και καλυμμένα κανάλια.

Η απώλεια της εμπιστευτικότητας μπορεί να συμβεί με ποικίλους τρόπους όπως για παράδειγμα μέσω κακής εφαρμογής δικαιωμάτων διαδικτύου. Υπάρχουν κάποια στοιχεία των τηλεπικοινωνιών που χρησιμοποιούνται για να διασφαλίσουν την εμπιστευτικότητα όπως:

- Τα Πρωτόκολλα ασφάλισης δικτύου
- Οι Υπηρεσίες πιστοποίησης δικτύου
- Οι Υπηρεσίες κρυπτογράφησης δεδομένων
- Τα Δικαιώματα πνευματικής ιδιοκτησίας: περιλαμβάνονται εφευρέσεις, έργα τέχνης, μουσικής και φιλολογίας αλλά και σχεδιασμούς, τα οποία καλύπτονται από νόμους πνευματικής ιδιοκτησίας δηλαδή προστατεύουν πνευματικές δημιουργίες, διπλώματα ευρεσιτεχνίας, όπου και ακούσια οδός επικοινωνίας όπου επιτρέπει την ανταλλαγή πληροφοριών και όπου μπορούν να επιτευχθούν μέσω χρονισμού των μηνυμάτων ή την ακατάλληλη χρήση των μηχανισμών αποθήκευσης.
- Η Ανάλυση κίνησης: είναι η μορφή παραβίασης της εμπιστευτικότητας που μπορεί να πραγματοποιηθεί με την ανάλυση του όγκου, την πηγή αλλά και τον προορισμό της κίνησης του μηνύματος, την ταχύτητα, ακόμη και αν αυτό είναι κωδικοποιημένο. Επίσης η αυξημένη δραστηριότητα μηνυμάτων και υψηλές

εξάρσεις κίνησης μπορεί να υποδηλώνουν ότι υπάρχει κάποιο σημαντικό γεγονός που λαμβάνει χώρα.

- Η Κρυπτογράφηση: περιλαμβάνεται η διαμόρφωση των μηνυμάτων ώστε να είναι δύσκολο να αναγνωριστούν από μη εξιουσιοδοτημένη οντότητα ακόμη και εάν έχουν υποκλαπεί. Επίσης το μέγεθος της προσπάθειας που χρειάζεται για την αποκρυπτογράφηση του μηνύματος σχετίζεται με το πόσο ισχυρό είναι το κλειδί κρυπτογράφησης, την ποιότητα αλλά και δύναμη του αλγόριθμου κρυπτογράφησης.

- Η Διεπαφή: είναι η δυνατότητα μίας οντότητας να χρησιμοποιεί και να συνδέει πληροφορίες που προστατεύονται σε ένα επίπεδο ασφάλειας για να "ξεσκεπάσει" πληροφορίες που προστατεύονται σε ένα πιο υψηλό επίπεδο ασφάλειας.

4.2.2 Ακεραιότητα

Η Ακεραιότητα αναφέρεται στην αξιοπιστία των δεδομένων. Για να υπάρχει ακεραιότητα, τα δεδομένα πρέπει να προστατεύονται από μη εξιουσιοδοτημένη τροποποίηση. Η απώλεια ακεραιότητας μπορεί να συμβεί μέσω εσκεμμένης επίθεσης για αλλαγή των πληροφοριών(για παράδειγμα μία αλλοίωση ιστοσελίδας), ή περισσότερο συχνά, χωρίς πρόθεση(τα δεδομένα αλλοιώνονται κατά λάθος από έναν χειριστή).

Τα στοιχεία που χρησιμοποιούνται για να εξασφαλίσουν την ακεραιότητα είναι:

Οι Υπηρεσίες ανίχνευσης εισβολής

Οι Υπηρεσίες τοίχου προστασίας

Η Διαχείριση ασφάλειας επικοινωνιών

Τέλος, υπάρχουν τρεις αρχές που απαιτούνται για να ικανοποιηθεί η έννοια της ακεραιότητας της πληροφορίας στο σύννεφο:

1. Τα δεδομένα είναι εσωτερικά και εξωτερικά σταθερά
2. Μη εξιουσιοδοτημένες τροποποιήσεις δεν γίνονται σε δεδομένα από εξιουσιοδοτημένο προσωπικό ή επεξεργασίες
3. Δεν γίνονται τροποποιήσεις σε δεδομένα από μη εξιουσιοδοτημένο προσωπικό ή επεξεργασίες

4.2.3 Διαθεσιμότητα

Η διαθεσιμότητα αναφέρεται στην προσβασιμότητα των δεδομένων και διασφαλίζει την έγκαιρη πρόσβαση στα δεδομένα του σύννεφου ή στους πόρους επεξεργασίας του σύννεφου. Ακόμα εγγυάται ότι τα συστήματα λειτουργούν κανονικά όταν χρειάζονται και ότι οι υπηρεσίες ασφαλείας του συστήματος βρίσκονται σε καλή λειτουργική κατάσταση. Τέλος το αντίστροφο της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας είναι η αποκάλυψη, η μετατροπή, και η καταστροφή.

4.3 Οφέλη Ασφάλειας[36]

Στα οφέλη που μπορούν να αποκομίσουν οι επιχειρήσεις από την χρήση των προαναφερθέντων cloud υπηρεσιών, πέρα από την αναφορά στους κινδύνους που μπορούν να προκύψουν από τη χρήση των Cloud υπηρεσιών, θα ήταν σκόπιμο να αναφέρουμε ότι **:**

Είναι σημαντικό το οικονομικό όφελος των επιχειρήσεων που υιοθετούν cloud υπηρεσίες καθώς και οι τύποι μέτρων ασφαλείας που εφαρμόζονται κατά κύριο λόγο είναι φθηνότεροι**.** Επομένως οι επιχειρήσεις επιτυγχάνουν προστασία δεδομένων και κινήσεων με χαμηλό κόστος. Για την επίτευξη της μέγιστης προστασίας γίνεται χρήση αμυντικών μέτρων τα οποία μπορεί να είναι τα ακόλουθα:

- Φίλτρα διακινούμενων πληροφοριών
- Ελλείψεις σε hardware και software

[36] Ηλιοπούλου Σοφία, Cloud Computing, 2014, σελ 47

- Ισχυρή πιστοποίηση
- Υποβοηθούμενες λύσεις διαχείρισης ταυτότητας αναγνώρισης

Από τους μεγάλους παρόχους υπηρεσιών νέφους συχνά προσφέρονται ανοιχτά τυποποιημένα περιβάλλοντα για τη διαχείριση των υπηρεσιών ασφαλείας. Αυτό προσφέρει μια ανοιχτή αγορά υπηρεσιών ασφαλείας, όπου οι πελάτες μπορούν να επιλέξουν αρχικά ή να μεταπηδήσουν σε άλλο πάροχο πιο εύκολα με πολύ χαμηλά λειτουργικά κόστη. Δηλαδή ένας χρήστης μπορεί να έχει στη διάθεσή του τους πόρους που προσφέρονται από έναν πάροχο, πλην τον πόρο παροχής ασφάλειας, και τον πόρο παροχής ασφάλειας να τον αντλούν από άλλο πάροχο επιλέγοντας ανά πάσα στιγμή από μια ανοιχτή αγορά. Επομένως ο χρήστης μπορεί να αυξήσει τον τελευταίο πόρο κατά βούληση, ανάλογα με την εκάστοτε ζήτηση, χωρίς να επηρεάζονται οι υπόλοιποι πόροι του συστήματός του.

Επιπροσθέτως, ένα σημαντικό όφελος είναι η γρήγορη επέκταση των πόρων που υποστηρίζονται από τις Cloud υπηρεσίες. Η επέκταση των πόρων ευνοείται από την εξέλιξη τη τεχνολογίας κάνοντάς τους με αυτό τον τρόπο να μπορούν να ανταποκριθούν στις απαιτήσεις της εκάστοτε επιχείρησης. Οι πάροχοι υπηρεσιών Νέφους διαθέτουν επίσης πόρους και δυνατότητες αναδιανομής τους όπως είναι το φιλτράρισμα πληροφοριών.

Τέλος, για τις περισσότερες επιχειρήσεις η ασφάλεια είναι το πιο σημαντικό ζήτημα που λαμβάνεται υπόψη κατά τη μετάβαση των λειτουργιών τους σε Cloud.

Οι επιλογές τους γίνονται βάση:

- της εμπιστευτικότητας,
- των γενικών οφελών από το Cloud Computing,
- των ρίσκων και των συστάσεων για την ακεραιότητα και την αυθεντικότητα ασφάλειας των πληροφοριών,
- της ασφάλειας των υπηρεσιών που προσφέρει ο πάροχος.

Αυτό οδηγεί τους παρόχους των υπηρεσιών Νέφους να βελτιώσουν την ασφάλεια που προσφέρουν μέσα από τον ανταγωνισμό της αγοράς.

Τα σημαντικότερα οφέλη ασφάλειας των υπηρεσιών Cloud, συνοπτικά, είναι τα εξής:

4.3.1 Οικονομικά Οφέλη

Επειδή τα μέτρα ασφαλείας που εφαρμόζονται στις υπηρεσίες Cloud έχουν χαμηλό κόστος, ο χρήστης μπορεί να κάνει ευκολότερα χρήση των υπηρεσιών αυτών χωρίς ιδιαίτερο κόστος. Τα μέτρα ασφαλείας μπορεί να περιλαμβάνουν φίλτρα για τις διακινούμενες πληροφορίες, ισχυρή πιστοποίηση, λύσεις για τη διαχείριση ταυτότητας αναγνώρισης κλπ. Έτσι προκύπτουν τα εξής οφέλη:

α. Διαχείριση απειλών: ένας απλός καταναλωτής ή μια μικρή επιχείρηση δεν διαθέτει τα μέσα και τους τρόπους για να αντιμετωπίσει τυχών απειλές. Οι πάροχοι των υπηρεσιών Cloud ωστόσο διαθέτουν μπορούν να βρουν τρόπους ακόμα και να αναπτύξουν στρατηγικές διαχείρισης απειλών.

β. Πολλαπλές τοποθεσίες:για την αναπαραγωγή περιεχομένου, οι πάροχοι συντηρούν κάποιους οικονομικούς πόρους κάνοντας έτσι εφικτή την αποφυγή αποτυχιών. Με αυτό τον τρόπο απορρίπτεται οποιαδήποτε ζημιά.

γ. Άμεση ανταπόκριση σε οποιαδήποτε πρόκληση:οι πάροχοι των υπηρεσιών Cloud μπορούν να αναγνωρίσουν άμεσα ένα κακόβουλο λογισμικό και αυτό λόγω της εφαρμογής συστημάτων που τους επιτρέπουν την άμεση ανταπόκριση.

δ. Δίκτυα αιχμής: οι Cloud υπηρεσίες παρέχουν δυνατότητες αποθήκευσης και επεξεργασίας πληροφοριών μέσω προηγμένων τεχνολογιών, προσφέροντας στους χρήστες αξιοπιστία, βελτιωμένη ποιότητα και λιγότερα προβλήματα δικτύου.

4.3.2 Γρήγορη επέκταση πόρων

Οι υποστηριζόμενοι από τις υπηρεσίες cloud πόροι (αποθήκευση, επεξεργασία δεδομένων, μνήμη, χρήση εικονικών μηνυμάτων, υπηρεσίες δικτύου), έχουν τη δυνατότητα να επεκταθούν γρήγορα υποβοηθούμενοι και από την διαρκή εξέλιξη της τεχνολογίας. Οι πάροχοι διαθέτουν αρκετούς πόρους και δυνατότητα αναδιανομής τους, προκειμένου να αυξήσουν τα μέτρα ασφαλείας όταν πρόκειται να πραγματοποιηθεί

πιθανή «επίθεση». Με αυτόν τον τρόπο μπορούν να περιοριστούν οι επιθέσεις και οι επιπτώσεις που αυτές επιφέρουν, χρησιμοποιώντας συνδυαστικά την ευέλικτη αναδιανομή των πόρων και την κατάλληλη μέθοδο βελτιστοποίησης των πόρων.

4.3.3 Συγκέντρωση των πόρων

Η συγκέντρωση των πόρων έχει αρκετά πλεονεκτήματα πέρα από κάποια μειονεκτήματα. Θεωρώντας την ύπαρξη ικανοποιητικών μέτρων ασφαλείας δεδομένη, η συγκέντρωση των πόρων πλεονεκτεί στη φθηνότερη παραμετροποίηση και στο φθηνότερο έλεγχο πρόσβασης ανά μονάδα πόρου, στη φθηνότερη εφαρμογή ολοκληρωμένης πολιτικής ασφάλειας και ελέγχου πάνω στη διαχείριση δεδομένων και στη διαχείριση περιστατικών, όπως επίσης και φθηνότερες διαδικασίες συντήρησης.

4.3.4 Αναβαθμίσεις και προεπιλογές

Με τις τελευταίες εκδόσεις και ρυθμίσεις ασφαλείας στο Cloud Computing οι εικόνες των εικονικών μηχανών και το software που χρησιμοποιείται από τους πελάτες μπορεί να αναβαθμιστεί. Παράλληλα με αυτό οι υπηρεσίες IaaS προσφέρουν περιβάλλοντα προγραμμάτων τα οποία παρέχουν τη δυνατότητα λήψης φωτογραφίας από το εικονικό περιβάλλον και να συγκρίνεται με το αρχικό. Οι αναβαθμίσεις πολλές φορές λαμβάνουν χώρα πιο γρήγορα πάνω στη πλατφόρμα. Αυτά είναι όλα τα οφέλη που αφορούν τη βελτίωση της ασφάλειας.

ΚΕΦΑΛΑΙΟ 5ο

5.ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΩΝ ΔΥΝΑΤΟΤΗΤΩΝ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ(CLOUD COMPUTING) ΣΤΗΝ ΕΥΡΩΠΗ

5.1 Στρατηγική της ΕΕ για την αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους[37]

[37] http://europa.eu/rapid/press-release, Ευρωπαϊκή Επιτροπή, 2013, σελ 1

Τα οικονομικά οφέλη είναι πολύ μεγαλύτερα και ανέρχονται σε 160 δισεκατομμύρια ευρώ ετησίως, ήτοι περίπου σε 300 ευρώ κατά κεφαλή ετησίως σε περίπτωση ανάληψης πανευρωπαϊκής δράσης. Σήμερα το συνοθύλευμα διαφορετικών τεχνολογιών σε επίπεδο κρατών μελών αυξάνει την αβεβαιότητα των επιχειρήσεων σχετικά με τις νομικές υποχρεώσεις τους καθυστερώντας τοιουτοτρόπως την υιοθέτηση του υπολογιστικού νέφους. Μολονότι είναι ευπρόσδεκτες οι πρωτοβουλίες στα κράτη μέλη για το υπολογιστικό νέφος, όπως η πρωτοβουλία Andromede στη Γαλλία, το G-Cloud στο Ηνωμένο Βασίλειο και το Trusted Cloud στη Γερμανία, δεν επαρκούν ούτε είναι ο αποτελεσματικότερος τρόπος για να αυξηθεί το μέγεθος της αγοράς επωφελώς για όλους.

5.2 Οφέλη για την οικονομία και την απασχόληση από μια ευρωπαϊκή στρατηγική για το υπολογιστικό νέφος

Από νέες εκτιμήσεις προκύπτει ότι τα έσοδα χάρη στο υπολογιστικό νέφος στην ΕΕ θα μπορούσαν να ανέλθουν σε περίπου 80 δισεκ. Ευρώ μέχρι το 2020, αν επιτύχει η πολιτική παρέμβαση (υπερδιπλασιάζοντας την ανάπτυξη του εν λόγω τομέα). Ως εκ τούτου η εν λόγω στρατηγική αφορά τη δημιουργία ενός νέου κλάδου και τη βελτίωση της ανταγωνιστικότητάς μας έναντι πρωτίστως των Ηνωμένων Πολιτειών. Γενικότερα αναμένονται καθαρά ετήσια κέρδη 160 δισεκ. Ευρώ στο ΑΕΠ της ΕΕ μέχρι το 2020(ήτοι συνολικά κέρδος 600 περίπου δισεκ. Ευρώ μεταξύ 2015 και 2020), εάν υλοποιηθεί πλήρως η στρατηγική της ΕΕ για το υπολογιστικό νέφος. Ειδάλλως, τα οικονομικά οφέλη θα είναι χαμηλότερα κατά δύο τρίτα. Ως επί το πλείστον τα ως άνω οφέλη προέρχονται από τη δυνατότητα των επιχειρήσεων να κάνουν οικονομίες ή να αποκτούν πρόσβαση σε τεχνολογίες που τις καθιστά παραγωγικότερες. Ως προς τη συνολική απασχόληση, αναμένεται δημιουργία 3,8 εκατομμυρίων θέσεων εργασίας μετά την πλήρη εφαρμογή της στρατηγικής έναντι 1,3 εκατομμυρίων, αν δεν αντιμετωπιστούν τα κανονιστικά και άλλα εμπόδια των αντιστοίχως ασκούμενων πολιτικών.

5.3 Ευρωπαϊκή σύμπραξη για το υπολογιστικό νέφος(ECP)και τι θα το κάνει

Η ευρωπαϊκή σύμπραξη για το υπολογιστικό νέφος(ECP) θα αποτελείται από στελέχη υψηλού επιπέδου, αρμόδια για τις προμήθειες δημοσίων ευρωπαϊκών φορέων και καθοριστικής σημασίας παράγοντες του κλάδου της ΤΟ και των τηλεπικοινωνιών. Η ECP, υπό την καθοδήγηση του διοικητικού συμβουλίου της, θα φέρνει σε επαφή τις δημόσιες αρχές προμηθειών και τις κοινοπραξίες του κλάδου με στόχο την υλοποίηση προ- εμπορικών δράσεων για προμήθειες. Αυτό θα επιτρέψει στους ανωτέρω να προσδιορίσουν τις απαιτήσεις του δημόσιου τομέα όσον αφορά το υπολογιστικό νέφος για την ανάπτυξη προδιαγραφών σχετικά με την προμήθεια ΤΟ και να παρέχουν εφαρμογές αναφοράς. Τοιουτοτρόπως θα διευκολυνθεί η στροφή προς κοινή ή από κοινού προμήθεια υπηρεσιών υπολογιστικού νέφους από δημόσιους οργανισμούς βάσει κοινών απαιτήσεων χρήσης. Η ECP δεν αποσκοπεί στη δημιουργία φυσικής υποδομής για το υπολογιστικό νέφος. Αντίθετα, μέσω των απαιτήσεων που θα προωθήσουν τα συμμετέχοντα κράτη μέλη και οι εμπλεκόμενες δημόσιες αρχές με στόχο να επιβληθούν σε όλη την Ευρωπαϊκή Ένωση, στόχος της είναι να εξασφαλιστεί ότι η εμπορική προσφορά υπηρεσιών υπολογιστικού νέφους στην Ευρώπη, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, θα είναι δεόντως προσαρμοσμένη στις ευρωπαϊκές ανάγκες.

5.4 Λειτουργία ευρωπαϊκής σύμπραξης για το υπολογιστικό νέφος(ECP)

Το διοικητικό συμβούλιο θα παρέχει συμβουλές σχετικά με τους στρατηγικούς προσανατολισμούς, ιδίως όσον αφορά την υιοθέτηση από τον δημόσιο τομέα των υπηρεσιών υπολογιστικού νέφους. Το άλλο βασικό συστατικό στοιχείο της ECP είναι το επίπεδο εφαρμογής: Έχει ήδη διατεθεί αρχικός προϋπολογισμός 10 εκατ. Ευρώ για ένα έργο προεμπορικών προμηθειών στη θεματική ενότητα ΤΠΕ του 7^{ου} προγράμματος πλαισίου για την έρευνα. Το έργο αυτό θα απαιτήσει στενή συνεργασία και συστράτευση μεταξύ των επιμέρους φορέων του δημοσίου τομέα στα διάφορα κράτη-μέλη ώστε να παγιωθούν οι απαιτήσεις του δημόσιου τομέα για την προμήθεια και τη χρήση των υπηρεσιών υπολογιστικού νέφους.

5.4.1 Πώς βοηθά η συγκεκριμένη στρατηγική στην άσκηση των δικαιωμάτων μου ως χρήστη των υπηρεσιών του υπολογιστικού νέφους

Μία από τις κύριες δράσεις της συγκεκριμένης στρατηγικής είναι να εκπονηθούν οι όροι και οι προϋποθέσεις μιας πρότυπης σύμβασης στην οποία να αντιμετωπίζονται τα ζητήματα που δεν καλύπτονται από το κοινό ευρωπαϊκό δίκαιο των πωλήσεων, όπως: η διατήρηση των δεδομένων μετά τη λήξη της σύμβασης, η δημοσιοποίηση των δεδομένων και η ακεραιότητα, η τοποθεσία και η μεταφορά των δεδομένων ή η άμεση και η έμμεση ευθύνη. Ο εντοπισμός και η ανάπτυξη συνεκτικών λύσεων στο πεδίο των συμβατικών όρων και προϋποθέσεων αποτελεί μέσον ενθάρρυνσης ευρύτερης εξοικείωσης με τις υπηρεσίες του υπολογιστικού νέφους μέσω της αύξησης της εμπιστοσύνης των καταναλωτών.

5.5 Εξασφάλιση συνεκτικής κανονιστικής ρύθμισης σε παγκόσμιο επίπεδο

Το υπολογιστικό νέφος αποτελεί παγκόσμιο εγχείρημα που προϋποθέτει ενίσχυση του διεθνούς διαλόγου για την ασφαλή και απρόσκοπτη διασυνοριακή χρήση του. Η Ευρωπαϊκή Επιτροπή εργάζεται, μέσω του διεθνούς διαλόγου για το εμπόριο, την επιβολή του νόμου, την ασφάλεια και την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο ώστε να αντιμετωπισθούν πλήρως οι νέες προκλήσεις που προκύπτουν από το υπολογιστικό νέφος. Οι εν λόγω διάλογοι πραγματοποιούνται στο πλαίσιο οργανισμών όπως ο ΠΟΕ και ο ΟΟΣΑ για την προώθηση κοινών στόχων όσον αφορά τις υπηρεσίες πληροφορικής μέσω του υπολογιστικού νέφους, καθώς και σε διμερές επίπεδο με τις ΗΠΑ, την Ιαπωνία και άλλες χώρες.

5.6 Πως μπορώ να γνωρίζω αν τα στοιχεία μου έχουν αποθηκευτεί στην Ευρώπη ή αλλού

Οι όροι και προϋποθέσεις επαφής θα πρέπει να καλύπτουν το ζήτημα της θέσης των δεδομένων. Ωστόσο, οι τυποποιημένες συμβάσεις που ενίοτε επιβάλλονται αναλλοίωτες από πολλούς φορείς παροχής υπηρεσιών υπολογιστικού νέφους σήμερα δεν μπορούν να

περιλαμβάνουν ανάλογες πληροφορίες. Η στρατηγική υπογραμμίζει την ανάγκη να διατυπωθούν πρότυποι συμβατικοί όροι και προϋποθέσεις για την αντιμετώπιση των ζητημάτων που δεν καλύπτονται από το κοινό ευρωπαϊκό δίκαιο των πωλήσεων, όπως, μεταξύ άλλων, τα δεδομένα θέσης.

5.7 Οι συνέπειες με τα δεδομένα αν κλείσει η εταιρεία (που χρησιμοποιώ για την παροχή υπηρεσιών μέσω του υπολογιστικού νέφους.)

Αυτό θα πρέπει κανονικά να καλύπτεται από τους συμβατικούς όρους και τις προϋποθέσεις. Η ανάγκη για σαφέστερη προστασία αποτελεί το λόγο για τον οποίο η Επιτροπή προτίθεται να εκπονήσει πρότυπους συμβατικούς όρους και προϋποθέσεις για την αντιμετώπιση των ζητημάτων που δεν καλύπτονται από το κοινό ευρωπαϊκό δίκαιο των πωλήσεων.

5.8 Διαλειτουργικότητα στα υπολογιστικά νέφη. Αλλαγή παρόχου υπολογιστικού νέφους

Προς το παρόν οι υπηρεσίες που παρέχονται από διαφορετικά υπολογιστικά νέφη δεν είναι όσο διαλειτουργικές θα μπορούσαν. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους μπορεί να χρησιμοποιούν διαφορετικά λειτουργικά συστήματα ή εφαρμογές διεπαφής που δεν είναι διαλειτουργικά, πράγμα που σημαίνει ότι το λογισμικό που έχει διαμορφωθεί για να λειτουργεί με έναν πάροχο υπηρεσιών υπολογιστικού νέφους δεν μπορεί εύκολα να λειτουργήσει με κάποιον άλλο πάροχο. Αυτό θα μπορούσε να οδηγήσει σε εξάρτηση από έναν φορέα παροχής υπηρεσιών δεδομένου ότι δεν είναι απαραίτητα εύκολο να μεταφερθούν τα δεδομένα από το ένα υπολογιστικό νέφος σε κάποιο άλλο(δέσμιος πελάτης).

5.9 Η στρατηγική αντιμετώπιση ευρύτερων θεμάτων ασφάλειας στο υπολογιστικό νέφος

Η στρατηγική δεν ασχολείται με θέματα ασφαλείας που σχετίζονται με το διαδίκτυο και το επιγραμμικό περιβάλλον. Η Επιτροπή θα ασχοληθεί με γενικές προκλήσεις ασφάλειας στον κυβερνοχώρο στη στρατηγική της για την ασφάλεια στον κυβερνοχώρο. Αυτή η μελλοντική στρατηγική θα ασχοληθεί με όλους τους παρόχους

υπηρεσιών της κοινωνίας των πληροφοριών, συμπεριλαμβανομένων των φορέων που παρέχουν υπηρεσίες υπολογιστικού νέφους. Μεταξύ άλλων, θα αναφέρει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα τα οποία θα πρέπει να ληφθούν για να αντιμετωπιστούν οι κίνδυνοι ασφαλείας. Επίσης θα καθιερώσει για τις αρμόδιες αρχές υποχρεώσεις για την υποβολή εκθέσεων όσον αφορά σημαντικά συμβάντα.

5.10 Πως μπορεί να εξελιχθεί το cloud computing

Το cloud computing δέχεται σκληρή κριτική που προέρχεται από πολέμιούς του οι οποίοι το θεωρούν ως μια υπερχρησιμοποιημένη φράση χωρίς πραγματική σημασία.

Πέραν όμως των επικριτών υπάρχουν πολλοί επαγγελματίες που βλέπουν το «σύννεφο» όχι μόνο σαν κάτι χρήσιμο αλλά σαν κάτι που θα εξελιχθεί.

Ερευνητές που ασχολήθηκαν με το cloud computing και το μέλλον του εξέφρασαν ενδιαφέρουσες απόψεις για το μέλλον του, οι οποίες παρατίθενται κατωτέρω:

Ο Plummer είπε ότι συνολικά τρεις τάσεις προς εξέλιξη των cloud αποτελούν τη βάση μιας ασυνέχειας που θα δημιουργήσει μια νέα ευκαιρία για να διαμορφωθεί η σχέση μεταξύ αυτών που χρησιμοποιούν μηχανογραφικές υπηρεσίες και αυτών που τις πουλούν. Στην ουσία αυτό σημαίνει πως οι χρήστες υπηρεσιών σχετικών με την τεχνολογία των πληροφοριών θα είναι σε θέση να εστιάσουν σε αυτά που τους παρέχει η υπηρεσία αντί στο πως υλοποιούνται ή που φιλοξενούνται οι υπηρεσίες.

Όταν είπε ο Plummer «οι επιχειρήσεις περνούν το κατώφλι μεταξύ του internet ως ενός καναλιού επικοινωνίας και της σκόπιμης παράδοσης υπηρεσιών μέσω του internet, τότε αρχίζουμε αληθινά να κατευθυνόμαστε προς μια οικονομία βασισμένη στην κατανάλωση των πάντων, από χώρο αποθήκευσης έως υπολογιστές, έως βίντεο, έως διαχείριση χρηματοδοτήσεων».[38] Η Gartner προέβλεψε τρεις ξεχωριστές αλλά ελαφρώς επικαλυπτόμενες φάσεις εξέλιξης του cloud computing. Η πρώτη φάση έως το 2011, ήταν η φάση των

[38] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter: Cloud Computing: Πρακτική προσέγγιση, Αθήνα 2010, σελ 310

πρωτοπόρων. Η δεύτερη φάση που ήταν από το 2010 έως το 2013 σχετίζονταν με την σταθεροποίηση της αγοράς. Είχε προβλέψει ότι μέχρι το 2012 η αγορά SEAP θα γεμίσει με λύσεις από μεγάλους και μικρούς προμηθευτές ο ανταγωνισμός δε θα οδηγούσε έξω από την αγορά πολλούς αδύναμους φορείς με αποτέλεσμα την εξαγορά εταιρειών. Κατά τη διάρκεια αυτής της φάσης παγίωσης η υποδομή SEAP θα γινόταν πιο ελκυστική σε ένα μεγαλύτερο εύρος πιθανών αγοραστών της με συνέπεια να έχουμε μια πιο έντονη και συντηρητική βάση χρηστών.

Στην τρίτη φάση από το 2012 έως το 2015 και μετά θα φθάσουμε στην κρίσιμη μάζα και θα γίνει εμπορικοποίηση. Ένας μεγάλος αριθμός μεγάλων προμηθευτών SEAP θα εξουσιάζει στην αγορά παρέχοντας de facto πρότυπα. Η επέκταση της αγοράς σε όλο πιο συντηρητικές βάσεις χρηστών θα μετατοπίσει και άλλο την έμφαση της αγοράς από την καινοτομία στη σταθερότητα, το κόστος και την προστασία της επένδυσης.

Η Gartner βλέπει το cloud computing ως ένα στυλ χρήσης υπολογιστών όπου παρέχονται μαζικά κλιμακούμενες υπολογιστικές δυνατότητες χρησιμοποιώντας τεχνολογίες του Διαδικτύου σε πολλαπλούς εξωτερικούς πελάτες.

Προβλέπει ότι ο αντίκτυπος του cloud computing σε προμηθευτές της τεχνολογίας των πληροφοριών θα είναι τεράστιος. Υποστηρίζει ότι το cloud computing είναι μια αναπτυσσόμενη έννοια που θα διαρκέσει πολλά χρόνια για να ωριμάσει πλήρως χωρίς αυτό να σημαίνει ότι το μοντέλο του cloud computing αποτελεί απλώς την επόμενη γενιά του διαδικτύου. Μπορούμε να πούμε[39] ότι το cloud computing είναι στα σπάργανα. Μπορούμε να το φανταστούμε σαν το internet το 1995, που δεν ήταν πολύ γοητευτικό, ήταν κάπως άτεχνο, αλλά ωστόσο χρήσιμο. Καθώς όλο και περισσότεροι άνθρωποι ασχολούνται μαζί του έχει εξελιχθεί και έχει αλλάξει(και θα συνεχίσει έτσι). Να περιμένουμε λοιπόν περισσότερη εξέλιξη στο cloud computing.

[39] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter: Cloud Computing: Πρακτική προσέγγιση, Αθήνα 2010, σελ 314

5.11 Αξιολόγηση κριτηρίων σχετικά με τα προτεινόμενα συστήματα και εφαρμογή αυτών σε τομείς όπως η υγεία, η εκπαίδευση κλπ – Πίνακας Έρευνας[40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51][52]

Κατόπιν μελέτης δεκατριών άρθρων σχετικά με το Cloud Computing πραγματοποιήθηκε αναλυτικός έλεγχος αυτών (=State of art) και ειδικότερα αξιολόγησή τους, βάσει κριτηρίων, μεταξύ των οποίων συμπεριλαμβάνονται (=επίγνωση πλαισίου, αποδοτικότητα, γενίκευση, ιδιωτικότητα κλπ) και είναι τα κάτωθι περιγραφόμενα, σύμφωνα με τα οποία διαμορφώθηκε ο πίνακας έρευνας:

- **Επίγνωση Πλαισίου**

[40] C. Stergiou, K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing…applications: a survey", Wiley, International Journal of Network Management, pp. 1-12, May 2016.
[41] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, vol. 78, part 3,pp. 964-975, January 2018
[42] C. Stergiou, K. E. Psannis, A. P. Plageras, G. Kokkonis, Y. Ishibashi, "Architecture for Security in IoT Environments", in Proceedings of 26th IEEEInternational Symposium on Industrial Electronics, 19 – 21 June 2017, Edinburg, Scotland, UK
[43] A. P. Plageras, C. Stergiou, K. E. Psannis, G. Kokkonis, Y. Ishibashi, Byung-Gyu Kim, Brij Gupta, "Efficient Large-Scale Medical Data…Things", in Proceedings of 19th IEEE International Workshop on the Internet of Things and Smart Services, 24-26 July 2017, Thessaloniki, Greece
[44] A. P. Plageras, K. E. Psannis,C. Stergiou, H. Wang, B. Gupta, "Efficient IoT-based sensor BIG Data...Smart Buildings", Future Generation Computer Systems, vol.82, pp. 349-357, May 2018
[45] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, B.-G. Kim, "Algorithms for efficient digital media..cloud networking", Journal of Multimedia Information System, vol. 5, no.1, pp. 27-34, March 2018
[46] C. Stergiou, K. E. Psannis, A. P. Plageras, T. Xifilidis,B. B. Gupta, "Security and Privacy of Big Data..in Cloud", in Proceedings of IEEE conference on Computer Communications, 15-20 April 2018, Honolulu, HI, USA.
[47] C. Stergiou, K. E. Psannis, B. Gupta, Y. Ishibashi, "Security, Privacy & Efficiency..for Big Data & IoT", Elsevier, Sustainable Computing, Informatics and Systems, vol. 19, pp. 174-184, September 2018
[48] C. Stergiou, A. P. Plageras,K. E. Psannis, T. Xifilidis,G. Kokkonis, S. Kontogiannis, K. Tsarava, A. Sapountzi, "Proposed High Level Architecture…Interactive Classroom", in Proceedings of IEEE conference SEEDA-CECNS M 2018, 22-24 September 2018, Kastoria, Greece
[49] C. Stergiou, K. E. Psannis, B. B. Gupta, "Secure Machine Learning scenario..network", Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications, in Press, 2019
[50] A. P. Plageras, K. E. Psannis, Y. Ishibashi, B.-G. Kim, "IoT-based Surveillance System for Ubiquitous Healthcare", 42nd Annual Conference of the IEEE Industrial Electronics Society, 24/10/2016-27/10/2016
[51] A. P. Plageras, K. E. Psannis, " Algorithms for Big Data Delivery over the Internet of Things", in Proceedings of 19th IEEE Conference on Business Informatics 2017(CBI2017), Doctoral Consortium, 24-26 July 2017, Thessaloniki, Greece
[52] A. P. Plageras, C. Stergiou, K. E. Psannis, Byung-Gyu Kim, Brij Gupta, Y. Ishibashi, "Solutions for Interconnectivity…Smart Hospital Building", in Proceedings of 15th IEEE International Conference on Industrial Informatics(INDIN 2017), 24-26 July 2017, Emden, Germany

Η δυνατότητα του προτεινόμενου συστήματος/πλατφόρμας να κατανοεί το πλαίσιο και να προσαρμόζεται αντίστοιχα (πχ να αντιλαμβάνεται την τοποθεσία του χρήστη)

- **Αποδοτικότητα**

Αποδοτικότητα είναι το πόσο αποτελεσματική είναι η πλατφόρμα στο να λύνει το πρόβλημα για το οποίο σχεδιάστηκε

- **Γενίκευση**

Γενίκευση είναι η ικανότητα του συστήματος να γενικεύεται σε παρόμοια προβλήματα με αυτό που περιγράφεται στο άρθρο

- **Ιδιωτικότητα**

Η ιδιωτικότητα αναφέρεται στην προστασία των προσωπικών δεδομένων, τη μη χρήση τους αν δεν υπάρχει ρητή αποδοχή από το χρήστη κλπ

- **Ασφάλεια**

Η Ασφάλεια έχει να κάνει με τα προσωπικά δεδομένα αλλά δεν περιορίζεται μόνο σε αυτά αλλά καλύπτει κάθε πιθανό κίνδυνο να δεχτεί κακόβουλη επίθεση το σύστημα και να υποστεί δυσλειτουργία

- **Επεκτασιμότητα**

Επεκτασιμότητα είναι η ικανότητα του συστήματος να μεγαλώνει σε αριθμό συνδεδεμένων συσκευών και να αποκτάει πολύ μεγαλύτερο μέγεθος από το αρχικά σχεδιασμένο, διατηρώντας τη λειτουργικότητά του

- **Διαλειτουργικότητα**

Διαλειτουργικότητα είναι η ικανότητα του συστήματος να λειτουργεί σε διαφορετικά περιβάλλοντα / λειτουργικά συστήματα / πρωτόκολλα επικοινωνίας και ανταλλαγής δεδομένων

- **IoT**

Αξιολογείται το κατά πόσο έχει ενσωματωθεί το IoT στο προτεινόμενο σύστημα

- **Cloud Computing**

Αξιολογείται το κατά πόσο έχει ενσωματωθεί το Cloud Computing στο προτεινόμενο σύστημα

- **Εφαρμογή**

Καταγράφεται ο τύπος της εφαρμογής που υποστηρίζει το προτεινόμενο σύστημα

Πίνακας 5: Πίνακας Έρευνας – Αξιολόγηση κριτηρίων

Άρθρο	**Επίγνωση Πλαισίου**	**Αποδοτικότητα**	**Γενίκευση**	**Ιδιωτικότητα**	**Ασφάλεια**	**Επεκτασιμότητα**	**Διαλειτουργικότητα**	**IoT**	**Cloud Computing**	**Εφαρμογή**
Security and Privacy of Big Data for Social Networking Services in Cloud	L	H	L	H	H	M	L	M	H	Social Networks
Algorithms for Big Data Delivery over the Internet of Things	M	M	H	L	L	M	H	H	M	Generic

Efficient IoT-based sensor BIG Data collection-processing and analysis in Smart Buildings	L	M	H	L	M	H	H	H	H	Architecture
Efficient Large-scale Medical Data (eHealth Big Data) Analytics in Internet of Things	M	M	L	M	M	L	L	M	H	Healthcare
Algorithms for efficient digital media transmission over IoT and cloud networking	L	H	H	L	L	H	M	H	H	Architecture
IoT-based Surveillance System for Ubiquitous Healthcare	L	H	L	M	H	H	L	H	H	Healthcare
Secure	L	M	M	L	H	H	H	H	H	Generic

Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network										
Recent advances delivered by mobile cloud computing and Internet of Things for Big data applications: A Survey	L	L	H	H	H	M	H	H	H	Generic
Secure integration of IoT and Cloud Computing	M	L	H	H	H	M	H	H	H	Generic
Architecture for security monitoring in IoT environments	L	M	H	H	H	M	H	H	M	Architecture
Solutions for Inter-connectivity and Security in a	L	M	L	H	H	H	H	H	M	Healthcare

Smart Hospital Building										
Proposed High Level Architecture of a Smart Interconnected Interactive Classroom	L	M	L	L	L	H	H	M	L	Education
Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT	L	L	H	H	H	M	M	H	H	Architecture

ΣΥΜΠΕΡΑΣΜΑ ΑΞΙΟΛΟΓΗΣΗΣ ΚΡΙΤΗΡΙΩΝ

Το συμπέρασμα που συνάγεται από την παραπάνω αξιολόγηση κριτηρίων είναι πως στα συστήματα που προτείνονται στα εν λόγω άρθρα έχουν ενσωματωθεί αρκετά καλά και σε υψηλό βαθμό οι τεχνολογίες IoT και Cloud Computing καθώς μόνο σε ένα από τα άρθρα η ενσωμάτωση του Cloud αξιολογήθηκε χαμηλή. Όσον αφορά τα λοιπά κριτήρια τα συστήματα φαίνεται να ανταποκρίνονται σε όλα εξίσου καλά και ιδίως στον τομέα της ασφάλειας που είναι από τους πιο σημαντικούς καθώς μόνο σε 3 από τα 13 άρθρα η απόδοση στον τομέα της ασφάλειας αξιολογήθηκε χαμηλή. Το μόνο από τα κριτήρια στο οποίο δεν ανταποκρίνονται ικανοποιητικά τα συστήματα αλλά χαμηλά είναι η επίγνωση πλαισίου δηλαδή η δυνατότητα των συστημάτων να κατανοούν το πλαίσιο και να προσαρμόζονται αντίστοιχα.

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

ΑΠΟΡΡΗΤΑ (ΑΡΘ 370Β, 370Γ ΠΚ)

ΚΕΦΑΛΑΙΟ 6^{Ο}

6.Η ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΣΦΑΙΡΑΣ ΤΟΥ ΑΤΟΜΟΥ

Στο Διαδίκτυο η ανάπτυξη τεχνικών Marketing και του ηλεκτρονικού εμπορίου έβαλε σοβαρούς προβληματισμούς για τη δυνατότητα συνύπαρξής τους με την προστασία της ιδιωτικής σφαίρας. Η δημιουργία αρχείων προσωπικών δεδομένων είναι εξαιρετικά εύκολη υπόθεση στο Διαδίκτυο. Πληροφορίες για πελάτες σε ηλεκτρονικά καταστήματα, αλλά και η απλή περιπλάνηση στο internet, γίνονται αντικείμενα συλλογής και ανάλυσης δημιουργώντας πρότυπα καταναλωτών, τα οποία μετά διατίθενται έναντι μεγάλης αμοιβής στους ενδιαφερόμενους. Αλλά και γενικότερα η ευκολία επικοινωνίας με ιδιαίτερα χαμηλό κόστος δύο υπολογιστών, που συχνά βρίσκονται χιλιάδες χιλιόμετρα μακριά καθώς και τα πολύμορφα ηλεκτρονικά fora συζητήσεων, που δεν παρέχουν καμία διασφάλιση του εμπιστευτικού χαρακτήρα των εκεί διοχετευμένων πληροφοριών, πολλαπλασιάζουν τον κίνδυνο παραβίασης της ιδιωτικής σφαίρας του ατόμου. [53]

Πολύ γρήγορα έγινε αντιληπτό στις περισσότερες χώρες της Ευρώπης και της Βόρειας Αμερικής ότι η ιδιωτική σφαίρα του ατόμου έχει ιδιαίτερη αξία που θα πρέπει να τύχει ειδικής προστασίας. Η νομική αντιμετώπιση του ζητήματος ήταν διαφορετική από κράτος σε κράτος, αφού σε άλλες περιπτώσεις κατοχυρώθηκε με διατάξεις του Συντάγματος ή ειδικών νόμων και αλλού η σχετική προστασία επιτεύχθηκε νομολογιακά. Παντού όμως αναγνωρίστηκε το δικαίωμα του ατόμου σε μια ιδιωτική σφαίρα, στην οποία οι πτυχές της ζωής του είναι και θα πρέπει να μείνουν προσωπικές. Εξαιτίας αυτού έγινε νωρίς κατανοητό ότι ο προσωπικός χώρος του ατόμου θα πρέπει να τυγχάνει πάντα ιδιαίτερης προστασίας ιδίως από προσβολές τις οποίες καθιστά δυνατές η διαρκώς αυξανόμενη ανάπτυξη της τεχνολογίας.

[53] Καράκωστας Κ. Ιωάννης : Δίκαιο και Internet. Νομικά ζητήματα του διαδικτύου, Αθήνα 2009, σελ 147

6.1 Ηλεκτρονικό έγκλημα «computer crime»

Αναφορικά με την νέα αυτή κατηγορία εγκλημάτων που προέκυψε στην παγκόσμια κοινότητα με την ανάπτυξη των ηλεκτρονικών υπολογιστών και του Διαδικτύου, έχουν διατυπωθεί κατά διαστήματα πληθώρα ορισμών προκειμένου να περιγράψουν τις νέες και πρωτόγνωρες για το ποινικό δίκαιο εγκληματικές συμπεριφορές.[54] Στην αγγλική γλώσσα χρησιμοποιούνται διάφοροι όροι για να περιγράψουν το ηλεκτρονικό έγκλημα που οι συνηθέστεροι είναι computer – crime, e – crime, high tech – crime, ως γενικότεροι και ακολουθούν οι όροι cyber – crime, internet – crime, internet – related crime, ως ειδικότεροι, καθώς σε αυτή την περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου. Αντίστοιχα στην ελληνική γλώσσα χρησιμοποιούνται αδιακρίτως διάφοροι όροι όπως: έγκλημα υψηλής τεχνολογίας, έγκλημα πληροφορικής, ηλεκτρονικό έγκλημα, έγκλημα που διαπράττεται μέσω η/υ, διαδικτυακό έγκλημα, έγκλημα του κυβερνοχώρου. Οι δύο τελευταίοι όροι περιλαμβάνουν το στοιχείο της δικτύωσης. Συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, φορητές συσκευές(notebooks) κλπ. Οι εν λόγω συσκευές μπορεί είτε να αποτελούν το στόχο κάποιας επίθεσης, είτε το μέσο διάπραξης κάποιας επίθεσης ή κάποιου εγκλήματος.[55]

Το βασικό ζήτημα για το οποίο έχει δημιουργηθεί διχογνωμία στην επιστήμη έγκειται στην ακριβή σημασία του όρου «ηλεκτρονικό έγκλημα» και κυρίως στη διάκρισή του από το «κυβερνοέγκλημα».

Δεν ανταποκρίνεται στην πραγματικότητα η άποψη ότι το έγκλημα στον Κυβερνοχώρο(cyber crimes) αποτελεί τον ίδιο τύπο εγκλήματος με το «**κοινό**» ή «**συμβατικό έγκλημα**» και η μόνη διαφορά που το διακρίνει απ'αυτό είναι ότι διαπράττεται σε διαφορετικό περιβάλλον δηλ σε ηλεκτρονικό περιβάλλον και μάλιστα σε περιβάλλον διαδικτύου. Υπάρχουν εγκλήματα που διαπράττονται τόσο σε κοινό όσο και σε ηλεκτρονικό περιβάλλον, ενώ άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών χωρίς δηλαδή να υπάρχει

[54] Γκότση Μαρίνα: Το ηλεκτρονικό έγκλημα στην Ελληνική έννομη τάξη……., Θεσ/νίκη 2008, σελ 49

[55] Δημητρίου Δήμητρα:Επιθέσεις κατά συστημάτων πληροφοριών. Το Διεθνές Ενωσιακό και Ελληνικό πλαίσιο προστασίας, Θεσ/νίκη 2014, σελ 7

σύνδεση των υπολογιστών με το διαδίκτυο(ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται). Μία άλλη τέλος κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικά στο περιβάλλον του κυβερνοχώρου.

Αξιοσημείωτη είναι σύμφωνα με τα ανωτέρω η διάκριση του ηλεκτρονικού εγκλήματος σε τρεις κατηγορίες όσον αφορά στις μορφές του ηλεκτρονικού εγκλήματος.[56]

Μια πρώτη κατηγορία αφορά **το ηλεκτρονικό έγκλημα**, αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών. Για παράδειγμα η συκοφαντική δυσφήμηση μπορεί να διαπραχθεί και με τη χρήση η/υ, μέσω της δημοσίευσης στο internet μιας σελίδας με προσβλητικό περιεχόμενο για ένα πρόσωπο(άρθρα 362,363 ΠΚ). Επίσης συχνά παρατηρούνται περιστατικά εκβίασης μέσω internet(άρθρο 385 ΠΚ) ή αντιγραφής πνευματικών έργων(άρθρο 66 Ν 2121/1993). Στην κατηγορία αυτή δύναται να προστεθεί ο ορισμός ότι " Ηλεκτρονικό Έγκλημα θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία"[57]

Στη δεύτερη κατηγορία εντάσσονται τα εγκλήματα που διαπράττονται **μόνο με ηλεκτρονικούς υπολογιστές** στα οποία αποδίδεται ο ορισμός του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης(ΟΟΣΑ) σύμφωνα με τον οποίο «πληροφοριακό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που έχει σχέση με την αυτόματη επεξεργασία και τη μεταφορά στοιχείων». Χαρακτηριστικό έγκλημα της κατηγορίας αυτής αποτελεί η παράνομη αντιγραφή λογισμικού (άρθρο 370Γ παρ 1 ΠΚ) .

Στην τρίτη κατηγορία εντάσσονται τα **γνήσια εγκλήματα** στο κυβερνοχώρο με την έννοια της ποινικοποίησης της συμπεριφοράς, που έχει σχέση αποκλειστικά με τη χρήση του Διαδικτύου (cybercrimes). Τα πιο συχνά εγκλήματα του Κυβερνοχώρου είναι η διασπορά κακόβουλου λογισμικού, καθώς και η διάδοση παιδικού πορνογραφικού υλικού μέσω του Διαδικτύου. Σύμφωνα με αυτή την προσέγγιση τα γνήσια εγκλήματα

[56] Αγγελή Ι: Διαδίκτυο(internet) και ποινικό δίκαιο:Έγκλημα στον Κυβερνοχώρο(cybercrime – internet crime) Ποιν.Χρον.2000, σελ678

[57] Καργόπουλος Αλέξανδρος – Ιωάννης: Κυβερνο-έγκλημα:Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου, www.esdi.gr

του κυβερνοχώρου διαπράττονται αποκλειστικά με τη χρήση του διαδικτύου.[58] Δεν είναι αρκετή για τη στοιχειοθέτησή τους μόνο η χρήση του ηλεκτρονικού υπολογιστή διότι σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή.[59]

ΚΕΦΑΛΑΙΟ 7^{Ο}

7. ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

7.1 Διεθνές και Ευρωπαϊκό Νομοθετικό Πλαίσιο

Στις αρχές της δεύτερης χιλιετίας με δεδομένες τις θεμελιώδεις αλλαγές που επέφερε η ψηφιοποίηση, η σύγκλιση και η συνεχιζόμενη παγκοσμιοποίηση των δικτύων υπολογιστών, το έντονο ενδιαφέρον της διεθνούς κοινότητας για την πρόληψη και την καταστολή του Κυβερνοεγκλήματος αποτυπώθηκε στη σύμβαση που τα κράτη – μέλη του Συμβουλίου της Ευρώπης υπέγραψαν για το Κυβερνοέγκλημα στη Βουδαπέστη(CETS No 185, Budapest, 23 XI.2001, σε ισχύ από τις 01.07.2004). Η Ελλάδα είναι συμβαλλόμενο κράτος στην εν λόγω διεθνή σύμβαση. Η παραπάνω σύμβαση υπεγράφη επειδή οι επιθέσεις κατά συστημάτων πληροφοριών, και ιδίως οι επιθέσεις που συνδέονται με το οργανωμένο έγκλημα ,αποτελούν συνεχώς αυξανόμενη απειλή ,τόσο στην Ευρωπαϊκή Ένωση όσο και παγκοσμίως , εντείνοντας τις ανησυχίες για το ενδεχόμενο τρομοκρατικών επιθέσεων ή επιθέσεων με πολιτικά κίνητρα κατά των συστημάτων πληροφοριών που αποτελούν μέρος των υποδομών ζωτικής σημασίας των κρατών μελών της Ένωσης(σκέψη 3 της Οδηγίας 2013/40/ΕΕ).

Υπάρχουν στοιχεία που δείχνουν μια τάση διάπραξης όλο και πιο επικίνδυνων και επαναλαμβανόμενων επιθέσεων μεγάλης κλίμακας κατά συστημάτων πληροφοριών που συχνά μπορούν να έχουν ζωτική σημασία για τα κράτη μέλη ή για ειδικές δραστηριότητες του δημοσίου ή του ιδιωτικού τομέα. Η τάση αυτή συνοδεύεται από την ανάπτυξη όλο και πιο εξελιγμένων μεθόδων, όπως η δημιουργία και η χρήση των αποκαλούμενων «botnet» (δίκτυα προγραμμάτων ρομπότ) , η οποία περιλαμβάνει διάφορα στάδια της αξιόποινης πράξης , καθένα από τα

[58] Δημητρίου Δήμητρα: Το ηλεκτρονικό έγκλημα στην Ελληνική έννομη τάξη, Θεσσαλονίκη 2008,σελ9
[59] Βλαχόπουλος Κων: "Ηλεκτρονικό Έγκλημα – Μορφές, Πρόληψη, Αντιμετώπιση", Αθήνα 2007, σελ 9

οποία μπορεί από μόνο του να θέσει σε σοβαρό κίνδυνο το δημόσιο συμφέρον (σκέψη 5 της Οδηγίας 2013/40/ΕΕ).

7.2 Το Ενωσιακό Νομικό Πλαίσιο και η σύμβαση για το Κυβερνοέγκλημα

Η παραπάνω σύμβαση των 26 χωρών κρατών – μελών για το Κυβερνοέγκλημα[60] υπεγράφη όταν τα κράτη – μέλη της Ευρωπαϊκής Ένωσης ,από κοινού με άλλες χώρες του κόσμου συνειδητοποίησαν ότι έπρεπε να δημιουργηθεί μία συνθήκη η οποία να έχει ως φιλοδοξία την καταπολέμηση του εγκλήματος στο διαδίκτυο που έμελλε να λάβει μεγαλύτερες διαστάσεις με το πέρασμα του χρόνου. Μάλιστα , οι ενέργειες αυτές έπρεπε να είναι κοινές , καθώς «μία αποτελεσματική μάχη ενάντια στο Κυβερνοέγκλημα απαιτεί αυξημένη ,ταχεία και αποτελεσματική συνεργασία σε ποινικά ζητήματα». Επιπλέον , τα κράτη – μέλη ,από κοινού με τις συμβαλλόμενες στη Συνθήκη χώρες ,είχαν πειστεί μεταξύ άλλων , πως η «παρούσα Συνθήκη είναι απαραίτητη για να αποτραπεί οποιαδήποτε ενέργεια θα στρεφόταν κατά της εμπιστευτικότητας ,ακεραιότητας και διαθεσιμότητας των συστημάτων πληροφοριών , δικτύων και δεδομένων υπολογιστή , καθώς επίσης και την κατάργηση τέτοιων συστημάτων , δικτύων και δεδομένων , προνοώντας για την ποινικοποίηση τέτοιων συμπεριφορών…» Η σύμβαση αυτή υπογράφηκε από είκοσι έξι[61] χώρες κράτη – μέλη του Συμβουλίου της Ευρώπης ,όπως επίσης και τέσσερις χώρες παρατηρητές.[62]
Αργότερα η σύμβαση υπογράφηκε και από άλλες δέκα οκτώ χώρες[63].

Σημαντικό είναι να διευκρινίσουμε τους στόχους που έθεσε η ανωτέρω σύμβαση .Αυτοί ήταν η εναρμόνιση του Ουσιαστικού Ποινικού Δικαίου ,

[60] Σύρος Γεώργιος: Τεχνική Θεώρηση και νομική προσέγγιση στα πλαίσια του Ενωσιακού Ελληνικού Δικαίου

[61] Οι χώρες αυτές ήταν οι εξής:Αλβανία , Αρμενία ,Αυστρία, Βέλγιο,Βουλγαρία,Κροατία,Κύπρος,Εσθονία,Φιλανδία,Γαλλία,Γερμανία,Ελλάδα,Ουγγαρία,Ιταλία,Μολδαβία,Ολλανδία,Νορβηγία,Πολωνία,Πορτογαλία,Ρουμανία,Ισπανία,Σουηδία,Ελβετία,Π.Γ.Δ.Μ,Ουκρανία και Ηνωμένο Βασίλειο

[62] Αυτές ήταν η Ιαπωνία ,ο Καναδάς , η Νότια Αφρική και οι ΗΠΑ

[63] Οι χώρες αυτές ήταν οι εξής:Ανδόρα ,Αζερμπαϊτζάν, Βοσνία-Ερζεγοβίνη, Τσεχική Δημοκρατία,Δανία,Γεωργία,Ιρλανδία,Λετονία,Λιχτενστάιν,Λιθουανία,Λουξεμβούργο,Μάλτα,Μονακό, Μαυροβούνιο,Σερβία,Σλοβενία,Σλοβακία και Τουρκία.

η εναρμόνιση του Δικονομικού Ποινικού Δικαίου και η θέσπιση κανόνων Διεθνούς Δικαστικής Συνεργασίας.

7.3 Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης

Κάποια χρόνια αργότερα, και με ακόμη επιτακτικότερη την ανάγκη συνεργασίας μεταξύ κρατών – μελών, αρμοδίων αρχών και υπηρεσιών, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης επαναπροσδιόρισε το νομοθετικό πλαίσιο για τις επιθέσεις κατά συστημάτων πληροφοριών, αντικαθιστώντας ρητά την Απόφαση – Πλαίσιο του Συμβουλίου της Ευρωπαϊκής Ένωσης με την από 12.08.2013 Οδηγία 2013/40/ΕΕ,[64] σύμφωνα με το άρθ. 83 παρ 1 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης, προβλέποντας ποινικές κυρώσεις τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας. Στην σκέψη 15 της Οδηγίας αποσαφηνίζεται ρητά ότι η Σύμβαση του Συμβουλίου της Ευρώπης του 2001 για το έγκλημα στον κυβερνοχώρο αποτελεί "το νομικό πλαίσιο αναφοράς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών" και βάση της εν λόγω Οδηγίας, ενώ λίγο παρακάτω στη σκέψη 34, ο σκοπός της Οδηγίας συνίσταται στην "τροποποίηση και επέκταση των διατάξεων της απόφασης- πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της 24-02-2005, για τις επιθέσεις κατά των συστημάτων πληροφοριών" παρέχοντας εξαρχής το κύριο ερμηνευτικό εργαλείο. Και αυτό διότι, όπως εκτίθεται κυρίως στις σκέψεις 2,4 και 6, τα συστήματα πληροφοριών είναι βασικό στοιχείο για την πολιτική, κοινωνική και οικονομική αλληλεπίδραση στην Ένωση και η κοινωνία εξαρτάται σε υψηλό και αυξανόμενο βαθμό από τέτοια συστήματα. Υπάρχουν δε στοιχεία, που δείχνουν μια τάση διάπραξης όλο και πιο επικίνδυνων και επαναλαμβανόμενων επιθέσεων μεγάλης κλίμακας κατά συστημάτων πληροφοριών που συχνά μπορούν να έχουν ζωτική σημασία για τα κράτη – μέλη ή για ειδικές δραστηριότητες του

[64] Σκέψη 11 της Οδηγίας: «Η παρούσα Οδηγία προβλέπει ποινικές κυρώσεις τουλάχιστον για τις περιπτώσεις που δεν είναι ήσσονος σημασίας. Τα κράτη μέλη θα πρέπει να μπορούν να καθορίζουν τι συνιστά περίπτωση ήσσονος σημασίας σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές.....»

δημοσίου ή του ιδιωτικού τομέα. Ενώ τέλος, ιδιαίτερη μνεία γίνεται για τα εργαλεία που μπορούν να χρησιμοποιηθούν για την διάπραξη των αδικημάτων που αναφέρονται στην Οδηγία, με έμφαση στην αποφυγή της ποινικοποίησης μέσω απαίτησης συνδρομής στο πρόσωπο του δράστη άμεσης πρόθεσης χρησιμοποίησης των εργαλείων για την διάπραξη αυτών των αδικημάτων.

Υπό το πρίσμα συνεπώς των ανωτέρω σκέψεων, στο άρθρο 2 της Οδηγίας δόθηκαν εκ νέου οι ορισμοί των εννοιών «**σύστημα πληροφοριών**», «**ηλεκτρονικά δεδομένα**», «νομικό πρόσωπο» και «**χωρίς δικαίωμα**», στο άρθρο 3 τυποποιήθηκε «η παράνομη πρόσβαση σε συστήματα πληροφοριών» και στο άρθρο 7 με τίτλο «εργαλεία που χρησιμοποιούνται για την διάπραξη των αδικημάτων», προβλέφθηκε η ποινικοποίηση των προπαρασκευαστικών πράξεων. Εδώ πρέπει να διασαφηνιστεί πως αναφορικά με το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα τόσο η προϊσχύουσα Απόφαση-Πλαίσιο όσο και η Οδηγία έχουν το ίδιο περιεχόμενο, με μόνη διαφορά ότι η Οδηγία απαιτεί ρητά παραβίαση μέτρου ασφαλείας για να θεμελιωθεί ποινικά ευθύνη για παράνομη πρόσβαση σε πληροφοριακό σύστημα και πλέον με την Οδηγία ποινικοποιούνται οι συναφείς προπαρασκευαστικές πράξεις. Έτσι, με αυτές τις ρυθμίσεις η Οδηγία[65] πράγματι έχει ως νομικό πλαίσιο αναφοράς την Σύμβαση του Συμβουλίου της Ευρώπης, την οποία και ακολουθεί.

Επίσης, στο άρθρο 16 προβλέφθηκε ως απώτατο χρονικό όριο μεταφοράς των ρυθμίσεων της Οδηγίας στα εθνικά δίκαια των κρατών- μελών η 4η .09.2015 και στο άρθρο 17 προβλέφθηκε ως απώτατο χρονικό όριο η 4η -09-2017 προκειμένου η Επιτροπή να υποβάλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αναφορικά με την αξιολόγηση των επιμέρους μέτρων που έχουν λάβει τα κράτη – μέλη, και ως εκ τούτου την συμμόρφωση τους προς τις ρυθμίσεις της Οδηγίας, για τα οποία θα γίνει λόγος παρακάτω.

7.3.1 Εθνικές νομοθετικές παρεμβάσεις με το Ν 4411/2016.

Στην Ελλάδα μέχρι την έκδοση του **Ν.4411/2016** δεν υπήρχε νόμος που να αναφέρεται αποκλειστικά σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από απόψεως

[65] Σκέψη 15 της Οδηγίας: «Τα συμπεράσματα του Συμβουλίου της 27ης και 28ης Νοεμβρίου 2008 ανέφεραν ότι τα κράτη μέλη και η Επιτροπή θα πρέπει να αναπτύξουν νέα στρατηγική λαμβάνοντας υπόψη το περιεχόμενο της Σύμβασης του Συμβουλίου της Ευρώπης του 2001 για το έγκλημα στον Κυβερνοχώρο…..»

ποινικού δικαίου. **Ο νόμος 1805/1988** αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα: Με το άρθρο 3 του νόμου αυτού προσετέθησαν τρία νέα άρθρα στον Ποινικό Κώδικα ,το αρ. 370Β ,370Γ και 386Α.

Ο Έλληνας νομοθέτης με το Ν 4411/2016 κύρωσε την από 23-11-2001 Σύμβαση του Συμβουλίου της Ευρώπης, καθιστώντας την αναπόσπαστο μέρος του εσωτερικού ελληνικού δικαίου με αυξημένη μάλιστα τυπική ισχύ κατ'άρθρο 28 Σ, και μετέφερε στο εθνικό δίκαιο την Οδηγία. Η Σύμβαση με την Οδηγία συμβαδίζουν και συνεπώς δεν προκύπτουν ζητήματα αντινομίας. Ειδικότερα, ως προς το εξεταζόμενο στην παρούσα εργασία ποινικό αδίκημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα, η συμμόρφωση του ελληνικού ποινικού δικαίου με τις ρυθμίσεις της Σύμβασης και κυρίως της πλέον σύγχρονης Οδηγίας πραγματοποιήθηκε: α) με την εισαγωγή των όρων «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα» στο άρθρο 13 του ΠΚ, β)την αντικατάσταση της παρ. 2 του αρ.370Γ ΠΚ και γ)την εισαγωγή του νέου αρ 370Ε που ποινικοποιεί τις προπαρασκευαστικές πράξεις μεταξύ άλλων και του αρ. 370Γ παρ 2και 3.[66]

Πρόκειται για μια ποινική διάταξη με μεγάλο εύρος εφαρμογής διότι μετά τις ρυθμίσεις του Ν 4411/2016, ποινικοποιείται υπό συγκεκριμένες προϋποθέσεις κάθε παράνομη πρόσβαση σε σύστημα πληροφοριών, είτε εν όλω είτε εν μέρει, δηλαδή το αποκαλούμενο στη γλώσσα των δραστών «hacking».

Πρέπει να αναφερθεί ότι η διερεύνηση αυτή ήταν επιτακτική διότι τα νέα μορφώματα αξιόποινης συμπεριφοράς που δημιούργησε η διάδοση και επικράτηση του διαδικτύου δεν καλύπτονταν από τις υπάρχουσες ποινικές διατάξεις.

Με το Ν 4411/2016 που δημοσιεύθηκε στο **ΦΕΚ 142/Α/5 - 8 – 2016** γίνεται:[67]

α. Επικαιροποίηση της ποινικής νομοθεσίας στον τομέα της «Κυβερνοεγκληματικότητας» και ειδικότερα κυρώθηκε η σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο που υπογράφηκε στη Βουδαπέστη και το πρόσθετο πρωτόκολλο αυτής αναφορικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής

[66] Πριλή Σταυρούλα. Η Παράνομη πρόσβαση σε πληροφοριακό σύστημα κατ'άρ 370Γ παρ.2 Ποινικού Κώδικα, Αθήνα 2017, σελ 9

[67] https//www.e-nomothesia.gr/nomikes plirofories

φύσης που διαπράττονται μέσω συστημάτων υπολογιστών που υπογράφηκε στο Στρασβούργο στις 28 Ιανουαρίου 2003 και β. Τιμωρούνται ενέργειες που στρέφονται κατά των δικτύων πληροφοριών, δηλαδή πράξεις που αποσκοπούν στην από πρόθεση πρόκληση βλάβης στα δίκτυα και στρέφονται κατά της ακεραιότητας , της διαθεσιμότητας των δεδομένων ή των συστημάτων πληροφορικής. Επιπλέον τιμωρούνται πράξεις που αφορούν την παράνομη πρόσβαση, την υποκλοπή ,την παρεμβολή σε δεδομένα και τις παρεμβολές σε συστήματα.

ΚΕΦΑΛΑΙΟ 8^{Ο}

8. ΕΙΔΙΚΟΤΕΡΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΣΥΜΒΑΣΗΣ ΓΙΑ ΤΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η αξονική σημασία της Σύμβασης της Βουδαπέστης και εν ταυτώ της 2013/40/ΕΕ Οδηγίας, που επικυρώθηκαν με τον Ν 4411/2016(ΦΕΚ Ά 142/3.8.2016), επικαιροποιώντας την ποινική μας νομοθεσία, αναδεικνύεται από την ευρύτητα και βαρύτητα των επιμέρους ρυθμίσεων. Η εισαγωγή στο άρθρο 13 στοιχ. η΄ και θ΄ ΠΚ[68] [69] των ορισμών του πληροφοριακού συστήματος και των ψηφιακών δεδομένων, συνιστά πρώτο βήμα αυτής της επικαιροποίησης του Ελληνικού νομικού πλαισίου για την Κυβερνοεγκληματικότητα. Αντίστοιχο βήμα προωθείται με τη μεταφορά των αυθεντικών ορισμών της ως άνω Οδηγίας για τις Επιθέσεις κατά Συστημάτων Πληροφοριών και για τα χρησιμοποιούμενα για αυτές εργαλεία. Εξάλλου, οι συνολικές ρυθμίσεις στο γενικό και αφηρημένο επίπεδο του νόμου συμπληρώνουν και εν πολλοίς οργανώνουν ένα πολυεπίπεδο θεσμικό πλαίσιο που καλείται να αντιμετωπίσει τον υδραργυρικό χώρο της Κυβερνοεγκληματικότητας.

[68] Άρθρο 13 στοιχ. η ΠΚ
«Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων…..»

[69] Άρθρο 13 στοιχ.θ ΠΚ
«Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία»

8.1 Οι κατ'έκαστον διατάξεις ουσιαστικού δικαίου

Οι ουσιαστικού ποινικού δικαίου διατάξεις της Σύμβασης της Βουδαπέστης, όπως ρυθμίζονται στην 1η Ενότητα του 2ου Κεφαλαίου της,[70] αφορούν εγκλήματα κατά της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικού υπολογιστή, εγκλήματα σχετιζόμενα με υπολογιστές, εγκλήματα σχετικά με το περιεχόμενο και εγκλήματα σχετικά με πνευματικά και συγγενικά δικαιώματα.[71]

8.2 Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών

Στο πλαίσιο της σύμβασης της Βουδαπέστης με αφετηρία τη σκέψη ότι η ασφάλεια των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να ικανοποιεί την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων, προωθήθηκε η αξίωση ποινικοποίησης της εκ προθέσεως και χωρίς δικαίωμα πρόσβασης στο σύνολο ή σε τμήμα συστήματος ηλεκτρονικών υπολογιστών, δηλαδή του λεγόμενου διεθνώς «hacking». Ως «hacking» (εισβολή) κατανοείται η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα Η/Υ, σκοπός της οποίας καταρχήν δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα.
Γίνεται αντιληπτό ότι ποινικοποίηση της απλής πρόσβασης σε ηλεκτρονικά δεδομένα, ανεξάρτητα από την επέλευση περιουσιακού οφέλους ή ζημίας, αντανακλά την ανάγκη αντιμετώπισης των κινδύνων από τις εξελίξεις της πληροφορικής και ειδικότερα την ανάγκη προστασίας του δικαιώματος κάθε προσώπου για διατήρηση συγκεκριμένων δεδομένων ως απόρρητων και άρα ως μη προσβάσιμων στον καθένα. Υποστηρίζεται, πάντως, και η άποψη ότι πέραν του απορρήτου η διάταξη προστατεύει και το έννομο αγαθό της περιουσίας, ειδικά όταν ο νόμιμος κάτοχος του συστήματος είναι κάποιο νομικό πρόσωπο, αλλά και η

[70] https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016
[71] Δαλακούρας Ι.Θεοχάρης : Ηλεκτρονικό έγκλημα, Θεσσαλονίκη 2018, σελ 7

άποψη[72] ότι προστατευόμενο έννομο αγαθό είναι η ασφάλεια του ηλεκτρονικού συστήματος, δηλαδή η πρόληψη της πρόσβασης από μη εξουσιοδοτημένα άτομα.

Ο όρος «χωρίς δικαίωμα» χρησιμοποιείται τόσο στη διάταξη του άρθρου 370Γ παρ.1 ΠΚ όσο και στις σχετικές διατάξεις της Σύμβασης για το κυβερνοέγκλημα καθώς και του Πρόσθετου Πρωτοκόλλου αυτής , με την επισήμανση ότι η χωρίς δικαίωμα πρόσβαση συνιστά ιδιαιτερότητα των αδικημάτων αυτών και αποτελεί ρητή προϋπόθεση της παράνομης ενέργειας. Εύλογα τονίζεται, άλλωστε, ότι η έκφραση «χωρίς δικαίωμα» παραπέμπει σε συγκατάθεση, η οποία αποκλείει ήδη την αντικειμενική υπόσταση του εγκλήματος και δεν αίρει απλώς τον άδικο χαρακτήρα της πράξης, αφού όταν αυτή συντρέχει το προστατευόμενο έννομο αγαθό δεν προσβάλλεται καν.[73]

Η χώρα μας ανταποκρίθηκε πλήρως στην υποχρέωση συμμόρφωσης με το άρθρο 2 της Σύμβασης για την προστασία του απορρήτου, «Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος πρόσβαση στο σύνολο ή σε μέρος ενός συστήματος υπολογιστή, όταν αυτή διαπράττεται από πρόθεση…», καθόσον η συναξιολόγηση των διατάξεων των άρθρων 4 και 15του Ν 3471/2006 για τα προσωπικά δεδομένα και 1 και 11 του Ν 3917/2011 για τα ηλεκτρονικά δεδομένα, του άρθρου 370Β ΠΚ για τη μη πρόσβαση σε απόρρητα συγκεκριμένου είδους(κρατικά, επιστημονικά, επαγγελματικά ή επιχείρησης του δημόσιου ή του ιδιωτικού τομέα) ή σε δεδομένα που ο ίδιος ο κάτοχός τους μεταχειρίζεται ως απόρρητα και του άρθρου 370Γ παρ.2 ΠΚ για την απαγόρευση απλής πρόσβασης σε στοιχεία που έχουν εισαχθεί σε Η/Υ καλύπτει επαρκώς το προστατευόμενο πεδίο.

8.3 Η παράνομη παρέμβαση ή άλλως παράνομη υποκλοπή δεδομένων

Με το άρθρο 3 της Σύμβασης[74] προωθήθηκε η ποινικοποίηση της εκ προθέσεως και άνευ δικαιώματος παρέμβασης ή υποκλοπής που γίνεται με τεχνικά μέσα σε μη δημόσιες διαβιβάσεις των δεδομένων υπολογιστή από ή με σύστημα υπολογιστή, περιλαμβανομένων ηλεκτρομαγνητικών εκπομπών

[72] Βλαχόπουλος Κ : Ηλεκτρονικό έγκλημα, Μορφές – Πρόληψη – Αντιμετώπιση, Νομική Βιβλιοθήκη, 2007, σελ 137

[73] Δαλακούρας Ι. Θεοχάρης: Ηλεκτρονικό έγκλημα, Θεσσαλονίκη 2018,σελ 8

[74] Δαλακούρας Ι. Θεοχάρης : Ηλεκτρονικό έγκλημα, Θεσσαλονίκη 2018, σελ 9

από σύστημα υπολογιστή που μεταφέρει δεδομένα υπολογιστή. «Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η υποκλοπή δια τεχνικών μέσων μη δημοσίων διαβιβάσεων δεδομένων υπολογιστή από και προς ή εντός ενός συστήματος υπολογιστή..». Ευθεία στόχευση της οικείας ρύθμισης αποτέλεσε η «πληρέστερη προστασία του απορρήτου των επικοινωνιών μέσω συστημάτων πληροφοριών», καθώς η ισχύς της καλύπτει όλες τις μορφές ηλεκτρονικής μεταφοράς δεδομένων, όπως λ.χ. μέσω τηλεφώνου, μέσω fax, μέσω email ή άλλου τρόπου μεταφοράς.
Σε εναρμόνιση προς τα ανωτέρω το άρθρο 370Γ ΠΚ, στη νέα διατύπωσή του, τιμωρεί στη δεύτερη παράγραφο το αποκαλούμενο hacking,δηλαδή τη χωρίς δικαίωμα πρόσβαση στο σύνολο ή σε τμήμα ενός πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφάλειας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148». Κατά το γράμμα της διάταξης τιμωρείται κάθε αυθαίρετη πρόσβαση σε δεδομένα ή στοιχεία που βρίσκονται αποθηκευμένα στον υπολογιστή του θύματος, αλλά και κάθε αθέμιτη πρόσβαση σε δεδομένα που μεταδίδονται με συστήματα τηλεπικοινωνιών. Συνεπώς καταλαμβάνεται στο πεδίο εφαρμογής της διάταξης τόσο η παγίδευση δικτύων μετάδοσης δεδομένων(wire tapping) όσο και η ακρόαση ψηφιακά μεταδιδόμενων επικοινωνιών, η διείσδυση στο ηλεκτρονικό ταχυδρομείο ενός προσώπου, καθώς και η πρόσβαση σε ξένα συστήματα επεξεργασίας ή αποθήκευσης δεδομένων, δηλαδή κάθε είδους παράνομη πρόσβαση σε κλειδωμένο πληροφοριακό σύστημα που κατά το κοινώς λεγόμενο «χακάρεται» από τον δράστη.

ΚΕΦΑΛΑΙΟ 9^{Ο}

9.ΤΟ ΕΛΛΗΝΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

9.1 Η συνταγματική προστασία του ιδιωτικού βίου στην Ελλάδα

Η Ελευθερία του ιδιωτικού βίου στην Ελλάδα προστατεύεται από ένα πλέγμα συνταγματικών διατάξεων, διεθνών συνθηκών και διατάξεων

ειδικών ποινικών νόμων που εξεδόθησαν βάσει κοινοτικών οδηγιών, που δίνουν το μέτρο και την έκταση της παρεχόμενης προστασίας. Κατ'αρχήν η θεμελιώδης διάταξη του άρθρου 2 παρ 1 του Συντάγματος σύμφωνα με την οποία «ο σεβασμός και η προστασία της αξίας του ανθρώπου, αποτελούν την πρωταρχική υποχρέωση της πολιτείας» εγγυάται την προστασία των ειδικών εκδηλώσεων ή αγαθών τα οποία ανήκουν στην προσωπικότητα του ατόμου και συνιστούν αναπόσπαστο τμήμα της αξίας του.[75]Στο ίδιο άρθρο 2 παρ 1 εδαφ 2 του Συντάγματος τονίζεται ότι «Η Ελλάδα, ακολουθώντας τους γενικά αναγνωρισμένους κανόνες του διεθνούς δικαίου, επιδιώκει την εμπέδωση της ειρήνης, της δικαιοσύνης, καθώς και την ανάπτυξη των φιλικών σχέσεων των λαών και των κρατών». Επίσης το δικαίωμα στον ιδιωτικό βίο ως πρωταρχική εκδήλωση της προσωπικότητας προστατεύεται και από τη θεμελιώδη διάταξη του άρθρου 5 παρ 1 του Συντάγματος, σύμφωνα με την οποία « Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και πολιτική ζωή της χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη.»

Η προσωπική ελευθερία επιτρέπει την ελεύθερη ανάπτυξη της προσωπικότητας του ανθρώπου η ιδιωτική δε σφαίρα του ατόμου αποτελεί συστατικό στοιχείο της προσωπικότητάς του.

Οι παραπάνω διατάξεις συμπληρώνονται με τα άρθρα 9 και 19 του συντάγματος που δημιουργούν το πλέγμα που κατοχυρώνουν το απαραβίαστο της ιδιωτικής ζωής του ατόμου, ως και το απόρρητο των επικοινωνιών. Συγκεκριμένα σύμφωνα με το άρθρο 9 παρ1 εδαφ 2 του Συντάγματος «**Η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη**» που σημαίνει ότι απαγορεύεται η δημοσιοποίηση της ζωής του ανθρώπου. Δηλαδή απαγορεύεται κάθε επέμβαση που αποσκοπεί στην παρακολούθηση ή με οποιοδήποτε τρόπο ή μέσο καταγραφή της ιδιωτικής ζωής καθώς και ο εξαναγκασμός του ατόμου να αποκαλύπτει στοιχεία που τον αφορούν. Η προστασία του άρθρου 9 συμπληρώνεται με την διάταξη του άρθρου 9^{A} του Συντάγματος, όπως συμπληρώθηκε με την τελευταία αναθεώρηση του Συντάγματος, η οποία ορίζει ότι «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή που

[75] Καράκωστας Κ.Ιωάννης: Δίκαιο και Ίντερνετ , νομικά ζητήματα του διαδικτύου, Αθήνα 2009, σελ 151

συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Επίσης σύμφωνα με το άρθρο 19 παρ 1 «Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων».
Οι παραπάνω διατάξεις προστατεύουν κατ'αρχήν άμεσα τον ιδιώτη από κάθε προσβολή εκ μέρους φορέων της κρατικής εξουσίας, παρέχουν δε προστασία από κάθε μέσο τηλεπικοινωνίας που υπάρχει σήμερα ως και κάθε προσβολής από μέρους άλλων ιδιωτών δεδομένης της έμμεσης τριτενέργειας την οποία αναπτύσσουν οι σχετικές συνταγματικές διατάξεις. Επίσης σύμφωνα με το άρθρο 25 παρ 1, όπως συμπληρώθηκε μετά την τελευταία αναθεώρηση του Συντάγματος προβλέπεται πλέον ρητώς ότι « *Τα δικαιώματα του ανθρώπου ως ατόμου και ως μέλους του κοινωνικού συνόλου και η αρχή του κοινωνικού κράτους δικαίου τελούν υπό την εγγύηση του Κράτους*». Όπως ρητώς επίσης προβλέπεται στο ίδιο άρθρο 25 του Συντάγματος η εφαρμογή, η διασφάλιση των ατομικών δικαιωμάτων και η προστασία αυτών παρέχεται και έναντι των ιδιωτών από το κράτος, όπως ορίζει το αναφερόμενο άρθρο: «*Όλα τα κρατικά όργανα υποχρεούνται να διασφαλίζουν την ανεμπόδιστη και αποτελεσματική άσκησή τους*» η προστασία δε αυτή παρέχεται και έναντι των ιδιωτών, βάσει της παρ 1 του αναφερόμενου άρθρου 25 που ορίζει ότι «*τα δικαιώματα αυτά ισχύουν και στις σχέσεις μεταξύ ιδιωτών στις οποίες προσιδιάζουν*» .
Η παραπάνω παρεχόμενη προστασία[76] ενδυναμώνεται με τις διατάξεις που έχουν θεσπιστεί στο κοινό δίκαιο για την προστασία του απορρήτου των επικοινωνιών όπως τα άρθρα 370Α, 370Β και 370Γ' του Ποινικού Κώδικα και οι γενικές προστατευτικές ρυθμίσεις που παρέχονται με τα άρθρα 57,59,739,914,920 και 932 του Αστικού Κώδικα.

9.2 Απόρρητα στο Διαδίκτυο

Η προστασία του απορρήτου αποσκοπεί στη διασφάλιση της ελεύθερης προσωπικής επικοινωνίας και προϋποθέτει δύο πρόσωπα, εκείνο που αποστέλλει το μήνυμα και εκείνο που το δέχεται. Βασικό στοιχείο της προσωπικής ανταπόκρισης ή επικοινωνίας είναι η μυστικότητα του περιεχομένου της. Η παραπάνω αναφερόμενη διάταξη του άρθρου 25 παρ 1

[76] Καρακώστας Κ. Ιωάννης : Δίκαιο και Ίντερνετ. Νομικά ζητήματα του διαδικτύου, Αθήνα 2009, σελ 153

του Συντάγματος ορίζει ρητά ότι η προστασία παρέχεται τόσο έναντι επεμβάσεων της κρατικής εξουσίας όσο και έναντι ιδιωτών.
Η συνταγματική προστασία του απορρήτου της επικοινωνίας εκτείνεται σε όλα τα μέσα τηλεπικοινωνίας που υπάρχουν σήμερα είτε ενσύρματα είτε ασύρματα καθώς και σε οποιαδήποτε ανακαλυφθούν μελλοντικά. Συνεπώς προστατεύεται και το απόρρητο της επικοινωνίας στο Διαδίκτυο.[77]
Πρέπει να τονιστεί πως αντικείμενο προστασίας δεν είναι το μήνυμα καθ'εαυτό, αλλά το απόρρητο του μηνύματος. Είναι αδιάφορο, αν το μήνυμα έχει προσωπικό ή επαγγελματικό χαρακτήρα. Το απόρρητο της επικοινωνίας μέσω Διαδικτύου, σύμφωνα με μια άποψη, δεν καλύπτει μόνο το περιεχόμενο του ηλεκτρονικού μηνύματος αλλά και τα εξωτερικά στοιχεία της επικοινωνίας, δηλαδή τα δεδομένα και τα στοιχεία που περιγράφουν μια διαδικτυακή σύνδεση πχ η ταυτότητα των χρηστών, ο τόπος, ο χρόνος και η διάρκεια της επικοινωνίας.
Όπως έχει υποστηριχθεί καθένας έχει δικαίωμα συμμετοχής στη κοινωνία της πληροφορίας και το κράτος υποχρεούται με τις εγγυήσεις που παρέχουν τα άρθρα 9,9Α και 19, να διευκολύνει την πρόσβαση, την παραγωγή, την ανταλλαγή και τη διάδοση των πληροφοριών που διακινούνται ηλεκτρονικά.[78]
Ωστόσο η επικοινωνία μέσω internet είναι εξ'ορισμού επικοινωνία σε δημοσιότητα, ένας χώρος ελεύθερης έκφρασης που μπορεί να συμμετέχει ο καθένας (πχ με τη δημιουργία μιας ιστοσελίδας , με αναρτήσεις σε blogs, με τη συμμετοχή μέσω προσωπικού λογαριασμού στα μέσα κοινωνικής δικτύωσης – social media).
Το απόρρητο είναι το απολύτως μυστικό. Αυτό βέβαια εξαρτάται από τη βούληση των επικοινωνούντων χρηστών υπάρχει και προστατεύεται με την προϋπόθεση να έχει τηρηθεί μια στοιχειώδης διαδικασία διαφύλαξής του μέσω ειδικών προγραμμάτων και κωδικών. Έτσι απόρρητο υπάρχει όταν κάποιος έχει δημιουργήσει ένα απόρρητο προφίλ σε μια ιστοσελίδα στο οποίο έχει δικαίωμα πρόσβασης μόνο ο ίδιος με τη χρήση κατάλληλων κωδικών. Αντίθετα ένα ηλεκτρονικό μήνυμα το οποίο διαβιβάζεται χωρίς τη λήψη μέτρων ασφάλειας, δεν καλύπτεται από το απόρρητο και επομένως μπορεί να διαβαστεί από άλλους χρήστες, από τα κρατικά όργανα ή τον παροχέα πρόσβασης. Έτσι, οι αρμόδιες αρχές, στα πλαίσια ερευνών για την εξακρίβωση ενός εγκλήματος, εφόσον τα στοιχεία αυτά έχουν καταστεί

[77] Καράκωστας Κ. Ιωάννης: Δίκαιο και Ίντερνετ : Νομικά ζητήματα του Διαδικτύου, Αθήνα 2009, σελ 153
[78] Σανιδάς Γ. : Γνωμ. Εισ ΑΠ 9/2009, Ποιν Χρ. 2010, 498

κοινά και προσιτά σε οποιοδήποτε χρήστη ή διαχειριστή σελίδας, δικαιούνται να ζητούν από τους παρόχους υπηρεσιών Διαδικτυακής επικοινωνίας τα «ηλεκτρονικά ίχνη» της εγκληματικής πράξης, χωρίς να είναι αναγκαίο να προηγηθεί άδεια κάποιας αρχής.[79]

Το άρθρο 19 του Συντάγματος καθιερώνει εκτός από το απόρρητο της επικοινωνίας και την ελευθερία της επικοινωνίας. Ελευθερία της επικοινωνίας σημαίνει ότι κάθε άτομο είναι ελεύθερο να επιλέγει το είδος, το μέσο και τον τρόπο επικοινωνίας μέσω του Διαδικτύου. Η επικοινωνία μπορεί να γίνεται μεταξύ των χρηστών σε οποιοδήποτε μέρος της επικράτειας ή και στο εξωτερικό. Το απαραβίαστο του απορρήτου ισχύει και όταν η επικοινωνία γίνεται με πρόσωπα που βρίσκονται κάτω από το καθεστώς ειδικών σχέσεων εξουσίας. Διατάξεις νόμων που επιτρέπουν τον έλεγχο της ηλεκτρονικής αλληλογραφίας είναι αντισυνταγματικές και ανίσχυρες.

9.3 ΝΕΟΣ ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ

Το σχέδιο του Νέου Ποινικού Κώδικα αποτελεί πόνημα της τελευταίας νομοπαρασκευαστικής επιτροπής που συστάθηκε με την αριθ 38882/ 18 -5 – 2015 (ΦΕΚ 375/26 -5 – 2015 τ. ΥΟΔΔ) απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, όπως αυτή τροποποιήθηκε και συμπληρώθηκε με μεταγενέστερες αποφάσεις του ίδιου Υπουργού.[80] Το τελευταίο αυτό σχέδιο Νέου Ποινικού Κώδικα, υπήρξε αποτέλεσμα επεξεργασίας τόσο των προηγουμένων Σχεδίων Ποινικού Κώδικα που είχαν παραδοθεί από προηγούμενες νομοπαρασκευαστικές επιτροπές όσο και νέων απόψεων που εκτέθηκαν επί συγκεκριμένων ζητημάτων.

Σύμφωνα με την αιτιολογική έκθεση[81] στο σχέδιο Νόμου «Κύρωση Ποινικού Κώδικα» σημαντικές είναι οι επεμβάσεις στο 22^{ο} κεφάλαιο « προσβολές του ατομικού απορρήτου και της απόρρητης επικοινωνίας» κυρίως σε ότι αφορά τον εξορθολογισμό των ποινών.

[79] Δημητρίου Δήμητρα: Οι επιθέσεις κατά συστημάτων πληροφοριών. Το διεθνές Ενωσιακό και Ελληνικό πλαίσιο προστασίας, Θεσσαλονίκη 2014, σελ 108

[80] Έκθεση Δημόσιας Διαβούλευσης, στην αιτιολογική έκθεση σχεδίου Νόμου «Κύρωση του Ποινικού Κώδικα», σελ 140

[81] Αιτιολογική έκθεση, (3-6-2019) στο σχέδιο νόμου «Κύρωση του Ποινικού Κώδικα», σελ 71

Οι βασικές σκέψεις[82] που αποτέλεσαν τη βάση της όλης μεταρρυθμιστικής προσπάθειας στο χώρο του Ποινικού Δικαίου αποτυπώνονται συνοπτικά στο προοίμιο της Αιτιολογικής Έκθεσης. Ειδικότερα μετά την καθοριστική επίδραση που άσκησε στο δικαιϊκό σύστημα το Σύνταγμα του 1975 ήταν φανερό ότι ο ΠΚ είχε ανάγκη ενός ριζικού εκσυγχρονισμού, αλλά και ιδεολογικού αποχρωματισμού, ώστε να ανταποκριθεί στις σύγχρονες αντιλήψεις τόσο για την αντεγκληματική πολιτική όσο και για την προστασία του πολίτη από την κατάχρηση της ποινικής καταστολής και την εφαρμογή της αρχής του κράτους δικαίου. Είναι σαφές, λοιπόν, πως παράλληλα με τη διατήρηση των δημοκρατικών και φιλελεύθερων χαρακτηριστικών του ΠΚ, ήταν αναγκαίος ο εξορθολογισμός και η ανανέωσή του ώστε να ανταποκρίνεται στις ανάγκες του σύγχρονου κοινωνικού κράτους δικαίου και στις προκλήσεις που αντιμετωπίζει. Τούτο επέβαλε τη διαμόρφωση ενός συστήματος ποινικών κυρώσεων που να ανταποκρίνεται στις σύγχρονες απόψεις για την ποινή, τη διαγραφή εγκλημάτων που δεν προστατεύουν υπαρκτά και σημαντικά για το κοινωνικό σύνολο έννομα αγαθά, την αποκατάσταση της αναλογικότητας που συχνά παραβιαζόταν με επιμέρους αποσπασματικές τροποποιήσεις, την ακρίβεια και σαφήνεια των διατάξεων και την κατά το δυνατό νομοτεχνική αρτιότητά του. Αξιοσημείωτο είναι επίσης το ότι ο ποινικός νομοθέτης αναφέρει στην αιτιολογική έκθεση επιγραμματικά τις βασικές αρχές που διέπουν τις ρυθμίσεις του Ποινικού Κώδικα, προκειμένου αυτές να αποτελέσουν είτε μεμονωμένα είτε σε συνδυασμό πολύτιμο βοήθημα κατά την ερμηνεία και την εφαρμογή του.

Συγκεκριμένα στο εικοστό δεύτερο κεφάλαιο (άρθρα 370 – 371) τίθεται ο τίτλος με βάση τα έννομα αγαθά που προστατεύονται από τις περιεχόμενες σε αυτό διατάξεις. Σύμφωνα με τα ανωτέρω:
α. Στο άρθρο **370Γ** έχει ενταχθεί το έγκλημα που τυποποιείται σήμερα στο άρθρο **370Β**.«*Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών*». Διευκρινίζεται το

[82]Χαραλαμπάκης Αριστοτέλης :Ο νέος ποινικός κώδικας: Μια πρώτη ερμηνευτική προσέγγιση του Ν 4619/2019/, Αθήνα, Νομική Βιβλιοθήκη 2019

περιεχόμενο της έννοιας των απορρήτων, αυξάνεται η ποινή όταν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων και ορίζεται ότι η πράξη τιμωρείται μόνο κατ' έγκληση.
Στο άρθρο **370Δ** τιμωρείται όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών (παρ 1), καθώς και όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση (παρ 2).
Το σύγχρονο Ποινικό Δίκαιο επιδιώκει την αποτελεσματική προστασία των εννόμων αγαθών και την ουσιαστική εξασφάλιση του προσώπου από τις παραδοσιακές καταχρήσεις της ποινικής καταστολής.[83]

Πιο συγκεκριμένα το άρθρο 370Β του παλαιού ΠΚ εισήχθη στο 370Γ του νέου ΠΚ και μία σημαντική αλλαγή που σημειώθηκε είναι ότι αφαιρέθηκε η παρ. 3 του παλαιού 370Β, στο νέο 370Γ ΠΚ. Η παρ. 3 του παλαιού 370Β που αναφερόταν «*στο στρατιωτικό ή διπλωματικό απόρρητο ή απόρρητο που αναφέρεται στην ασφάλεια του κράτους*» είχε ενταχθεί σε ένα άρθρο και κατ' επέκταση σε ένα κεφάλαιο(=το εικοστό δεύτερο) που προστάτευε το ατομικό απόρρητο και το απόρρητο της επικοινωνίας. Όμως παρέπεμπε ρητά με την παλαιά του διατύπωση στα άρθρα **146** και **147 ΠΚ** που αφορούσαν τις προσβολές κρατικών απορρήτων και ειδικότερα στο δεύτερο κεφάλαιο για τις προσβολές της διεθνούς υπόστασης της χώρας. Οι όροι «στρατιωτικό και διπλωματικό απόρρητο» δεν υπάρχουν πλέον σαν όροι στο νέο ΠΚ, θεωρώ όμως πως έχουν ενταχθεί στον όρο «κρατικό απόρρητο» που σύμφωνα με την ερμηνεία του νέου ΠΚ στη διάταξη του άρθρου **149 ΠΚ** «*ως κρατικό απόρρητο ορίζεται ειδικότερα ένα γεγονός, αντικείμενο ή πληροφορία, η πρόσβαση στα οποία είναι δυνατή σε ένα προσδιορισμένο κύκλο προσώπων και που χαρακτηρίζονται ως μυστικά για να αποφευχθεί ο κίνδυνος προσβολής της εδαφικής ακεραιότητας, της αμυντικής ικανότητας, των διεθνών σχέσεων ή των οικονομικών συμφερόντων του ελληνικού κράτους και της διεθνούς ειρήνης*» και οπότε πλέον η παρ.3 του παλαιού 370Β ΠΚ έχει ενταχθεί στο **νέο 146 ΠΚ** και τιμωρείται με αυτό. Παλαιότερα άλλωστε εθεωρείτο πως η παραπομπή στο άρθρο 146 ΠΚ για την αυστηρότερη τιμωρία του δράστη ήταν άνευ ουσίας

[83] Αιτιολογική Έκθεση (3-6-2019), στο σχέδιο νόμου «Κύρωση του Ποινικού Κώδικα», Βασικές αρχές, σελ 2

καθώς ο δράστης όχι απλά δεν τιμωρούνταν αυστηρότερα αλλά στην ουσία έμενε ατιμώρητος αφού γινόταν παραπομπή για να τιμωρηθεί ένα ατομικό έννομο αγαθό(= το απόρρητο της επικοινωνίας του 370Β) με μία διάταξη που προστατεύει ένα κρατικό(=την ασφάλεια του κράτους), δηλαδή προκαλούνταν σύγχυση ως προς το έννομο αγαθό. Οπότε λογικά και ορθά αφαιρέθηκε κατά την άποψή μου η παρ. 3 από το νέο 370Γ ΠΚ για τους λόγους που προανέφερα αλλά και ορθά για τους ίδιους λόγους κρίνω πως αφαιρέθηκε το τελευταίο εδάφιο της παρ. 2 του 370Γ ΠΚ που αναφέρεται στις διεθνείς σχέσεις και στην ασφάλεια του κράτους.

Επιπρόσθετα η αλλαγή στην παρ.1 του 370Δ ΠΚ , όσον αφορά την ποινή που παλαιά ήταν φυλάκιση και χρηματική ποινή, στο άρθρο 370Γ παρ.1 έγινε πλέον «χρηματική ποινή ή παροχή κοινωφελούς εργασίας» και είναι μία κοσμογονική μεταρρύθμιση, καθώς η προσφορά κοινωφελούς εργασίας συγκαταλέγεται από το **άρθρο 50 του νέου ΠΚ** ρητά στις κύριες ποινές. Με τη συμπλήρωση που έγινε στο κείμενο του νέου ΠΚ, με τη διάταξη του άρθρου 2 παρ. 2 εδ. ε' ΠΝΠ ΦΕΚ Α' 106/27.6.2019, η κοινωφελής εργασία πραγματοποιείται προς όφελος του κοινού σε δημόσιες υπηρεσίες, οργανισμούς τοπικής αυτοδιοίκησης ή μη κερδοσκοπικά πρόσωπα ιδιωτικού δικαίου, που ορίζονται με απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και των κατά περίπτωση συναρμόδιων Υπουργών. Οπότε κατά την ερμηνεία του νέου ΠΚ και κατά την άποψή μου η εν λόγω αλλαγή φαίνεται να είναι τόσο υπέρ του κατηγορουμένου όσο και της κοινωνίας εν γένει.

Τέλος, η τελευταία αλλαγή που έγινε στα άρθρα που εξετάζω στην εργασία μου είναι ότι δεν υπάρχει πλέον στο νέο 370Δ ΠΚ, η παρ. 4 του παλαιού 370Γ που όριζε «*Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση*», δηλαδή το έγκλημα του 370Δ ΠΚ πλέον διώκεται αυτεπαγγέλτως. Η αλλαγή αυτή θεωρήθηκε αναγκαία κατά την άποψή μου διότι σε αυτή τη διάταξη τιμωρείται ένα έγκλημα που συνιστά τον «πυρήνα» του ποινικού δικαίου και γι' αυτό, για την πληρέστερη προστασία των φυσικών και των νομικών προσώπων που μπορεί να δεχθούν παράνομη πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή στα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών παραβιάζοντας απαγορεύσεις ή μέτρα ασφάλειας, η δίωξη να μπορεί να επέμβει άμεσα και να τους παρέχει τη μέγιστη δυνατή προστασία χωρίς να υφίσταται οποιοδήποτε είδος καθυστέρησης της όλης διαδικασίας με την υποβολή

εγκλήσεως από την πλευρά του θύματος, ως πρότερον. Εξυπηρετείται, συνεπώς με αυτό τον τρόπο η ταχεία απονομή της δικαιοσύνης, που στην ανάγκη ύπαρξης αυτής προωθούνται και νέοι θεσμοί. Κατά την ερμηνεία και του νέου ΚΠΔ[84] κρίθηκε πως αυτός προωθεί μια πολύπλευρη μεταρρύθμιση στην κατεύθυνση ενίσχυσης της αξιακής του δομής αλλά και της λειτουργικότητάς του. Είναι πρόδηλο πως ο νέος Κώδικας θα καταστεί λειτουργικός, αν καταξιωθούν στην πράξη οι νέες μορφές συναινετικής και αποκαταστατικής δικαιοσύνης και κυρίως αν εφαρμοστούν με σύνεση και αίσθημα δικαιότητας όλες οι διατάξεις του νέου Κώδικα.

Συμπερασματικά καταλήγουμε στο ότι ο νέος ΠΚ ως προς τη συνολική του εικόνα, έχει θετικό πρόσημο. Βέβαια, αυτό δεν σημαίνει ότι με τη θέσπισή του απαλείφθηκαν όλα τα προβλήματα που προκύπτουν κατά την εφαρμογή του ποινικού δικαίου και αυτό γιατί μπορεί να έγινε εκσυγχρονισμός του Ποινικού Κώδικα, που αποτελεί τον κορμό της ποινικής νομοθεσίας, αλλά υπάρχουν και πολλοί ειδικοί ποινικοί νόμοι που εμπεριέχουν ρυθμίσεις που χρήζουν οπωσδήποτε επείγουσας διορθωτικής παρέμβασης από τον ποινικό νομοθέτη. Εάν θέλουμε πάντως να αποδώσουμε μονολεκτικά τη σκοπιμότητα που υπηρετεί ο Κώδικας θα χρησιμοποιήσουμε δύο όρους: «εκσυγχρονισμός»(=απάλειψη αναχρονιστικών θεσμών, κατάργηση πολλών εγκλημάτων που η ύπαρξή τους σηματοδοτούσε παρωχημένα κατάλοιπα καθώς και εισαγωγή νέων ρυθμίσεων που είτε προϋπήρχαν διάσπαρτες σε ειδικούς νόμους είτε εισάγονται για πρώτη φορά) και «εξορθολογισμός»(=ριζική αναδιαμόρφωση του συστήματος επιβολής της ποινής, την υποβάθμιση πολλών κακουργημάτων σε πλημμελήματα, την πρόβλεψη ηπιότερων ποινών σε αρκετά κακουργήματα).Αυτοί οι δύο όροι έχουν καταστεί πλέον απολύτως αναγκαίοι εν όψει της προβληματικής διόγκωσης της ποινικής καταστολής τόσο σε εύρος όσο και σε βάθος.

ΚΕΦΑΛΑΙΟ 10^{Ο}

10. ΆΡΘΡΟ 370Β ΠΚ

10.1 Η ΝΟΜΟΤΥΠΙΚΗ ΜΟΡΦΗ ΤΟΥ ΑΡΘΡΟΥ 370Β Π.Κ

[84] Δαλακούρας Θεοχάρης: Ο νέος κώδικας ποινικής δικονομίας : Μία πρώτη ερμηνευτική προσέγγιση του Ν 4620/2019/,Αθήνα, Νομική Βιβλιοθήκη 2019, σελ. 118

10.1.1 Το βασικό αδίκημα του άρθρου 370Β παρ1 ΠΚ:

Σύμφωνα με τη παρ1 του άρθρου 370Β ΠΚ:[85]

«Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή του ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.»

Το άρθρο 370Β εισήχθη στο ελληνικό δίκαιο με το άρθρο 3 του Ν 1805/1988 στο κεφάλαιο 22^{Ο} του Π.Κ που προστατεύει τα απόρρητα που σχετίζονται με η/υ.[86] Αιτία της δημιουργίας της διάταξης αυτής αποτέλεσε η βιομηχανική κατασκοπεία που αποτέλεσε σοβαρότατο κίνδυνο για την οικονομική ζωή και την επιχειρηματικότητα, ως μορφή εγκληματικότητας μέσω των η/υ.

Η ως άνω διάταξη τιμωρεί την **αθέμιτη** αντιγραφή, την αποτύπωση, τη χρησιμοποίηση, τη γνωστοποίηση και με οποιοδήποτε άλλο τρόπο παρέμβαση σε κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα του δημόσιου ή ιδιωτικού τομέα. Τα παραπάνω απόρρητα υπό μορφή πάντα των στοιχείων ή προγραμμάτων υπολογιστών, συνιστούν το προστατευόμενο **έννομο αγαθό** της παραπάνω διάταξης.

Είναι εμφανές ότι θεμελιώδης έννοια της αντικειμενικής υπόστασης της παραγ 1 του άρθρου 370Β ΠΚ αποτελεί η έννοια του απορρήτου. Στον ορισμό του απορρήτου, κατά την κρατούσα στη θεωρία άποψη υιοθετείται η υποστηριζόμενη ευρέως «μικτή θεωρία».[87] Το **απόρρητο** συναποτελείται από ένα αντικειμενικό στοιχείο, που σημαίνει ότι η πληροφορία δεν πρέπει να είναι γνωστή παρά μόνο σε ένα περιορισμένο κύκλο προσώπων και από

[85] Η παρ 1 του άρθρου 370Β, στο Νέο Ποινικό Κώδικα , Ν. 4619/11 – 6 – 2019(ΦΕΚ 95/11 – 6 – 2019 τ.Α), παραμένει αυτούσια στην παρ 1 του Νέου άρθρου 370Γ.

[86] Στο Νέο Ποινικό Κώδικα (Ν 4619/ 11 – 6 – 2019) στο ίδιο κεφάλαιο όσο και στα ίδια άρθρα 370 – 371, με τίτλο «Προσβολές του ατομικού απορρήτου και της απόρρητης επικοινωνίας» προστατεύονται τα απόρρητα που σχετίζονται με η/υ, τίθεται δε ο τίτλος με βάση το έννομο αγαθό που προστατεύεται από τις περιεχόμενες σε αυτό διατάξεις…

[87] Βασιλάκη Ε. Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών: η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του Ν 1805/88, Αθήνα 1993, σελ 162

ένα υποκειμενικό στοιχείο, που σημαίνει ότι πρέπει να υπάρχει το ενδιαφέρον ενός προσώπου να διατηρηθεί μυστικό. Σύμφωνα με την «**μικτή θεωρία**»[88] για να θεωρηθούν τα στοιχεία και τα προγράμματα του η/υ ως απόρρητα θα πρέπει να συντρέχουν δύο βασικές προϋποθέσεις. Αφενός τα απόρρητα να είναι από τη φύση τους προσιτά σε περιορισμένο κύκλο προσώπων δηλαδή να μην είναι κοινώς γνωστά και αφετέρου να υπάρχει δικαιολογημένο ενδιαφέρον εκ μέρους του νομίμου κατόχου τους να κρατηθούν τα στοιχεία/δεδομένα και τα προγράμματα απόρρητα γεγονός το οποίο καταδεικνύεται από τα τεράστια ποσά που δαπανώνται για την κατασκευή των προγραμμάτων και εκφράζεται και από τα μέτρα προστασίας που λαμβάνονται.

Ο Έλληνας νομοθέτης, όπως προκύπτει από το κείμενο του νόμου έλαβε υπόψη του την παραπάνω κρατούσα και ορθή μικτή θεωρία, κατά την κατάρτιση του άρθρου 370Β Π.Κ. Ωστόσο μια προσεκτική ανάγνωση του εδ.β της παρ 1και δη της έκφρασης «**και εκείνα που....**» θα μπορούσε να δημιουργήσει την εντύπωση ότι δεν αποκλείεται και η προστασία δεδομένων και προγραμμάτων για τα οποία ο κάτοχός τους δεν έχει εκδηλώσει ρητά τη βούλησή του να τα τηρήσει απόρρητα, αλλά ούτε εμφανίζεται κάποιο δικαιολογημένο ενδιαφέρον του κατόχου τους ως προς την τήρηση του απορρήτου π.χ θα μπορούσαν να χαρακτηριστούν ως απόρρητα τα προσωπικά στοιχεία των υπαλλήλων μιας επιχείρησης[89]. Ως προς το ζήτημα αυτό η λύση βρίσκεται στη συσταλτική ερμηνεία της διάταξης με την υιοθέτηση της «**μικτής θεωρίας**» έτσι ώστε να προστατεύονται μόνο εκείνα τα εμπορικά, επιχειρηματικά κλπ απόρρητα, τα οποία και από αντικειμενικής άποψης θεωρούνται απόρρητα και τα οποία χρήζουν προστασίας εξ'αιτίας δικαιολογημένου συμφέροντος και όχι αποκλειστικά επειδή το θέλησε ο νόμιμος κάτοχός τους , ενώ ειδικά για την περίπτωση του βιομηχανικού και εμπορικού απορρήτου, μόνο όταν η συμπεριφορά μπορεί να βλάψει την ανταγωνιστικότητα της επιχείρησης.[90]

[88] Καράκωστας Κ. Ιωάννης: Δίκαιο και Ίντερνετ, Νομικά ζητήματα του διαδικτύου, Αθήνα 2009, σελ 162

[89] Μυλωνόπουλος Χρήστος: Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, σειρά ΠΟΙΝΙΚΑ, Αθήνα 1991, σελ 73

[90] Δημητρίου Δήμητρα: Οι επιθέσεις κατά συστημάτων πληροφοριών: Το Διεθνές Ενωσιακό και Ελληνικό πλαίσιο Προστασίας, Θεσσαλονίκη 2014, σελ 124

10.1.2 Η Έννοια του όρου «αθέμιτα»

Κομβικής σημασίας για την ερμηνεία της διάταξης του άρθρου 370Β παρ 1 είναι ο όρος «**αθέμιτα**» και το ερώτημα που έχει ανακύψει στη θεωρία για το εάν ο όρος αυτός αποτελεί στοιχείο της αντικειμενικής υπόστασης του εγκλήματος ή ειδικό στοιχείο του αδίκου,[91] επί κατάφασης του οποίου υπάρχει και τελικό άδικο.

Αθέμιτα πράττει κάποιος όταν δεν στηρίζεται σε έναν κανόνα δικαίου, ο οποίος να του επιτρέπει την πράξη του αυτή, ενεργεί δηλαδή παράνομα. Αθέμιτα πράττει επίσης και κάποιος που δεν έχει το δικαίωμα να ενεργήσει κατ'αυτόν τον τρόπο[92] ή όπως αναφέρεται χαρακτηριστικά στην Αιτιολογική Έκθεση του σχεδίου ΠΚ του 1933 «άνευ δικαιώματος χορηγούντος την προς τοιαύτην ενέργειαν εξουσίαν».[93]

Υποστηρίζεται[94] ότι κριτήριο για τη διάκριση των στοιχείων της αντικειμενικής υπόστασης από τα «**ειδικά στοιχεία του αδίκου**», θα μπορούσαν να αποτελέσουν τα «**επίπεδα κρίσεως του αδίκου**».

Στο πρώτο επίπεδο της διαπιστωτικής κρίσης του αδίκου(της προσβολής για το έννομο αγαθό) ανήκει η αντικειμενική υπόσταση με τα στοιχεία της, καθώς αυτή «**ενδείχνει**» το κατ'αρχήν άδικο περιγράφοντας την προσβολή του εννόμου αγαθού από τη συμπεριφορά του δράστη. Στο δεύτερο επίπεδο ανήκει η κρίση για το τελικό στάδιο η οποία είναι δευτερογενής καθώς προϋποθέτει την πλήρωση της αντικειμενικής υπόστασης. Σε αυτό το επίπεδο αντιπαρατίθενται τα έννομα αγαθά του δράστη και του θύματος, σταθμίζονται και μέσα από την σχετικότητα της προστασίας τους, προκύπτει το τελικό συμπέρασμα για τον τελικά άδικο χαρακτήρα της πράξης. Δηλαδή συμπερασματικά τα στοιχεία που ανήκουν στο πρώτο επίπεδο κρίσης δείχνουν την προσβολή και αφορούν την προστασία του εννόμου αγαθού, ενώ τα «**ειδικά στοιχεία του αδίκου**», που ανήκουν στο δεύτερο επίπεδο αξιολόγησης, δείχνουν τη δικαιολόγηση της προσβολής και λειτουργούν υπέρ του δράστη.[95]

---

[91] Λαμπάκη Χρ σε Χαραλαμπάκη Αρισ : Ποινικός Κώδικας, ερμηνεία κατ'άρθρο τομ Β, σελ 2960

[92] Λαμπάκη σε Χαραλαμπάκη Αρισ: Ποινικός Κώδικας, ερμηνεία κατ'άρθρο τομ Β, σελ 2960

[93] Αιτ Εκθ ΣχΠΚ 1933 σελ 549-550

[94] Μανωλεδάκης Ιωάννης : Ποινικό Δίκαιο, Επιτομή Γενικού Μέρους, 2005,σελ 604

[95] Δημητρίου Δήμητρα : Οι επιθέσεις κατά συστημάτων πληροφοριών: Το Διεθνές Ενωσιακό και Ελληνικό πλαίσιο προστασίας, Θες/νίκη 2014, σελ 124

Η **νομολογία** του **ΑΠ,**[96] σε σχέση με το αμφιλεγόμενο ζήτημα εάν ο όρος **αθέμιτα** αποτελεί στοιχείο της αντικειμενικής υπόστασης ή ειδικό στοιχείο του αδίκου φαίνεται να κατατείνει προς τη δεύτερη εκδοχή. Από τη θεωρία ωστόσο έχει διατυπωθεί[97] η[98] άποψη ότι η «συναίνεση του ομιλούντος» από τη στιγμή που καταργεί εννοιολογικά την «**παγίδευση**» ή την «**παρέμβαση**», συνιστά λόγο αποκλεισμού της αντικειμενικής υπόστασης, από τη στιγμή μάλιστα που έχουμε να κάνουμε με ένα ατομικό έννομο αγαθό του οποίου ο φορέας έχει την εξουσία διάθεσης. Συνεπώς κατ'αυτήν την άποψη συνιστά στοιχείο της αντικειμενικής υπόστασης του εγκλήματος του αρθ. 370Β παρ 1.

Η πρακτική σημασία της διάκρισης αυτής εντοπίζεται κυρίως σε ζητήματα πλάνης, καθώς ανάλογα με την επιλογή που θα ακολουθήσει κανείς θα οδηγηθεί σε διαφορετική μορφή πλάνης.[99] Έτσι εάν ο όρος αθέμιτα θεωρηθεί στοιχείο της αντικειμενικής υπόστασης του εγκλήματος , τυχόν πλάνη του δράστη ως προς αυτό θα είναι πραγματική πλάνη. Εάν αντίθετα, θεωρήσουμε τον όρο αθέμιτα ειδικό στοιχείο του αδίκου, τυχόν πλάνη του δράστη ως προς αυτό θα είναι νομική πλάνη και ο δράστης θα πρέπει να αποδείξει και το συγγνωστό αυτής προκειμένου να κριθεί ατιμώρητος και ως εκ τούτου η θέση του ως κατηγορουμένου θα είναι δυσχερέστερη.[100]

10.2 Η έννοια του απορρήτου στο άρθρο 370Β ΠΚ

Στο άρθρο 370Β ΠΚ υιοθετείται η υποστηριζόμενη ευρέως «**μικτή θεωρία**» περί απορρήτου. Σύμφωνα για την ως άνω θεωρία για να θεωρηθεί ένα γεγονός «απόρρητο» πρέπει να συντρέχουν δύο βασικές προϋποθέσεις Ι/τα απόρρητα να είναι από τη φύση τους γνωστά σε περιορισμένο αριθμό προσώπων και ΙΙ/Να υπάρχει δικαιολογημένο ενδιαφέρον εκ μέρους του φορέα του να κρατηθεί το γεγονός αυτό ως απόρρητο, το οποίο να αποδεικνύεται αφενός από την ύπαρξη συμφέροντος (επαγγελματικής, οικονομικής κλπ φύσεως) και αφετέρου από τη βούληση του κατόχου τους να διατηρηθεί απόρρητο.

Ως **κρατικά απόρρητα** ορίζονται τα περιστατικά εκείνα με πρωτογενή σπουδαιότητα για την ίδια την κρατική υπόσταση και που κατά τη βούληση

[96] ΑΠ 1607/2007 Ποινικό Δίκαιο 2008, σελ 831
[97] Ανδρουλάκη Ν: Ποινικό Δίκαιο – Γενικό Μέρος (Θεωρία για το έγκλημα) 2η εκδ. 2006 , σελ 355
[98] Μανωλεδάκη Ιωαν : Ποινικό Δίκαιο – Γενική θεωρία, Αθήνα – Θεσσαλονίκη, 2004, σελ 851
[99] Λαμπάκη Χρ σε Χαραλαμπάκη Αριστ: Ποινικός Κώδικας. Ερμηνεία κατ'άρθρο τόμος Β, σελ 2961
[100] Γκότση Μαρίνα: Το ηλεκτρονικό έγκλημα στην ελληνική έννομη τάξη, Θεσσαλονίκη 2018, σελ 52

της Κυβέρνησης – λόγω της φύσης τους – δεν πρέπει να γίνονται γνωστά σε πρόσωπα που βρίσκονται έξω από το στενό υπηρεσιακό κύκλο γιατί η αποκάλυψή τους μπορεί να βλάψει σοβαρά συμφέροντα του κράτους.[101]

Ως **Απόρρητα Επιχείρησης** του δημόσιου ή ιδιωτικού τομέα θεωρούνται εκείνα που αναφέρονται στην κάτοχό τους επιχείρηση και αποτελούν συνήθως και επαγγελματικά απόρρητα.

Στη συνέχεια ως **επιστημονικά απόρρητα** θα μπορούσαν να θεωρηθούν αυτά που περιέχουν συστηματικές γνώσεις που αφορούν κάποιο γνωστικό αντικείμενο και έχουν υπαχθεί σε συγκεκριμένη συστηματική – μεθοδολογική κατάταξη, όπως είναι π.χ η διδακτορική διατριβή, η μελέτη, τα άρθρα κλπ.

Όσον αφορά πάντως κάποιες **ειδικότερες εκφάνσεις** του κρατικού απορρήτου και συγκεκριμένα τα στρατιωτικά και διπλωματικά απόρρητα ή τα απόρρητα που αναφέρονται στην ασφάλεια του κράτους εφαρμόζεται η παρ 3 του άρθρου 370Β ΠΚ.

Νόμιμος κάτοχος του απορρήτου είναι αυτός που βάσει νόμου ή σύμβασης το έχει στη φυσική του εξουσία και πρέπει να διακρίνεται από το δικαιούχο του απορρήτου. Πχ ο γιατρός που έχει την προσωπική καρτέλα του ασθενούς με στοιχεία της αρρώστιας του είναι κάτοχος του απορρήτου ενώ ο ασθενής είναι δικαιούχος. Κατά την νομολογία[102] όσον αφορά τα στοιχεία ή τα προγράμματα Η/Υ υποστηρίζεται ότι κάτοχος είναι εκείνος που έχει τη δυνατότητα εξουσίασης των στοιχείων ενός προγράμματος, η οποία συνίσταται στη δυνατότητα προσπέλασης, χρήσης ή διάθεσης των στοιχείων αυτού και στηρίζεται σε ένα νόμιμο δικαίωμα.

Η συγκατάθεση του νόμιμου κατόχου αποκλείει την αντικειμενική υπόσταση του εγκλήματος.[103]

10.3 Προστατευόμενο έννομο αγαθό του άρθρου 370Β ΠΚ

Στο άρθρο 370Β ΠΚ προστατεύεται το απόρρητο(κρατικό ,επιστημονικό, επαγγελματικό ή απόρρητο επιχείρησης του δημοσίου ή του ιδιωτικού

[101] Λαμπάκη Χ σε Χαραλαμπάκη Αριστοτέλη :Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο , τομ. Δεύτερος σελ 2980 με περαιτέρω παραπομπή σε Κονταξή Α,2000, σελ 3149

[102] Λαμπάκη Χ σε Χαραλαμπάκη Αριστοτέλη: Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο, τομ. Δεύτερος σελ 2980 και Συμβ Εφ.Αθ.2949/2003

[103] Λαμπάκη Χ σε Χαραλαμπάκη Αριστοτέλη: Κώδικας, Ερμηνεία κατ'άρθρο, τομ. Δεύτερος, σελ 2981. Ποιν. Δικ 2004, σελ 1110

τομέα) που έχει τη μορφή στοιχείου ή προγράμματος Η/Υ[104] καλύπτοντας έτσι τις περιπτώσεις της διαδεδομένης εμπορικής, βιομηχανικής, επιχειρησιακής κλπ κατασκοπείας. Κατ' άλλους υποστηρίζεται επίσης και η άποψη ότι προστατεύεται το έννομο αγαθό της περιουσίας ως συνόλου.[105] Ωστόσο η διάταξη του άρθρου 370Β ΠΚ δεν αναφέρει ως απαραίτητο στοιχείο την οικονομική αξία των προστατευόμενων απορρήτων και συνακόλουθα αποσυνδέει τα απόρρητα από την περιουσιακή τους ιδιότητα.[106]

10.4 Αντικειμενική υπόσταση του άρθρου 370Β ΠΚ

Δράστης «υποκείμενο τέλεσης» του εγκλήματος μπορεί να είναι ο οποιοσδήποτε («**όποιος**»). Όταν όμως ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων τότε εφαρμόζεται η παρ 2 του άρθρου 370Β ΠΚ. Αναφορικά με την «εγκληματική συμπεριφορά» στην παρ1 μνημονεύονται πέντε υπαλλακτικοί τρόποι τέλεσης του εγκλήματος(αντιγραφή, αποτύπωση, χρησιμοποίηση, αποκάλυψη και παραβίαση στοιχείων ή προγραμμάτων υπολογιστών).[107]

10.5 Υπαλλακτικοί τρόποι τέλεσης του εγκλήματος

Προχωρώντας στα στοιχεία της αντικειμενικής υπόστασης του αδικήματος του άρθρου 370Β παρ.1 αξίζει να σημειωθεί ότι αυτό τελείται με πέντε διαφορετικούς τρόπους τέλεσης, και συγκεκριμένα με αντιγραφή, αποτύπωση, χρησιμοποίηση, αποκάλυψη σε τρίτον και η οπωσδήποτε παραβίαση στοιχείων ή προγραμμάτων υπολογιστών. Με τον όρο «**αντιγραφή**» εννοείται στην ουσία η αναπαραγωγή με την έννοια της ενσωμάτωσης του στοιχείου ή του προγράμματος σε υλικό φορέα, χωρίς να συνιστά απαραίτητη προϋπόθεση η χρήση τεχνικών μέσων (με σχεδιασμό ή

[104] Λαμπάκη Χ σε Χαραλαμπάκη Αριστοτέλη:Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο, τομ. Δεύτερος, σελ 2977

[105] Κωνσταντινίδης Άγγελος: Η διακεκριμένη παραβίαση απόρρητων στοιχείων, Ποιν. Χρονικά 1997, 1216

[106] Βασιλάκη Ειρήνη: "Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών"Η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του Ν 1805/88, Ποινικά 40, Αθήνα 1993

[107] Λαμπάκη Χ σε Χαραλαμπάκη: Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο, τόμος Δεύτερος, σελ 2977

γραφή). Ακόμη και η φόρτωση ενός προγράμματος από έναν εξωτερικό φορέα στην εσωτερική μνήμη του η/υ μπορεί να θεωρηθεί ως αντιγραφή.[108]

Ως «**αποτύπωση**» θα μπορούσε να ορισθεί η αναπαραγωγή ενός ενσώματου (μόνιμου) αντιγράφου του προγράμματος ή των δεδομένων από κάποιο προϋπάρχον πρωτότυπο (π.χ με φωτοτύπηση). Αποτελεί ένα είδος αντιγραφής με την έννοια της μόνιμης αναπαράστασης του απορρήτου. Ως αποτύπωση θα μπορούσε να θεωρηθεί, με τα σημερινά δεδομένα της τεχνολογίας και η μεταφορά στοιχείων ή προγραμμάτων από τον η/υ του θύματος σε μια εξωτερική μονάδα αποθήκευσης (μονάδες cd/dvd, μονάδα σκληρού δίσκου, συσκευές αποθήκευσης usb).

Ως «**χρησιμοποίηση**» των απορρήτων στοιχείων ή προγραμμάτων υπολογιστών νοείται η χρήση αυτών σύμφωνα με το λειτουργικό προορισμό τους. Η χρησιμοποίηση μπορεί να συνίσταται και στην εμπορική του εκμετάλλευση με σκοπό το όφελος. Θα ήταν ωστόσο χρήσιμο να αντιληφθούμε την έννοια με έναν επιπρόσθετο όρο αυτόν της αξιοποίησης ώστε να αποφεύγεται η τιμώρηση πράξεων που δεν επισύρουν κανένα κίνδυνο για κάποιο έννομο αγαθό.

Ως «**αποκάλυψη** σε τρίτον» νοείται η με οποιονδήποτε τρόπο μερική ή ολική γνωστοποίηση του λογισμικού ή των στοιχείων, με τέτοιο τρόπο που να επιτρέπει την εκμετάλλευσή τους.[109] Για την τέλεση της αποκάλυψης δεν απαιτείται η εκ μέρους του δράστη γνώση του περιεχομένου των απορρήτων, σε κάθε περίπτωση πάντως το τρίτο πρόσωπο πρέπει να λαμβάνει άμεσα γνώση των δεδομένων ή των προγραμμάτων, δηλαδή από μόνη την ενέργεια της αποκάλυψης χωρίς να απαιτείται κάποια περαιτέρω ενέργεια από την πλευρά του. Έτσι ως αποκάλυψη μπορεί να θεωρηθεί η αποκάλυψη σε τρίτο ενός κρίσιμου κωδικού (password), ενώ έχει κριθεί ως τέτοια και η έναντι αμοιβής παραχώρηση σε διαφημιστή που έχει αναλάβει διαφημιστική καμπάνια, του πελατολογίου της εγκαλούσας εταιρίας.

Με την γενική περιγραφή «**οπωσδήποτε παραβιάζει**» στοιχεία και προγράμματα η/υ, με την έννοια της με οποιονδήποτε τρόπο παραβίασης των απορρήτων. Αυτός ο γενικόλογος τρόπος τέλεσης έχει επικριθεί από τη θεωρία για υπερβολική διεύρυνση του αξιοποίνου. Αυτή η διατύπωση του γενικόλογου τρόπου τέλεσης, είναι φανερό πως ήταν επιλογή του νομοθέτη και έγινε με σκοπό την κάλυψη περιπτώσεων που εξ'αιτίας της ραγδαίας

[108] Μυλωνόπουλος Χρήστος: Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, σειρά ΠΟΙΝΙΚΑ, Αθήνα 1991, σελ 74

[109] Λαμπάκη Χρ σε Χαραλαμπάκη Αρισ, Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο , τομ. 2ος ,σελ 2978 με περαιτέρω παραπομπή σε Ανδρέου Φ,2005,σελ 1505

τεχνολογικής εξέλιξης δεν θα μπορούσαν πιθανόν να υπαχθούν σε έναν από τους προηγούμενους τρόπους.

Αυτή η γενική διατύπωση, στη θεωρία έχει υποστηριχθεί ορθά,[110] [111] ότι δημιουργεί κίνδυνο υπερβολικής διεύρυνσης του αξιόποινου από την αόριστη περιγραφή της, για αυτό το λόγο θα πρέπει ο όρος «**οπωσδήποτε παραβιάζει**» να ερμηνευτεί περιοριστικά, ώστε η βαρύτητα της πράξης της παραβίασης να είναι ανάλογη με την απαξία των ρητά προαναφερομένων στην παρ 1 πέντε τρόπων τέλεσης του εγκλήματος (αντιγραφή, αποτύπωση, χρησιμοποίηση, αποκάλυψη και παραβίαση στοιχείων ή προγραμμάτων υπολογιστών).

Στο άρθρο 370Β ΠΚ προστατεύονται, όπως ρητά προβλέπεται στην παρ1, τα κρατικά, επιστημονικά, επαγγελματικά απόρρητα καθώς και τα απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα. Στο εδ.β της παρ1 φαίνεται όμως ότι ο νομοθέτης επεκτείνει την έννοια του προστατευόμενου απορρήτου προσθέτοντας και όλα εκείνα που ο νόμιμος κάτοχός τους **από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα**. Μια όμως τέτοια εκδοχή απορρήτου καλύπτει ολοκληρωτικά το πεδίο εφαρμογής της παρ.2 του άρθρου 370Γ ΠΚ με αποτέλεσμα να μη καταλείπεται κανένα νόημα στην ύπαρξη του τελευταίου. Για το λόγο αυτό υποστηρίζεται ότι η εφαρμογή του άρθρου 370Β ΠΚ πρέπει να περιοριστεί σε περιπτώσεις «παράνομης διείσδυσης» μόνο σε κρατικά, επιστημονικά, επαγγελματικά ή επιχειρησιακά απόρρητα, καλύπτοντας έτσι τις περιπτώσεις της διαδεδομένης εμπορικής, βιομηχανικής κλπ κατασκοπείας.[112] [113]

Επί της ανωτέρω απόψεως έχει υποστηριχθεί και η αντίθετη άποψη, σύμφωνα με την οποία, πλην των κρατικών, επιστημονικών κλπ απορρήτων, προστατεύονται και όλα εκείνα που ο νόμιμος κάτοχος από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα.[114] [115] Στην περίπτωση όμως αυτή αναγνωρίζεται η αναγκαιότητα ο όρος «δικαιολογημένο ενδιαφέρον» να αποτελεί ασφαλιστική δικλείδα, ούτως ώστε το αξιόποινο να μην εξαρτάται μόνο από το υποκειμενικό στοιχείο της

[110] Καιάφα – Γκμπάντι Μαρία: Ποινικό δίκαιο και καταχρήσεις πληροφορικής Αρμ/2007 σελ 1071

[111] Μυλωνόπουλος Χρήστος: Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, σειρά ΠΟΙΝΙΚΑ, Αθήνα 1991, σελ 77

[112] Λαμπάκης Χρ σε Χαραλαμπάκη: Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο, τόμος Δεύτερος, σελ 2979

[113] Καϊάφα – Γκμπάντι Μ. Ποινικό δίκαιο και καταχρήσεις της πληροφορικής Αρμ 2007, σελ 1058

[114] Βασιλάκη Ειρήνη: Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών:η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του Ν 1805/88. Σειρά ΠΟΙΝΙΚΑ, Αθήνα 1993,σελ 174

[115] Μαργαρίτης Μ: «Ποινικός Κώδικας» Ερμηνεία-Εφαρμογή, 2009,σελ 1033

θέλησης του κατόχου των πληροφοριών αλλά και από το αντικειμενικό στοιχείο του δικαιολογημένου ενδιαφέροντος.

10.6 Η Υποκειμενική υπόσταση του άρθρου 370Β ΠΚ

Το άρθρο 370Β είναι πλημμέλημα αφού ο δράστης του εγκλήματος τιμωρείται με φυλάκιση(άρθρο 18 εδ.β) και αφού ο Νόμος δεν προβλέπει ειδικά ότι τιμωρείται και όταν τελείται από αμέλεια (άρθρο 26 παρ 1 ΠΚ), τιμωρείται μόνο όταν τελείται με δόλο.[116]
Απαιτείται οποιοδήποτε είδος δόλου (αρκεί και ο ενδεχόμενος)[117] που πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος, καθώς δεν απαιτείται από το νόμο να τελούνται οι πράξεις εν γνώσει ορισμένων περιστατικών(άρθρο 27 ΠΚ).

10.7 Η διακεκριμένη μορφή της παρ.2 του άρθρου 370Β ΠΚ

Σύμφωνα με την παρ 2 του άρθρου 370Β[118]
"*Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας επιβάλλεται φυλάκιση τουλάχιστον ενός έτους*."
Η παρ 2 του άρθρου 370Β ΠΚ περιλαμβάνει δύο περιπτώσεις που επιβαρύνουν το αξιόποινο και εξ'αυτού του λόγου επιβολής αυξημένης ποινής σε σχέση με το βασικό έγκλημα. Ειδικότερα η διακεκριμένη μορφή του εγκλήματος του άρθρου 370Β συντρέχει Ι/ όταν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων και ΙΙ/όταν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας.
Όσον αφορά στην πρώτη περίπτωση "στην υπηρεσία του κατόχου των στοιχείων", θεωρείται ότι βρίσκεται ο δράστης όταν συνδέεται με τον κάτοχο των στοιχείων με οποιαδήποτε σχέση εξαρτημένης ή ανεξάρτητης εργασίας ή ακόμη και με σύμβαση έργου, ανεξαρτήτως αν η εργασία αυτή ανήκει στον δημόσιο ή ιδιωτικό τομέα.[119]

[116] Δημητρίου Δήμητρα: Οι επιθέσεις κατά συστημάτων πληροφοριών :Το Διεθνές Ενωσιακό και Ελληνικό πλαίσιο Προστασίας, Θεσσαλονίκη 2014,σελ 130
[117] Λαμπάκης Χ σε Χαραλαμπάκη Αριστοτέλη :Ποινικός Κώδικας, ερμηνεία κατ'άρθρο, τόμος β, σελ 2981
[118] Η παρ 2 του άρθρου 370Β, στον Νέο Ποινικό Κώδικα Ν. 4619/ 11-6-2019 (ΦΕΚ 95/ 11-6-2019 τ.Α), παραμένει αυτούσια στην παρ 2 του Νέου άρθρου 370Γ.
[119] Λαμπάκη Χ σε Χαραλαμπάκη Αριστοτ: Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο, τομ. 2ος,σελ 2981, με περαιτέρω παραπομπή σε Κωστάρα Α, 2007,σελ 1027

Ωστόσο με την ερμηνεία αυτή ένας ευρύς κύκλος προσώπων, όπως τα πρόσωπα του ΔΣ της επιχείρησης, δεν μπορούν να ενταχθούν στην παρ 2του άρθρου 370Β ΠΚ,[120] μολονότι στην πράξη αυτά τα πρόσωπα διαδραματίζουν πολλές φορές καθοριστικό ρόλο στη διοικητική δομή και στην οργανωτική λειτουργία της επιχείρησης.

Η νομολογία αντίστοιχα με τις αποφάσεις της τείνει προς την υιοθέτηση ευρείας ερμηνείας της έννοιας του εργαζομένου. Συγκεκριμένα έχει κριθεί[121] ότι «στην υπηρεσία του κατόχου των στοιχείων», ήταν ο υπάλληλος της εγκαλούσας εταιρίας, ο οποίος εργαζόταν ως αναλυτής – προγραμματιστής και εξ'αιτίας της ειδικότητάς του αυτής είχε τη δυνατότητα πρόσβασης στα καταχωρημένα στον Η/Υ της εταιρίας στοιχεία. Αλλά και η ΑΠ[122] δέχθηκε ότι οι κατηγορούμενοι η πρώτη υπάλληλος με σύμβαση εξαρτημένης εργασίας σε γραφείο γενικού τουρισμού και ο δεύτερος τεχνικός στον οποίο είχε ανατεθεί από την εγκαλούσα εταιρία η συντήρηση, η επισκευή και η ενημέρωση των Η/Υ της επιχείρησης, όντες στην υπηρεσία του κατόχου από κοινού αντέγραψαν σε δισκέτες το πελατολόγιο της επιχείρησης (επαγγελματικό της απόρρητο) και αποχωρώντας από αυτή ίδρυσαν άλλη ανταγωνιστική εταιρία με όμοιο αντικείμενο, διαπράττοντας έτσι την επιβαρυντική περίπτωση της παρ 2 του άρθρου 370Β.

Στη δεύτερη περίπτωση διακεκριμένης μορφής η οικονομική αξία του προσβαλλόμενου αγαθού είναι αυτή που επιτείνει την επιβληθείσα ποινή. Για τη συνδρομή της περίπτωσης της «**ιδιαίτερα μεγάλης οικονομικής σημασίας**» του (παραβιαζόμενου) απορρήτου θα πρέπει να υπάρχει δυνατότητα οικονομικής αποτίμησης της αξίας τους με βάση συγκεκριμένα στοιχεία.[123]

Η οικονομική διάσταση του απορρήτου, σύμφωνα με την ορθότερη άποψη, με το «φορέα του», δηλαδή με βάση την επιχείρηση που ζημιώνεται από την πράξη και όχι με βάση το όφελος του τρίτου.

Από άλλους[124] [125]υποστηρίζεται η άποψη ότι ο προσδιορισμός μπορεί να γίνει και με βάση το όφελος του τρίτου.

---

[120] Μυλωνόπουλος Χρήστος : "Ηλεκτρονικοί Υπολογιστές και ποινικό δίκαιο", Ποινικά 33, Αθήνα-Κομοτηνή 1991, σελ 84

[121] Συμβ.Εφ.Αθ. 217/1997 Βούλευμα Υπερ. 1997,846

[122] ΑΠ 121/2003 Ποιν. Δικ 2003,619,Ποιν.Χρον. 2003, 846

[123] Συμβ Εφ.Αθ 217/1997 Υπέρ 1997,846

[124] Κωνσταντινίδης Α. Η διακεκριμένη παραβίαση απορρήτων στοιχείων Ποινικά Χρονικά 1997,σελ 1216

[125] Κονταξής Α «Ποινικός Κώδικας», Τόμος ΙΙ,2000, σελ 3147 - 3148

10.8 Η παραβίαση στρατιωτικών – διπλωματικών απορρήτων αρθρ. 370Β παρ 3.[126]

Σύμφωνα με την παρ 3 του άρθρου 370Β «*Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147*.»
Στην παρ 3 του άρθρου 370Β γίνεται ρητή παραπομπή στα άρθρα 146 και 147 του ΠΚ, ως προς το κυρωτικό μέρος, ειδικά για τα στρατιωτικά ή διπλωματικά απόρρητα ή τα απόρρητα που αναφέρονται στην ασφάλεια του κράτους. Η παραπομπή αυτή στο άρθρο 146 ΠΚ πρακτικά σημαίνει την αυστηρότερη τιμωρία του δράστη που τελεί το πλημμέλημα του άρθρου 370Β ΠΚ, σε συνδυασμό με την προσβολή στρατιωτικών ή διπλωματικών απορρήτων.
Με την παραπομπή όμως αυτή στο άρθρο 146 ΠΚ[127] όχι μόνο δεν τιμωρείται αυστηρότερα ο δράστης αλλά αντίθετα επί της ουσίας μένει ατιμώρητος για το άδικο που εμπεριέχεται στη διάταξη του 370Β ΠΚ. Διότι καθώς τιμωρείται ένα ατομικό έννομο αγαθό, με μια διάταξη που προστατεύει ένα κρατικό έννομο αγαθό και συγκεκριμένα την ασφάλεια του κράτους, προκαλείται σύγχυση ως προς το έννομο αγαθό.

Αναφορικά δε με το άρθρο 147 ΠΚ[128] (**παραβίαση μυστικών της πολιτείας από αμέλεια**) θεωρείται ότι εκ παραδρομής γίνεται παραπομπή σε ένα έγκλημα αμέλειας καθώς στο άρθρο 370Β ΠΚ δεν τυποποιείται η τέλεση της παραβίασης του απορρήτου από αμέλεια,[129] ενώ η πραγματική βούληση του νομοθέτη ήταν προφανώς να παραπέμψει στο αμέσως

[126] Η παρ 3 του άρθρου 370Β, στο Νέο Ποινικό Κώδικα Ν 4619/11-6-2019 (ΦΕΚ 95/11-6-2019 τ.Α), καταργείται εντελώς

[127] 1. «Όποιος με πρόθεσή του και παράνομα παραδίδει ή αφήνει να περιέλθουν στην κατοχή ή τη γνώση του άλλου έγγραφα, σχέδια ή άλλα πράγματα ή ειδήσεις που τα συμφέροντα της πολιτείας των συμμάχων της επιβάλλουν να τηρηθούν απόρρητα απέναντι σε ξένη κυβέρνηση, τιμωρείται με κάθειρξη μέχρι δέκα ετών»
2.«Σε καιρό πολέμου ο υπαίτιος τιμωρείται με ισόβια ή πρόσκαιρη κάθειρξη μέχρι δέκα ετών»

[128] «Όποιος γίνεται από αμέλεια υπαίτιος κάποιας από τις πράξεις που αναφέρονται στο προηγούμενο άρθρο, αν αυτά τα σχέδια, τα έγγραφα, τα πράγματα ή οι ειδήσεις του είναι εμπιστευμένα υπηρεσιακώς ή του είναι προσιτά χάρη στη δημόσια υπηρεσία του ή χάρη σε εντολή της αρχής ή το έμαθε λόγω μιας σύμβασης από εκείνες που αναφέρονται στο άρθρο 145 του Κώδικα τιμωρείται με φυλάκιση μέχρι τριών ετών»

[129] Γκότση Μαρίνα: Το ηλεκτρονικό έγκλημα στην ελληνική έννομη τάξη. Οι προσβολές κατά των συστημάτων πληροφοριών και η ποινική αντιμετώπισή τους κατά το ελληνικό και ενωσιακό δίκαιο, Θεσσαλονίκη 2018, σελ 58

επόμενο αδίκημα της κατασκοπείας που προβλέπεται στο άρθρο 148 ΠΚ. Έτσι η παραπομπή στο άρθρο 147 ΠΚ είναι άνευ εφαρμογής και ουσίας, καθώς δεν μπορεί, κατά την ορθή ερμηνεία της διάταξης, να νοηθεί η τέλεση του αδικήματος από αμέλεια.[130]

ΚΕΦΑΛΑΙΟ 11^{Ο}

11. ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΑΡΘΡΟΥ 370Γ παρ 1 ΠΚ

Το αδίκημα της παρ 1 του άρθρου 370Γ ΠΚ, έχει παραμείνει αυτούσιο από το έτος 1988, οπότε και εισήχθη.
Η παραπάνω διάταξη του άρθρου 370Γ παρ 1 έχει ως κάτωθι :
«*Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή «διακοσίων ενενήντα(290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ*».
Γίνεται αντιληπτό ότι η παρ.1 του άρθρου 370 ΠΚ[131] έχει στενό υλικό αντικείμενο καθ΄ότι θεμελιώνει αξιόποινο για όποιον χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα ηλεκτρονικών υπολογιστών. Στην παράγραφο λοιπόν αυτή προστατευόμενο έννομο αγαθό είναι τα προγράμματα ηλεκτρονικών υπολογιστών.
Με το άρθρο 370Γ παρ 1 στοιχειοθετείται η αξιόποινη συμπεριφορά όταν «**χωρίς δικαίωμα**» ο δράστης εν όλω ή εν μέρει, αντιγράφει δηλαδή ενσωματώνει σε κάποιον υλικό φορέα το πρόγραμμα, ώστε να μπορεί να γίνει κατανοητό άμεσα ή έμμεσα από τον άνθρωπο ή «χρησιμοποιεί» δηλαδή εκμεταλλεύεται – απολαμβάνει τις ωφέλειες των λειτουργιών του προγράμματος, το εκτελεί.[132]

---

[130] Λαμπάκη ΧΡ σε Χαραλαμπάκη Αριστοτέλη, Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο, Ειδικό μέρος, Τόμος Δεύτερος, σελ 2980

[131] Η παρ 1 του άρθρου 370Γ στο Νέο Ποινικό Κώδικα Ν 4619/11-6-2019 (ΦΕΚ 95/11-6-2019 τ.Α) αποτυπώνεται τροποποιημένη στην παρ 1 του άρθρου 370Δ, ως κάτωθι:" Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας"
Τροποποιείται συνεπώς η παραπάνω παραγρ του προηγούμενου άρθρου 370Γ "ως προς το ύψος των ποινών και ως προς το είδος αυτής".

[132] Κιούπη Δ: Ποινικό Δίκαιο και ίντερνετ, Αθήνα – Κομοτηνή, 1999, σελ 141

Την πράξη της παρ 1 τελεί και ο δράστης που χρησιμοποιεί τα προγράμματα του ηλεκτρονικού υπολογιστή για να διεκπεραιώνει υποθέσεις που δεν ανήκουν στον κύκλο εργασιών του εργοδότη του η κοινώς λεγόμενη «κλοπή χρόνου ή time theft».[133]

Προστατευόμενο έννομο αγαθό στην παρ.1 είναι «τα προγράμματα ηλεκτρονικών υπολογιστών» ως περιουσιακό αγαθό και μάλιστα η οικονομική αξία της πληροφορίας. Στην εισηγητική έκθεση του Ν. 1805/1988, ο οποίος αποτέλεσε αναμφίβολα το ελληνικό ποινικό δίκαιο πληροφορικής και θεσπίστηκε για να καλύψει τα κενά που δημιουργήθηκαν με τη ραγδαία εξέλιξη της τεχνολογίας και την ευρεία χρήση του ηλεκτρονικού υπολογιστή, αναφέρεται σαφώς πως «κρίθηκε αναγκαία η θέσπιση της διάταξης αυτής αν ληφθεί υπ'οψιν η μεγάλη δαπάνη η οποία απαιτείται για την παραγωγή προγραμμάτων καθώς και οξύτατος ανταγωνισμός που έχει αναπτυχθεί στον κλάδο αυτό».

Μπορούμε με βεβαιότητα να πούμε ότι με την διάταξη της παρ 1 δεν προστατεύεται το μηχανικό μέρος «hardware» του ηλεκτρονικού υπολογιστή αλλά το λογισμικό «software» δηλαδή τα προγράμματα και τα δεδομένα που έχουν αποθηκευθεί στη μνήμη του ηλεκτρονικού υπολογιστή ή των περιφερειακών συσκευών του. Προστατεύεται δε οποιαδήποτε είδος προγράμματος α/ανεξαρτήτως του αν συγκεντρώνει τα χαρακτηριστικά του έργου πνευματικής ιδιοκτησίας β/ανεξαρτήτως του αν είναι απόρρητο και γ/ανεξαρτήτως συγκεκριμένης οικονομικής αξίας.[134]

Ως πρόγραμμα ηλεκτρονικού υπολογιστή θα πρέπει να αναφερθεί πως νοείται[135] μια ενότητα οδηγιών και κανονισμών που περιέχουν τα αναγκαία στοιχεία για τη λύση ενός προβλήματος και κατατάσσονται σε τρεις κατηγορίες α/ανάλογα με την βαθμίδα ανάπτυξής τους : σε πηγαία ή σε αντικειμενικά προγράμματα, β/ανάλογα με το ποιος είναι ο αποδέκτης του υπολογιστή ή χρήστης σε: προγράμματα συστημάτων ή εφαρμογών αντίστοιχα και γ/ανάλογα με τον αριθμό των προσώπων που τα χρησιμοποιούν σε: ατομικά και προγράμματα για πολλούς χρήστες.

[133] Μυλωνόπουλος Χ: Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Αθήνα – Κομοτηνή 1991, σελ 89

[134] Βλαχόπουλος Κ: «Ηλεκτρονικό έγκλημα. Μορφές – Πρόληψη – Αντιμετώπιση» 2007, σελ 217

[135] Φιλόπουλος Π.:Ποινική προστασία Απορρήτου, συστηματική ερμηνεία άρθρων 370 – 371 ΠΚ, Αθήνα – Θεσσαλονίκη 2015, σελ 174

11.1 Το άρθρο 370Γ παρ.2 ΠΚ – Διακρίσεις και χαρακτηρισμοί

Η πλέον σημαντική διάταξη για την προστασία του απορρήτου στον χώρο των ηλεκτρονικών υπολογιστών και της επικοινωνίας μέσω Διαδικτύου είναι το άρθρο 370Γ παρ2 του ΠΚ.[136] Η διάταξη αυτή προστέθηκε με το άρθρο 4 του Ν 1805/1988 και σκοπό έχει την τιμωρία της χωρίς δικαίωμα πρόσβασης σε συστήματα πληροφοριών ή σε προγράμματα Η/Υ.
Η διάταξη του άρθρου 370Γ παρ 2 , έχει ως κάτωθι:
"*Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών παραβιάζοντας απαγορεύσεις ή μέτρα ασφάλειας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση .Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148."*
Η διάταξη του αρ. 370Γ παρ.2 συνιστά κυρωτικό ποινικό κανόνα ο οποίος εμπεριέχει προστακτικό – απαγορευτικό κανόνα, καθόσον ο νομοθέτης απαγορεύει την χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα ή στα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών. Η πράξη της παράνομης πρόσβασης της παρ. 2 συνιστά κοινό έγκλημα αφού υποκείμενο μπορεί να είναι οποιοδήποτε πρόσωπο («όποιος»), ενώ η παρ.3 του αρ. 370Γ [137]που αναφέρει πως "*Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του*", συνιστά μη γνήσιο ιδιαίτερο έγκλημα, καθώς ο δράστης απαιτείται να είναι στην υπηρεσία του νομίμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων. Πρόκειται δε για έγκλημα ενέργειας,[138] καθώς το προστατευόμενο έννομο αγαθό πλήττεται με κάποια μυϊκή κίνηση του δράστη αντιληπτή με τις αισθήσεις η οποία επιφέρει ως μεταβολή στον εξωτερικό κόσμο την πρόσβαση στο πληροφοριακό

[136] Η παραγ 2 του άρθρου 370Γ στο Νέο Ποινικό Κώδικα Ν. 4619/11-6-2019 (ΦΕΚ 95/11-6-2019 τ.Α) αποτυπώνεται τροποποιημένη στην παρ 2 του άρθρου 370Δ, ως κάτωθι:
" Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση"
Κατά συνέπεια αφαιρέθηκε το εδαφ. 2 της παρ 2 του προηγούμενου άρθρου 370Γ που ανέφερε ότι "Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148"
[137] Η παραγ 3 του άρθρου 370Γ στο Νέο Ποινικό Κώδικα Ν 4619/11-6-2019 (ΦΕΚ 95/11-6-2019 τ.Α), παραμένει αυτούσιο στην παρ 3 του Νέου άρθρου 370Δ.
[138] Μυλωνόπουλος Χρήστος: Ποινικό Δίκαιο – Γενικό Μέρος Ι, 2007,σελ 153

σύστημα ή στα στοιχεία που μεταδίδονται. Η παραβίαση του εν λόγω απαγορευτικού πρωτεύοντος κανόνα («μην αποκτήσεις χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα») μπορεί να παραβιαστεί αποκλειστικά και μόνο με θετική συμπεριφορά εκείνου που παραβιάζει το πληροφοριακό σύστημα, και ποτέ με παράλειψη.[139] Το αυτό ερείδεται στην ρητά απαιτούμενη εκ της ισχύουσας διατάξεως σωρευτική συνδρομή παραβίασης (εκ μέρους του δράστη) απαγορεύσεων ή μέτρων ασφαλείας, η οποία ασφαλώς δεν μπορεί να λάβει χώρα με παράλειψη του δράστη (!). Η σωρευτική όμως αυτή συνδρομή δεν πρέπει να οδηγήσει στην εσφαλμένη άποψη ότι πρόκειται για σύνθετο έγκλημα, αλλά για απλό αφού μία πράξη τυποποιείται αυτοτελώς ως έγκλημα, η δε παραβίαση μέτρων ασφάλειας και απαγορεύσεων δεν συνιστούν αυτοτελή εγκλήματα, αλλά η συνδρομή τους καθιστά το έγκλημα πολύτροπο, δυνάμενο να πραγματωθεί με πλείονες τρόπους που προβλέπονται στην ειδική υπόσταση διαζευκτικά. Ειδικότερα, το υπό εξέταση έγκλημα είναι υπαλλακτικώς μικτό, καθότι όσοι τρόποι τέλεσης και αν πραγματωθούν μόνο ένα αδίκημα στοιχειοθετείται.

Ακόμη, εξόχως σημαντικός είναι και ο χαρακτηρισμός του εγκλήματος ως συμπεριφοράς ή αποτελέσματος, διάκριση η οποία έχει μεγάλη πρακτική σημασία αναφορικά με τον τόπο τέλεσης, τον χρόνο τέλεσης, την αρμοδιότητα των ποινικών αρχών, την ύπαρξη ή μη αντικειμενικού αιτιώδους συνδέσμου.[140]

Με τη διάταξη του άρθρου 370Γ παρ. 2 Π.Κ. τιμωρείται κάθε αυθαίρετη πρόσβαση – διείσδυση, δηλ, καλύπτεται τόσο η πρόσβαση σε δεδομένα ή στοιχεία που βρίσκονται αποθηκευμένα στον υπολογιστή του θύματος, πχ. στον σκληρό δίσκο(illegal access),όσο και η περίπτωση αθέμιτης πρόσβασης σε δεδομένα που μεταδίδονται με συστήματα τηλεπικοινωνιών(illegal interception). Τιμωρείται λοιπόν κάθε περίπτωση αυθαίρετης λήψης μεταδιδόμενων στοιχείων, όπως λ.χ η παγίδευση δικτύων μετάδοσης δεδομένων(wire tapping), η ακρόαση ψηφιακά μεταδιδόμενων επικοινωνιών(διαδικτυακά αναμεταδιδόμενες συζητήσεις – τηλεδιασκέψεις Internet Relay Chat IRC), η διείσδυση στο ηλεκτρονικό ταχυδρομείο ενός προσώπου, καθώς και η πρόσβαση σε ξένα συστήματα επεξεργασίας ή αποθήκευσης δεδομένων(π.χ. χωρίς δικαίωμα πρόσβαση του δράστη σε

[139] Πριλή Σταυρούλα- Αντιγόνη : Η παράνομη πρόσβαση σε πληροφοριακό σύστημα κατ'άρθ. 370Γ παρ2 Ποινικού Κώδικα, Αθήνα 2017,σελ 27

[140] Μυλωνόπουλος Χρήστος: Ποινικό Δίκαιο – Γενικό Μέρος Ι,2007,σελ 160

τράπεζα πληροφοριών ή σε ξένο προσωπικό η/υ με χρήση ξένου κωδικού ή με τη χωρίς δικαίωμα γνώση της ίδιας της κωδικής λέξης).
Τέλος θα πρέπει να τονιστεί ότι με τη διάταξη αυτή ο νομοθέτης τιμωρεί την παράνομη πρόσβαση καθ'εαυτή ανεξάρτητα από το σκοπό του δράστη και από το ειδικότερο είδος των στοιχείων, ενώ για την κατάφαση του εγκλήματος δεν απαιτείται κάποια επιπρόσθετη ενέργεια εκ μέρους του δράστη(αντιγραφή, βλάβη ή αλλοίωση δεδομένων κ.λ.π.). Στα πλαίσια του ελληνικού δικαίου δεν απαιτείται, για την τιμώρηση της συμπεριφοράς, να λάβει ο δράστης και γνώση των δεδομένων, αφού πρόσβαση σημαίνει απλά μια πράξη διείσδυσης. Υπό την έννοια αυτή το hacking έχει αυτοτελή απαξία, αφού η διείσδυση είναι φορέας αυτοτελούς αδίκου με τη μορφή έντονης διακινδύνευσης περαιτέρω έννομων αγαθών, δημιουργώντας τη δυνατότητα ανάγνωσης, απόκτησης ή αλλοίωσης στοιχείων και δεδομένων.[141] [142] [143]

11.2 Η αντικειμενική υπόσταση του άρθρου 370Γ παρ 2 ΠΚ

Η πράξη η οποία έχει επιλέξει ο ποινικός νομοθέτης να κολάσει στη διάταξη του αρθ. 370Γ παρ 2 είναι η απόκτηση πρόσβασης στο σύνολο ή σε τμήμα του πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών.
Ο Έλληνας νομοθέτης προέβη για πρώτη φορά στην ποινικοποίηση της χωρίς δικαίωμα πρόσβασης σε σύστημα η/υ δηλαδή του hacking με το άρθρο 4 του Ν 1805/1988, με το οποίο προστέθηκε για πρώτη φορά στον Ελληνικό ΠΚ η χωρίς δικαίωμα πρόσβαση σε στοιχεία η/υ με το άρθρο 370Γ παρ 2.
Με τον όρο απόκτηση πρόσβασης νοείται η απόκτηση δυνατότητας, είτε φυσικής είτε τεχνητής επίδρασης στα στοιχεία ή στο πληροφοριακό σύστημα του νομίμου κατόχου. Δηλαδή πρόκειται για κάθε διείσδυση ή εισβολή του δράστη η οποία του εξασφαλίζει την εν δυνάμει γνώση αυτών

[141] Βασιλάκη Ειρήνη: Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών. Ποινικά 40,Αθήνα 1993, σελ 80
[142] Καράκωστας Κ. Ιωάννης : Δίκαιο και Ίντερνετ. Νομικά ζητήματα του διαδικτύου, Αθήνα 2009,σελ 163
[143] Κιούπης Δημητ: "Ποινικό Δίκαιο και Internet" Ποινικά 57, Αθήνα- Κομοτηνή 1999, σελ 126

και τη δυνατότητα να προχωρήσει σε οποιαδήποτε περαιτέρω ενέργεια επιθυμεί.

Αντικείμενο της πρόσβασης και συνεπώς «**υλικό αντικείμενο**» του εγκλήματος αποτελούν α)τα στοιχεία που έχουν εισαχθεί σε η/υ ή σε περιφερειακή μνήμη η/υ. Ως τέτοια θεωρούνται[144] τα δεδομένα που έχουν καταγραφεί, συλληφθεί ή αποθηκευτεί στην κύρια μνήμη ή σε άλλο φορέα δεδομένων(πχ εξωτερικό δίσκο, μονάδα αποθήκευσης usb) και β)τα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών. Στην κατηγορία αυτή περιλαμβάνονται η μεταφορά δεδομένων από ένα υπολογιστή σε έναν άλλο, η απόκτηση δεδομένων από τράπεζες πληροφοριών(data banks) ως και η επικοινωνία μέσω ηλεκτρονικών συστημάτων όπως το ηλεκτρονικό ταχυδρομείο.[145] Στην παραπάνω έννοια της μετάδοσης των δεδομένων υπάγεται και η επεξεργασία αυτών τα οποία και προστατεύονται. Δεν προστατεύονται όμως όσα πρόκειται να εισαχθούν χωρίς να έχει ξεκινήσει η διαδικασία εισαγωγής τους ή όσα έχουν ήδη εξαχθεί από τους φορείς αποθήκευσης (π.χ όσα εκτυπώθηκαν). Συνάγεται κατά συνέπεια ότι τα μη αποθηκευμένα ή μη μεταδιδόμενα στοιχεία δεν υπάγονται στο προστατευτικό πλαίσιο της διάταξης.

Κατά τη μάλλον επικρατούσα άποψη[146] [147] το προστατευόμενο από το άρθρο 370Γ παρ 2 ΠΚ έννομο αγαθό είναι αυτό του απορρήτου υπό τυπική έννοια, δηλαδή το τυπικό δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει την πρόσβαση σε αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου υπό ουσιαστική έννοια και χωρίς να έχουν τα δεδομένα αυτά αποκλειστικά οικονομική αξία.[148] Το τυπικό περιεχόμενο του απορρήτου ουσιαστικά ταυτίζεται με την εμπιστευτικότητα ως έκφραση της ασφάλειας των πληροφοριών, δηλαδή την ιδιότητα των στοιχείων ενός συστήματος να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του. Σύμφωνα με τα παρατεθέντα ανωτέρω η απόκτηση πρόσβασης σε πληροφοριακό σύστημα προσιδιάζει αρκετά στο έγκλημα της διατάραξης

[144] Βασιλάκη Ειρήνη: "Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών"Ποινικά 40, Αθήνα 1993, σελ 86

[145] Μυλωνόπουλος Χρήστος: Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Αθήνα- Κομοτηνή 1991, σελ 93

[146] Μανωλόπουλος Χρήσ : Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Αθήνα 1991, σελ 92

[147] Σπυρόπουλος Φ : Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών(Hacking),Αθήνα 2016, σελ 177

[148] Αντίθετη άποψη είχε διατυπωθεί στη Νομολογία (Ναυτ Πειρ 530/2003) η οποία αναφέρει ότι με τη διάταξη του άρθρου 370Γ παρ 2 ΠΚ αποσκοπείται η τιμώρηση της παραβιάσεως μυστικών που έχουν σχέση με προγράμματα ηλεκτρονικών υπολογιστών και συνεπώς προστατεύεται το ουσιαστικό απόρρητο αυτών των προγραμμάτων. (Ποιν. Χρον. ΝΔ/2004, σελ 75)

οικιακής ειρήνης του άρθρου 334 ΠΚ. Σύμφωνα με την ειδική υπόσταση αυτού, το έγκλημα είναι τετελεσμένο με την παράνομη είσοδο του δράστη ή παραμονή του στο χώρο μετά την πρόσκληση του παθόντος, ανεξαρτήτως οποιασδήποτε μεταγενέστερης πράξης του δράστη[149] κατά λογική αντιστοιχία με την ειδική υπόσταση του αρθ. 370Γ παρ2 .
Το αξιόποινο της εν λόγω πράξης του αρθ 370Γ παρ2 ΠΚ, γίνεται αμέσως αντιληπτό, πως είναι ιδιαίτερα ευρύ καθότι αρκείται στην απόκτηση πρόσβασης και μόνο, η οποία δίνει την δυνατότητα για σωρεία μεταγενέστερων πράξεων – προσβολών του πληροφοριακού συστήματος.

11.3 Χωρίς δικαίωμα

Η φράση «**χωρίς δικαίωμα**» ταυτίζεται εννοιολογικά με τις έννοιες «αθέμιτα» ή «άνευ εξουσιοδοτήσεως» ή «χωρίς συγκατάθεση» του νομίμου κατόχου.
Η παραβίαση των απαγορεύσεων ή των μέτρων ασφάλειας του νομίμου κατόχου δεν αρκεί για την πλήρωση της αντικειμενικής υπόστασης του αδικήματος αν η πρόσβαση δεν υποκτάται και «χωρίς δικαίωμα» και τούτο διότι μπορεί κάποιος να αποκτήσει πρόσβαση σε πληροφοριακό σύστημα με παραβίαση μέτρων ασφάλειας, όχι απλά σε γνώση αλλά κατ'εντολήν του νομίμου κατόχου του. Συνεπώς στην περίπτωση αυτή δεν διαπράττει καμία αξιόποινη πράξη.
Με τον όρο «**χωρίς δικαίωμα**» του άρθρου 370Γ παρ 2 ΠΚ γεννώνται αντίστοιχα ερωτήματα με αυτά που ανακύπτουν με τις έννοιες «**αθέμιτα**» ή «**άνευ εξουσιοδοτήσεως**» του άρθρου 370Β Π.Κ. Αποτελεί δηλαδή ο όρος αυτός στοιχείο της αντικειμενικής υπόστασης του εγκλήματος και άρα πρέπει να περιέχεται στο δόλο του δράστη ή αποτελεί μόνο λόγο άρσης του αδίκου χαρακτήρα της πράξης του.
Για να καταλήξουμε σε ένα συμπέρασμα υπέρ της μίας ή της άλλης εκδοχής[150] θα πρέπει να εξετάσουμε αν η συμπεριφορά που τιμωρείται περικλείει και αυτό το αξιολογικό στοιχείο «η απαγόρευση δηλαδή να αφορά τη χωρίς δικαίωμα πρόσβαση σε στοιχεία». Σε καταφατική απάντηση το στοιχείο «χωρίς δικαίωμα» ανήκει στην αντικειμενική

[149] Μαργαρίτης Μ: «Ποινικός Κώδικας, Ερμηνεία – Εφαρμογή», 2009, σελ 902
[150] Βασιλάκη Ειρήνη :Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, Αθήνα – Κομοτηνή 1993, σελ 89

υπόσταση του εγκλήματος. Σε αρνητική απάντηση, αν δηλαδή η περιγραφή της εγκληματικής συμπεριφοράς οριοθετείται και χωρίς το παραπάνω στοιχείο η αναφορά του αποτελεί μόνο μια ένδειξη για τον δικαστή για την πιθανή συνδρομή κάποιου λόγου που αποκλείει το άδικο.[151]

Ο Νομοθέτης δεν θέλησε να ποινικοποιήσει την κάθε είδους πρόσβαση σε πληροφοριακό σύστημα με μόνη την παραβίαση μέτρων ασφαλείας αλλά αυτή που διαπράττεται χωρίς δικαίωμα, χωρίς την συγκατάθεση του νομίμου κατόχου με την οποία υφίσταται προσβολή του εννόμου αγαθού του τυπικού απορρήτου και αυτό για να αποκλειστεί η περίπτωση της υπερβολικής ποινικοποίησης.

Η αντικειμενική υπόσταση του εγκλήματος για να στοιχειοθετηθεί απαιτείται ρητά να τελείται η πράξη ενάντια ή χωρίς την βούληση του παθόντος φορέα του εννόμου αγαθού – νομίμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων που μεταδίδονται. Εάν λοιπόν δεν συντρέχει η βούληση του παθόντος τότε η πρόσβαση αποκτάται χωρίς δικαίωμα και πληρείται η αντικειμενική υπόσταση και συνεπώς το κατ'αρχήν άδικο του εγκλήματος. Συνεπώς το «χωρίς δικαίωμα» συνιστά στοιχείο της αντικειμενικής υπόστασης του άρθρου 370Γ παρ 2 και όχι λόγο άρσης του αδίκου.[152]

Η παραβίαση μέτρων ασφαλείας όπως είναι χαρακτηριστικά το «σπάσιμο» ενός ειδικού κωδικού πρόσβασης (password) είναι ένας ενδεικτικός και ιδιαίτερα συχνός τρόπος παράνομης πρόσβασης. Το γεγονός ότι πρόκειται για έναν ενδεικτικό τρόπο συνάγεται από την προσθήκη της λέξης «ιδίως» στη φράση «ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει ο νόμιμος κάτοχός τους». Τούτο σημαίνει ότι η παραβίαση των μέτρων ασφαλείας δεν είναι απαραίτητη για να καταφανεί το αξιόποινο του 370Γ παρ 2 ΠΚ καθώς αρκεί η αντίθετη βούληση του νομίμου κατόχου να έχει εκδηλωθεί με κάποιον αντικειμενικά διαγνώσιμο τρόπο π.χ να έχει τοποθετήσει τα στοιχεία σε κάποιον ιδιωτικό χώρο να είναι δηλαδή αυτά αποθηκευμένα στον ηλεκτρονικό υπολογιστή που βρίσκεται στην κατοικία ή στον επαγγελματικό χώρο . Η αναφορά είναι ενδεικτική, καθ'όσον δεν αποτελούν αναγκαίο όρο της αντικειμενικής υπόστασης αλλά έχουν ως σκοπό να δείξουν τη θέληση του νομίμου κατόχου να αποκλείσει άλλους από την πρόσβαση στα ηλεκτρονικά δεδομένα. Είναι συνεπώς σαφές πως η

[151] Δημητρίου Δήμητρα: Επιθέσεις κατά συστημάτων πληροφοριών: Το Διεθνές Ενωσιακό και Ελληνικό πλαίσιο Προστασίας, Θεσ/νίκη 2014,σελ 118

[152] Μυλωνόπουλος Χρήσ : Ποινικό Δίκαιο, Γενικό Μέρος Ι, 2007, σελ 254

χωρίς δικαίωμα πρόσβαση σε δεδομένα είναι η αξιόποινη και όταν ακόμη δεν παραβιάζονται μέτρα ασφάλειας, αρκεί βέβαια να προκύπτει κατά τρόπο αντικειμενικά διαγνώσιμο η βούληση του φορέα του εννόμου αγαθού να μην είναι τα δεδομένα του προσιτά σε τρίτους.
Ως «στοιχεία» θα πρέπει δε να θεωρούνται αυτά που έχουν εισαχθεί σε Η/Υ ή σε περιφερειακή μνήμη Η/Υ ή μεταδίδονται με συστήματα πληροφοριών (τηλεπικοινωνιών). Όσα στοιχεία έχουν καταγραφεί, συλληφθεί ή αποθηκευθεί στην κυρία μνήμη ή σε άλλο φορέα δεδομένων (π.χ σε εξωτερικό σκληρό δίσκο ή μονάδα USB) θεωρούνται ως «εισαχθέντα στοιχεία». Συνεπώς όσα δεν έχουν αποθηκευθεί δεν μπορούν να υπαχθούν στα ανωτέρω στοιχεία.[153]

11.4 Η έννοια παραβιάζοντας απαγορεύσεις ή μέτρα ασφάλειας

Η φράση "*ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει ο νόμιμος κάτοχός τους*" του άρθρου 370Γ παρ 2 ΠΚ έχει δημιουργήσει προβληματισμό καθώς ανακύπτει το ερώτημα αν για τη στοιχειοθέτηση του εγκλήματος απαιτείται να υπάρχει από την πλευρά του νομίμου κατόχου των δεδομένων συγκεκριμένη ενέργεια απαγόρευσης της πρόσβασης κάθε τρίτου σε αυτά.
Ο όρος «**απαγορεύσεις**» σύμφωνα με την κρατούσα στη θεωρία άποψη περιλαμβάνει σαφείς δηλώσεις βουλήσεως του νομίμου κατόχου είτε γραπτές είτε προφορικές που ενημερώνουν και αποτρέπουν οποιονδήποτε τρίτο να αποκτήσει πρόσβαση στα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών ή εν γένει στο πληροφοριακό σύστημα. Αυτές οι απαγορεύσεις μπορεί να είναι εμφανώς αναρτημένες είτε στο φυσικό χώρο όπου δραστηριοποιούνται οι υλικοί φορείς είτε να εμφανίζονται ως ηλεκτρονικές ειδοποιήσεις σε κάποιο στάδιο κατά την προσπάθεια εισόδου του δράστη στο πληροφοριακό σύστημα.
Η φράση «**μέτρα ασφαλείας**» του άρθρου 370Γ παρ 2 αφορά μέτρα που βοηθούν στην μη απόκτηση πρόσβασης από τρίτο πρόσωπο είτε αυτά τα μέτρα λαμβάνονται για μη απόκτηση πρόσβασης στο φυσικό χώρο όπως για παράδειγμα είναι το εγκατεστημένο σύστημα συναγερμού, οι κλειδαριές, οι σιδεριές κλπ, είτε πρόκειται για μέτρα ασφαλείας του λογισμικού ή πληροφοριακού συστήματος όπως για παράδειγμα είναι η κρυπτογράφηση

[153] Μυλωνόπουλος Χρήστος : Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Αθήνα 1991, σελ 94

στοιχείων.[154] Ο όρος κρυπτογράφηση συνίσταται στη μέσω μαθηματικών αλγορίθμων μετατροπή ενός προσιτού σε όλους κειμένου σε μια κωδικοποιημένη μορφή που δεν μπορεί να αποκωδικοποιήσει κανείς, αν δεν διαθέτει το μυστικό ειδικό κλειδί. Επίσης, η χρήση συνθηματικών ερωτήσεων, η ύπαρξη κωδικών πρόσβασης κλπ.

Η **παραβίαση** των απαγορεύσεων ή των μέτρων ασφαλείας **ορθότερο** είναι να κρίνονται κάθε φορά με αξιολόγηση όλων των συνθηκών τέλεσης για να μη καταλογιστεί στο δράστη και πράξη την οποία δεν έχει τελέσει κυρίως όταν πρόκειται για παραβίαση απαγορεύσεων ή μέτρων ασφαλείας του φυσικού χώρου.

11.5 Υποκειμενική υπόσταση του άρθρου 370Γ παρ 2 ΠΚ

Ο Νομοθέτης επέλεξε να τιμωρήσει την χωρίς δικαίωμα πρόσβαση σε δεδομένα τρίτων (π.χ αλλοίωσης, καταστροφής, εξάλειψης, αντιγραφής, ανακοίνωσης σε τρίτους κλπ), ανεξάρτητα από το αν η πρόσβαση πραγματοποιείται με επίμεμπτο σκοπό.

Το άρθρο 370Γ παρ 2 είναι πλημμέλημα αφού τιμωρείται με φυλάκιση ή με χρηματική ποινή(άρθρο 370Γ παρ 2 ΠΚ σε συνδυασμό με το άρθρο 18 παρ 2ΠΚ). Επίσης αφού ο νόμος δεν προβλέπει τίποτα ειδικότερο, το έγκλημα τιμωρείται μόνον από δόλο(άρθρο 26 παρ 1 ΠΚ). Επίσης επειδή η παράνομη πράξη πρέπει να γίνεται χωρίς δικαίωμα δηλαδή απαιτείται η γνώση ορισμένου περιστατικού, δεν αρκεί κατά την ορθότερη άποψη ο ενδεχόμενος δόλος.[155]

Κατ'άλλους[156] απαιτείται οποιοδήποτε είδος δόλου(αρκεί και ο ενδεχόμενος) που πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος, καθώς δεν απαιτείται από το νόμο να τελούνται οι πράξεις εν γνώσει ορισμένων περιστατικών (άρθρο 27 ΠΚ).

Η συμπεριφορά που περιγράφεται στο συγκεκριμένο άρθρο στην ουσία σκιαγραφεί την έννοια του απλού hacking με την έννοια της μη εξουσιοδοτημένης πρόσβασης σε ξένο υπολογιστή ή σύστημα υπολογιστών.[157]

---

[154] Καράκωστας Κ.Ιωάννης : Δίκαιο και Ίντερνετ. Νομικά ζητήματα διαδικτύου, 3η έκδοση, Αθήνα 2009, σελ 275

[155] Δημητρίου Δήμητρα: Οι επιθέσεις κατά συστημάτων πληροφοριών. Το Διεθνές Ενωσιακό και Ελληνικό Πλαίσιο προστασίας, Θεσσαλονίκη 2014, σελ 120

[156] Λαμπάκη Χ σε Χαραλαμπάκη Αριστ. Ποινικός Κώδικας :Ερμηνεία κατ'άρθρο, ειδικό μέρος, τόμος δεύτερος, σελ 2981

[157] Αργυρόπουλος Ανδρέας "Ηλεκτρονική εγκληματικότητα" στη σειρά Εγκληματικά 19, Αθήνα-Κομοτηνή 2001 σελ 34

ΕΠΙΛΟΓΟΣ

Με δεδομένες τις καταχρήσεις του Διαδικτύου και τον εντελώς απρόσωπο χαρακτήρα του αλλά και τις επικίνδυνες παρενέργειές του πρέπει να τονίζεται διαρκώς η ανάγκη προστασίας του ατόμου – χρήστη. Η προστασία αυτή είναι δυνατή και με δικαιικά μέσα που θα διασφαλίζουν αφ'ενός την ελευθερία χρήσης του Διαδικτύου και αφετέρου θα αποτρέπουν την κατάχρησή της. Η λύση στα προβλήματα που παρουσιάζονται θα δοθούν μετά από διεθνείς πρωτοβουλίες και μέσα από διεθνείς συμβάσεις καθώς και από την ίδια την τεχνολογία. Αλλά και τα κράτη μπορούν να παίξουν το ρόλο του ρυθμιστή του Διαδικτύου.

Το Διαδίκτυο πρέπει να μείνει ελεύθερο. Πρέπει να διευκολύνεται η ελεύθερη κυκλοφορία των κεφαλαίων και των ιδεών. Όμως, είτε θεωρηθεί ως Μέσο Μαζικής Επικοινωνίας, είτε ως μια απλή τηλεπικοινωνιακή υπηρεσία, είτε ως μια νέα παγκόσμια αγορά δεν πρέπει να ξεχνάμε ότι επίκεντρό του είναι ο άνθρωπος.

Με την παραπάνω ανάλυση δόθηκε μια σαφής και πλήρης εικόνα των τεχνικών που έχουν καθιερωθεί και είναι κοινά αποδεκτοί στον κλάδο της τεχνολογίας των πληροφοριών, ως και της έκτασης και των αδυναμιών της ποινικής αντιμετώπισης των προσβολών σε βάρος των συστημάτων πληροφοριών.

Τα πολύπλοκα και δαιδαλώδη συστήματα πληροφοριών που παρέχουν συνεχώς νέες δυνατότητες παράνομης πρόσβασης στα προσωπικά δεδομένα προσώπων και επιχειρήσεων και εξ'αιτίας αυτού κατακόρυφη αύξηση της εγκληματικότητας, απαιτούν τολμηρή προσέγγιση του φαινομένου. Η αντιμετώπιση των νέων μορφών εγκληματικότητας πρέπει να γίνει με αναγωγή σε υπερνομοθετικές αξίες και αρχές, σε επίπεδο συνταγματικών αξιών και αρχών του διεθνούς κοινοτικού δικαίου.

Επίσης, η επίγνωση πλαισίου είναι μία ιδιότητα των συστημάτων που θα πρέπει να βελτιωθεί δηλαδή να κατανοούν τα συστήματα το πλαίσιο και να προσαρμόζονται σε αυτό(=να αντιλαμβάνονται την τοποθεσία του χρήστη) και συνεπώς η βελτίωσή του αποτελεί στόχο για το μέλλον και αντικείμενο προς περαιτέρω έρευνα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Αγγελή Ι: Διαδίκτυο(Internet) και ποινικό δίκαιο: Έγκλημα στον Κυβερνοχώρο(cybercrime – internet crime)Ποινικά Χρονικά 2000
2. Ανδρουλάκη Ν: Ποινικό Δίκαιο – Γενικό Μέρος (Θεωρία για το έγκλημα)2η έκδοση, εκδ. Π.Ν.Σάκκουλας, 2006
3. Βασιλάκη Ειρήνη: Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών: η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του Ν1805/88, Αθήνα 1993
4. Βλαχόπουλος Κων: Ηλεκτρονικό έγκλημα – Μορφές, πρόληψη, αντιμετώπιση, Νομική Βιβλιοθήκη, Αθήνα 2002
5. Γκότση Μαρίνα: Το ηλεκτρονικό έγκλημα στην ελληνική έννομη τάξη. Οι προσβολές κατά συστημάτων πληροφοριών και η ποινική αντιμετώπισή τους κατά το ελληνικό και ενωσιακό δίκαιο, Θεσσαλονίκη 2018
6. Δαλακούρας Ι. Θεοχάρης: Ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη, Θεσσαλονίκη 2018
7. Δαλακούρας Ι. Θεοχάρης: Ο νέος κώδικας ποινικής δικονομίας : Μία πρώτη ερμηνευτική προσέγγιση του Ν 4620/2019/, Νομική Βιβλιοθήκη, Αθήνα 2019
8. Δημητρίου Δήμητρα: Επιθέσεις κατά συστημάτων πληροφοριών. Το διεθνές, ενωσιακό και ελληνικό πλαίσιο προστασίας, Θεσσαλονίκη 2014
9. Doswell R., G.L Simons : Πληροφορική και Εγκληματικότητα, Εκδ Δίαυλος, Αθήνα 1990
10. Ηλιοπούλου Σοφία: Cloud Computing, Άρτα 2014
11. Καϊάφα – Γκμπάντι Μαρία: Ποινικό δίκαιο και καταχρήσεις πληροφορικής, 2007
12. Καράκωστας Κ. Ιωάννης: Δίκαιο και Internet. Νομικά ζητήματα του διαδικτύου, εκδόσεις Π.Ν Σάκκουλας, Αθήνα 2009
13. Καργόπουλος Αλέξανδρος – Ιωάννης : Κυβερνοέγκλημα :Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου, www.esdi.gr
14. Κιούπη Δ: Ποινικό Δίκαιο και Ιντερνετ, Εκδ Α.Ν Σάκκουλα, Αθήνα – Κομοτηνή 1999
15. Κομνηνός Θόδωρος, Σπυράκης Παύλος. Ασφάλεια δικτύων και υπολογιστικών συστημάτων, Ελληνικά Γράμματα, Αθήνα 2002

16. Κονταξής Α: «Ποινικός Κώδικας», Τόμος ΙΙ Εκδ Π.Ν Σάκκουλας, 2000
17. Κωνσταντινίδης Άγγελος : Η διακεκριμένη παραβίαση απόρρητων στοιχείων, Ποινικά Χρονικά, 1997
18. Μανωλεδάκης Ιωάννης: Ποινικό Δίκαιο, Επιτομή Γενικού Μέρους 2005
19. Μανωλεδάκης Ιωάννης: Ποινικό Δίκαιο – Γενική Θεωρία, Αθήνα – Θεσσαλονίκη 2004
20. Μαργαρίτης Μ: «Ποινικός Κώδικας» Ερμηνεία – Εφαρμογή, Εκδ Π.Ν Σάκκουλας, 2η έκδοση, 2009
21. Μυλωνόπουλος Χρήστος: Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, σειρά Ποινικά, εκδ Α.Ν. Σάκκουλας, Αθήνα 1991
22. Μυλωνόπουλος Χρήστος: Ποινικό Δίκαιο – Γενικό Μέρος Ι, Εκδ Π.Ν Σάκκουλα, 2007
23. Πριλή Σταυρούλα: Η παράνομη πρόσβαση σε πληροφοριακό σύστημα κατ'άρθρο 370Γ παρ 2 Ποινικού Κώδικα, Αθήνα 2017

24. A. P. Plageras, C. Stergiou, K. E. Psannis, G. Kokkonis, Y. Ishibashi, Byung-Gyu Kim, Brij Gupta, "Efficient Large-Scale Medical Data…Things", in Proceedings of 19th IEEE International Workshop on the Internet of Things and Smart Services, 24-26 July 2017, Thessaloniki, Greece

25. A. P. Plageras, K. E. Psannis,C. Stergiou, H. Wang, B. Gupta, "Efficient IoT-based sensor BIG Data...Smart Buildings", Future Generation Computer Systems, vol.82, pp. 349-357, May 2018
26. A. P. Plageras, K. E. Psannis, Y. Ishibashi, B.-G. Kim, "IoT-based Surveillance System for Ubiquitous Healthcare", 42nd Annual Conference of the IEEE Industrial Electronics Society, 24/10/2016- 27/10/2016
27. A. P. Plageras, K. E. Psannis, " Algorithms for Big Data Delivery over the Internet of Things", in Proceedings of 19th IEEE Conference on Business Informatics 2017(CBI2017), Doctoral Consortium, 24-26 July 2017, Thessaloniki, Greece
28. A. P. Plageras, C. Stergiou, K. E. Psannis, Byung-Gyu Kim, Brij Gupta, Y. Ishibashi, "Solutions for Interconnectivity…Smart Hospital Building", in Proceedings of 15th IEEE International Conference on Industrial Informatics(INDIN 2017), 24-26 July 2017, Emden, Germany
29. Andreas P. Plageras, Kostas E. Psannis, Christos Stergiou, Haoxiang Wang, and B. B. Gupta, Efficient Sensor Big Data

Collection-Processing and Analysis in Smart Buildings, Future Generation Computer Systems. Volume 82, May 2018, Pages 349-357
30. Avishek Saha, Young-Woon Lee, Young-Sup Hwang, Kostas E. Psannis, Byung-Gyu Kim, Context-aware Block-based Motion Estimation Algorithm for Multimedia Internet of Things (IoT) Platform, Personal and Ubiquitous Computing (Springer), February 2018, Volume 22, Issue 1, pp 163–172
31. C. Stergiou, K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing…applications: a survey", Wiley, International Journal of Network Management, pp. 1-12, May 2016.
32. C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, vol. 78, part 3,pp. 964-975, January 2018
33. C. Stergiou, K. E. Psannis, A. P. Plageras, G. Kokkonis, Y. Ishibashi, "Architecture for Security in IoT Environments", in Proceedings of 26th IEEEInternational Symposium on Industrial Electronics, 19 – 21 June 2017, Edinburg, Scotland, UK
34. C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, B.-G. Kim, "Algorithms for efficient digital media..cloud networking", Journal of Multimedia Information System, vol. 5, no.1, pp. 27-34, March 2018
35. C. Stergiou, K. E. Psannis, A. P. Plageras, T. Xifilidis,B. B. Gupta, "Security and Privacy of Big Data..in Cloud", in Proceedings of IEEE conference on Computer Communications, 15-20 April 2018, Honolulu, HI, USA.
36. C. Stergiou, K. E. Psannis, B. Gupta, Y. Ishibashi, "Security, Privacy & Efficiency..for Big Data & IoT", Elsevier, Sustainable Computing, Informatics and Systems, vol. 19, pp. 174-184, September 2018
37. C. Stergiou, A. P. Plageras,K. E. Psannis, T. Xifilidis,G. Kokkonis, S. Kontogiannis, K. Tsarava, A. Sapountzi, "Proposed High Level Architecture…Interactive Classroom", in Proceedings of IEEE conference SEEDA-CECNS M 2018, 22-24 September 2018, Kastoria, Greece
38. C. Stergiou, K. E. Psannis, B. B. Gupta, "Secure Machine Learning scenario..network", Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications, in Press, 2019

39. Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, Secure integration of IoT and Cloud Computing, Elsevier, Future Generation Computer Systems, December 2016
40. Christos Stergiou and Kostas E. Psannis, Efficient and Secure BIG Data Delivery in Cloud Computing, Multimedia Tools and Applications, 2017
41. Christos Stergiou, Kostas E. Psannis, B.B. Gupta, and Yutaka Ishibashi, Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT, Sustainable Computing, Informatics and Systems, Elsevier, June 2018
42. C. Stergiou, Kostas. E. Psannis, A. P. Plageras, Y. Ishibashi, B.-G. Kim, "Algorithms for efficient digital media transmission over IoT and cloud networking", Journal of Multimedia Information System, vol. 5, no. 1, pp. 1-10, March 2018.
43. Androniki Sapountzi and Kostas E. Psannis, Social networking data analysis tools & challenges, Elsevier, Future Generation Computer Systems,Oct. 2016
44. Scambray Joel, Stuart McCenre, George Kurtz : ΧΑΚΕΡ. Επίθεση και Άμυνα, Εκδ. Μ. Γκιούρδας Αθήνα 2001
45. Σπυρόπουλος Φ: Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (Hacking) σειρά Ποινικά Εκδ. Α.Ν. Σάκκουλα Αθήνα 2016
46. Σύρος Γεώργιος: Τεχνική Θεώρηση και νομική προσέγγιση στα πλαίσια του Ενωσιακού Ελληνικού Δικαίου
47. Velte.T Anthony, Toby J.Velte, Robert Elsenpeter : Cloud Computing : Πρακτική προσέγγιση, Εκδ. Μ. Γκιούρδας, Αθήνα 2010
48. Τσεσμελής Βασίλειος: Ασφάλεια και εφαρμογές Cloud Computing
49. Φιλόπουλος Π: Ποινική προστασία απορρήτου, συστηματική ερμηνεία άρθρων 370- 371 ΠΚ, Εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη 2015
50. Χαραλαμπάκης Αριστοτ: Ποινικός Κώδικας, Ερμηνεία κατ'άρθρο, τομ. Δεύτερος, 2η έκδοση, Αθήνα 2014
51. Χαραλαμπάκης Αριστοτέλης :Ο νέος ποινικός κώδικας: Μια πρώτη ερμηνευτική προσέγγιση του Ν 4619/2019/, Νομική Βιβλιοθήκη, Αθήνα 2019

52. Theofanis Xifilidis and Kostas Psannis, Caching Hit Probability and Compressive Sensing Perspective for Mobile Cellular Networks, Simulation Modelling Practice and Theory Elsevier
53. Ψάννης Κωνσταντίνος, Στεργίου Χρήστος. Αποτελεσματική και Ασφαλής μεταφορά Big Data στο Cloud Computing με έναν αλγόριθμο, 2018
54. Kostas E, Psannis, Christos Stergiou, and B. B. Gupta, Advanced Media-based Smart Big Data on Intelligent Cloud Systems, IEEE Transactions on Sustainable Computing (T-SUSC), June 2018.
55. Andreas P. Plageras, Kostas E. Psannis, Christos Stergiou, Haoxiang Wang, and B. B. Gupta, Efficient Sensor BIG Data Collection-Processing and Analysis in Smart Buildings, Elsevier, Future Generation Computer Systems, 2017.
56. Vasileios Memos, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, Brij Gupta, An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework, Elsevier, Future Generation Computer Systems, 2017.
57. G. Kokkonis, Kostas E. Psannis, M. Roumeliotis, Y. Ishibashi, Efficient algorithm for transferring a real-time HEVC stream with haptic data through the internet, Journal of Real-Time Image Processing, Vol. 12, no 2, pp 343–355, Aug. 2016.
58. G. Kokkonis, Kostas E. Psannis, M. Roumeliotis, Real Time Wireless Multisensory Smart Surveillance With 3D - HEVC Streams for IOT, The Journal of SuperComputing, June 2016.
59. Ioanna Kakalou and Kostas E, Psannis, Coordination without Collaboration in Imperfect Games: the Primary User Emulation Attack Example, IEEE Access Journal, 2018
60. IoannaKakalou, Kostas E. Psannis, PiotrKrawiec, and RaduBadea, Cognitive Radio Network and Network Service Chaining towards 5G: challenges and requirements, IEEE Communications, September 2017.
61. Ioanna Kakalou, and Kostas Psannis, Sustainable and Efficient Data collection in Cognitive Radio Sensor Networks, IEEE Transactions on Sustainable Computing, Date of Publication: 26 April 2018
62. Kostas E, Psannis, Christos Stergiou, and BB Gupta, Advanced Media-based Smart Big Data on Intelligent Cloud Systems IEEE Transactions on Sustainable Computing, 2018 (Date of Publication: 21 March 2018)
63. Ioanna Kakalou and Kostas E, Psannis, Coordination without Collaboration in Imperfect Games: the Primary User Emulation

Attack Example, IEEE Access Journal, vol.6, pp. 5402 – 5414, 2018
64. Ioanna Kakalou, Kostas E. Psannis, Piotr Krawiec, and Radu Badea, Cognitive Radio Network and Network Service Chaining towards 5G: challenges and requirements, IEEE Communications, vol. 55, issue 11, pp. 145-151, 2017.
65. P. Huang, Y. Ishibashi, and Kostas. E. Psannis, Fairness assessment in networked games with olfactory and haptic senses, International Journal of Communications, Network and System Sciences (IJCNS), vol. 10, no. 8, pp. 173-186, Aug. 2017
66. Byung-Gyu Kim, Gwang-Soo Hong, and Kostas E. Psannis, Design of Efficient Shape Feature for Object-based Watermarking Technology, Multimedia Tools and Applications November 2017, Volume 76, Issue 21, pp 22741–22759'
67. https://el.wikipedia.org
68. https://europa.eu/rapid/press-release
69. https://cyberalert.gr/ypiresies-ypologistikou-nefous/
70. https://www.epest.gr/el/content/ypologistiko-nefos-cloud computing
71. https://www.economist.com/topics/cloud computing
72. https://www.symantec.com
73. https://www.stac.com
74. https://www.remotelyanywhere.com
75. https://www.cal.com
76. https://www.netopia.com
77. https://www.uk.research.att.com/vnc
78. https://www.e-nomothesia.gr/nomikes plirofories
79. https://www.lawspot.gr/nomikes-plirofories/nomothesia