Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΨΗΦΙΑΚΗ ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΔΙΟΙΚΗΣΗ»

Διπλωματική Εργασία

«ΜΙΑ ΠΡΟΤΑΣΗ ΣΧΕΔΙΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΗΝ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ-

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΤΟΥ Ε-ΕΦΚΑ»

Γιώτη Αναστασία

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής **ΣΤΑΜΑΤΙΟΥ ΙΩΑΝΝΗΣ**	
Α΄ Συν-Επιβλέπων **Αντωνοπούλου ‘Ηρα**	**Β΄ Συν-Επιβλέπων** **Παπαδόπουλος Δημήτριος**

Πάτρα, 27/03/2022

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της παρούσας διπλωματικής θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή κ.Σταματίου Ιωάννη, για την εμπιστοσύνη που μου έδειξε αποδεχόμενος να αναλάβει την καθοδήγησή μου, για την επίβλεψη και τις πολύτιμες συμβουλές του καθ'όλη την διάρκεια της συγγραφής, για την ευγένεια και την κατανόησή του στα άγχη μου.

Επίσης θα ήθελα να εκφράσω τις ευχαριστίες μου προς τα μέλη της επιτροπής κ.'Ηρα Αντωνοπούλου Πρόεδρο του Τμήματος και κ.Δημήτριο Παπαδόπουλο για την τιμή που μου έκαναν να μετέχουν στην επιτροπή της εργασίας.

Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου που πίστεψε σε μένα και στήριξε κάθε μου προσπάθεια με αμέριστη υπομονή και συμπαράσταση.

ΠΕΡΙΛΗΨΗ

Στόχος της δημόσιας διοίκησης είναι η άμεση εξυπηρέτηση και ικανοποίηση των αναγκών των πολιτών. Η μέγιστη αποδοτικότητα των πληροφοριακών συστημάτων του εκάστοτε οργανισμού είναι μία από τις συνιστώσες για την επίτευξη αυτού του στόχου. Θεωρώντας ότι η πολιτική ασφαλείας που εφαρμόζει κάθε οργανισμός στα πληροφοριακά του συστήματα επηρεάζει την πλήρη και ορθή χρήση των δυνατοτήτων που παρέχει το κάθε πληροφοριακό σύστημα, διερευνούμε και αναλύουμε τα μέτρα προστασίας που χρησιμοποιούνται στον e ΕΦΚΑ για την Κυβερνοασφάλεια.

Η συγκεκριμένη εργασία μελετά το ενδεχόμενο η ελλιπής εφαρμογή πολιτικής ασφαλείας στην πληθώρα των πληροφοριακών συστημάτων του e ΕΦΚΑ να ευθύνεται για την μειωμένη διαλειτουργικότητα των πληροφοριακών συστημάτων του οργανισμού με συνέπεια την αναποτελεσματικότητα των υπηρεσιών του.

Η υπάρχουσα βιβλιογραφία που χρησιμοποιήθηκε αφορά την κυβερνοασφάλεια, τα πληροφοριακά συστήματα και την διαλειτουργικότητα στην Δημόσια Διοίκηση τα οποία θα αναλύσουμε για την πλήρη κατανόηση της σημασίας των εννοιών. Μέσα από την ανάλυση αυτή θα διερευνήσουμε και θα κατανοήσουμε τους παράγοντες από τους οποίους εξαρτάται η αποτελεσματικότητα των πληροφοριακών συστημάτων του e ΕΦΚΑ.

Επειδή από την έρευνά μας δεν προέκυψαν βιβλιογραφικές αναφορές για το συγκεκριμένο θέμα που πραγματευόμαστε για να εξειδικεύσουμε και να αναλύσουμε το θέμα μας επιλέξαμε την ποιοτική έρευνα.

Ως εργαλείο της έρευνάς μας χρησιμοποιήσαμε τις λέξεις-κλειδιά σε συνεντεύξεις για την ανταλλαγή απόψεων με τα εμπλεκόμενα μέρη καθώς πιστεύουμε ότι μία υποκειμενική άποψη η οποία κρίνει και αξιολογεί μέσα από την καθημερινή εμπειρία της συναλλαγής με τους πολίτες είναι μία αξιόπιστη άποψη.

Συμπερασματικά επιβεβαιώνονται οι υποθέσεις μας για τους παράγοντες που επηρεάζουν την υπάρχουσα κατάσταση και τις αιτίες που δημιουργούν σύγχυση στους ασφαλισμένους πολίτες και αναποτελεσματικότητα στον μεγαλύτερο φορέα κοινωνικής ασφάλισης της χώρας. Στόχος μας να προταθούν εφικτές λύσεις που να μπορούν να εφαρμοστούν προκειμένου να βελτιωθεί η αποδοτικότητα.

Λέξεις-κλειδιά: Πληροφοριακά συστήματα στον e ΕΦΚΑ, Διαλειτουργικότητα, Απόδοση, Κυβερνοασφάλεια

Abstract

The goal of Public Administration is the unimpeded service and fulfilment of citizens needs. Achieving maximum efficiency of information systems for the separate agencies that comprise its parts is a major component to that end. Considering that the security policy that each agency has in effect with regard to its information systems affects the full and correct use of the latter's capabilities, we investigate and analyze the protective measures currently being used in e-EFKA for Cybersecurity.

This thesis examines the possibility that lackluster implementation of security policies in the variety of information systems that are involved in e-EFKA might be responsible for the reduced interoperability between said information systems, thereby effectively rendering the former's services inefficient.

The existing literature used concerns cybersecurity, information systems and interoperability in Public Administration, concepts which will be analyzed and elaborated to clarify their meaning and scope. Through this analysis, we will investigate and understand the factors on which the effectiveness of e-EFKA information systems depends.

Because our preliminary research did not produce bibliographic references for the problematic that concerns us, we chose to conduct qualitative research in order to specify and dissect our topic.

As a tool to aid our investigation, we utilized the keywords in interviews, to hear the perspectives and critiques of some of the relevant parties involved, as we believe that a subjective point of view that judges and evaluates through the daily experience of dealing with citizens is a legitimate and dependable point of view.

In drawing our conclusions, we found that our assumptions about the factors that affect the current situation, and about the causes that create confusion among insured citizens and inefficiency in the largest social security institution in the country, were confirmed. Our goal is to propose feasible solutions that can be implemented in order to improve efficiency.

Key-words: Information systems in e-ΕΦΚΑ, Interoperability, Efficiency, Cybersecurity

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ ΕΛΛΗΝΙΚΑ

ΕΦΚΑ	ΕΝΙΑΙΟΣ ΦΟΡΕΑΣ ΚΟΙΝΩΝΙΚΩΝ ΑΣΦΑΛΙΣΕΩΝ
ΕΟΠΥΥ	ΕΘΝΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ
Κ.Η.Υ.Κ.Υ	ΚΕΝΤΡΟ ΗΛΕΚΤΡΟΝΙΚΟΥ ΥΠΟΛΟΓΙΣΤΗ ΚΟΙΝΩΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ
ΗΔΙΚΑ	ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ
ΟΠΕΚΑ	ΟΡΓΑΝΙΣΜΟΣ ΠΡΟΝΟΙΑΚΩΝ ΕΠΙΔΟΜΑΤΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΗΣ ΑΛΛΗΓΕΓΓΥΗΣ
ΙΚΑ-ΕΤΑΜ	ΙΔΡΥΜΑ ΚΟΙΝΩΝΙΚΩΝ ΑΣΦΑΛΙΣΕΩΝ-ΕΝΙΑΙΟ ΤΑΜΕΙΟ ΑΦΑΛΙΣΗΣ ΜΙΣΘΩΤΩΝ
ΕΤΑΜ-ΜΜΕ	ΕΝΙΑΙΟ ΤΑΜΕΙΟ ΑΣΦΑΛΙΣΗΣ ΠΡΟΣΩΠΙΚΟΥ ΜΕΣΩΝ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ
ΕΤΑΑ	ΕΝΙΑΙΟ ΤΑΜΕΙΟ ΑΝΕΞΑΡΤΗΤΑ ΑΠΑΣΧΟΛΟΥΜΕΝΩΝ
ΟΑΕΕ	ΟΡΓΑΝΙΣΜΟΣ ΑΣΦΑΛΙΣΗΣ ΕΛΕΥΘΕΡΩΝ ΕΠΑΓΓΕΛΜΑΤΙΩΝ
ΟΓΑ	ΟΡΓΑΝΙΣΜΟΣ ΓΕΩΡΓΙΚΩΝ ΑΣΦΑΛΙΣΕΩΝ
ΝΑΤ	ΝΑΥΤΙΚΟ ΑΠΟΜΑΧΙΚΟ ΤΑΜΕΙΟ
ΤΑΥΤΕΚΩ	ΤΑΜΕΙΟ ΑΣΦΑΛΙΣΗΣ ΥΠΑΛΛΗΛΩΝ ΤΡΑΠΕΖΩΝ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΟΙΝΗΣ ΩΦΕΛΕΙΑΣ
ΕΤΑΤ	ΕΝΙΑΙΟ ΤΑΜΕΙΟ ΑΣΦΑΛΙΣΗΣ ΤΡΑΠΕΖΟΥΠΑΛΛΗΛΩΝ
ΓΛΚ	ΓΕΝΙΚΟ ΛΟΓΙΣΤΗΡΙΟ ΤΟΥ ΚΡΑΤΟΥΣ-ΔΙΕΥΘΥΝΣΗ ΧΟΡΗΓΗΣΗΣ ΣΥΝΤΑΞΕΩΝ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
ΚΕΑΟ	ΚΕΝΤΡΟ ΕΙΣΠΡΑΞΗΣ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΙΣΦΟΡΩΝ
ΚΕΠΑ	ΚΕΝΤΡΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΝΑΠΗΡΙΑΣ
ΟΔΕ	ΟΜΑΔΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΡΓΟΥ
ΟΚΑ	ΟΡΓΑΝΙΣΜΟΙ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ ΑΓΓΛΙΚΑ

EESSI	ELECRONIC EXCHANGE OF SOCIAL SECURITY INFORMATION ΕΥΡΩΠΑΙΚΟ ΣΥΣΤΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΝΤΑΛΛΑΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΓΙΑ ΤΗΝ ΚΟΙΝΩΝΙΚΗ ΑΣΦΑΛΙΣΗ
CEF	CONNECTING EUROPE FACILITY ΣΥΝΔΕΟΝΤΑΣ ΤΗΝ ΕΥΡΩΠΗ
INEA	INNOVATION AND NETWORK EXECUTIVE AGENCY ΕΚΤΕΛΕΣΤΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΚΑΙΝΟΤΟΜΙΑΣ ΚΑΙ ΔΙΚΤΥΩΝ
IR	INSTITUTIONREPOSITORY ΕΘΝΙΚΟΣ ΚΑΤΑΛΟΓΟΣ ΦΟΡΕΩΝ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ
CR	COMPUTER ROOM ΚΕΝΤΡΟ ΔΕΔΟΜΕΝΩΝ
AP	ACCESS POINT ΣΗΜΕΙΟ ΠΡΟΣΒΑΣΗΣ
RINA	REFERENCE IMPLEMENTATION FOR A NATIONAL APPLICATION ΕΦΑΡΜΟΓΗ ΑΝΑΦΟΡΑΣ ΓΙΑ ΕΘΝΙΚΗ ΕΦΑΡΜΟΓΗ
CPI	CASE PROCESSING INTERFACE ΔΙΕΠΑΦΗΕΠΕΞΕΡΓΑΣΙΑΣΥΠΟΘΕΣΗΣ
ENISA	EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY ΕΥΡΩΠΑΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ
GDPR	GENERAL DATA PROTECTION REGULATION ΚΑΝΟΝΙΣΜΟΣΠΡΟΣΤΑΣΙΑΣΠΡΟΣΩΠΙΚΩΝΔΕΔΟΜΕΝΩΝ
SSL	SECURESOCKETLAYER ΑΣΦΑΛΗ ΕΠΙΚΟΙΝΩΝΙΑ ΜΕΤΑΞΥ ΔΥΟ ΕΦΑΡΜΟΓΩΝ Η ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
TCP	TRANSMISSION CONTROL PROTOCOL ΣΥΛΛΟΓΗΠΡΩΤΟΚΟΛΛΩΝΕΠΙΚΟΙΝΩΝΙΑΣ
IP	INTERNET PROTOCOL
NL	NETWORK LAYER ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ
OPSEC	OPERATION SECURITY ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΑΣΦΑΛΕΙΑ

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Το τελευταίο χρονικό διάστημα ο e-ΕΦΚΑ ως φορέας, αλλά και οι υπάλληλοι που τον στελεχώνουν, έχουν γίνει αντικείμενο επικρίσεων και αρνητικών σχολιασμών σε πληθώρα δημοσιευμάτων. Ταυτόχρονα έχουν στοχοποιηθεί από τον ίδιο τον Υπουργό Εργασίας ως πρόβλημα που ζητά επιτακτικά την λύση του.

Την ίδια στιγμή σε καθημερινή βάση, χιλιάδες συνταξιούχοι, υποψήφιοι συνταξιούχοι και ασφαλισμένοι όλων των ηλικιών, εκφράζουν την αγωνία τους, την δυσαρέσκειά τους και την δικαιολογημένη αγανάκτησή τους για τον φορέα αφού η άμεση εξυπηρέτησή τους φαντάζει εξωπραγματική.

Σε όλες τις χώρες η κοινωνική ασφάλιση είναι ένα σύνθετο πρόβλημα με πολλές προεκτάσεις που απαιτεί οικονομικές και νομικές γνώσεις, ικανότητες διοίκησης και οργάνωσης αλλά κυρίως πολιτική βούληση για την δίκαιη και ορθή αντιμετώπιση των πολλαπλών θεμάτων που απορρέουν από την εφαρμογή των νομοθετημάτων και των κανονισμών που θα αναδιανείμουν δίκαια παροχές στους δικαιούχους τους-ασφαλισμένους.

Στην χώρα μας η δημόσια κοινωνική ασφάλιση είναι θεσμοθετημένη και κατοχυρωμένη από το Σύνταγμα. Στον παρελθόν και στο παρόν όμως υπάρχουν πολλές διαφοροποιήσεις σε μία διαρκή προσπάθεια ισορροπίας, ανάμεσα στην δημόσια κοινωνική ασφάλιση που μεριμνά για ανταποδοτικές παροχές στους ασφαλισμένους σύμφωνα με τις απαιτήσεις της κάθε εποχής, και τις πολιτικοοικονομικές προεκτάσεις που επηρεάζουν την εκάστοτε κυβέρνηση.

Δυστυχώς αυτές οι συνεχόμενες ανακατατάξεις, έχουν φέρει ένα αντίθετο αποτέλεσμα, δηλαδή μία ανισορροπία που δημιουργεί αναποτελεσματικότητα, ανασφάλεια, άγχος και αβεβαιότητα για το μέλλον της κοινωνικής ασφάλισης.

Το θέμα της δημόσιας κοινωνικής ασφάλισης το οποίο μας αφορά όλους, είτε ως εργαζόμενους στον φορέα, είτε ως ασφαλισμένους πολίτες αυτής της χώρας θα πρέπει να αντιμετωπισθεί με δραστικές λύσεις. Αρχικά θα ήταν χρήσιμο εάν αναγνωρίζονταν και αξιολογούνταν οι αιτίες που δημιουργούν τα προβλήματα.

Στα πλαίσια αυτά η συγκεκριμένη εργασία ερευνά εάν η πολιτική ασφαλείας που εφαρμόζεται στα πληροφοριακά συστήματα του e ΕΦΚΑ επηρεάζει την διαλειτουργικότητά τους και την αποδοτικότητά τους δημιουργώντας περαιτέρω προβλήματα στην εξυπηρέτηση των ασφαλισμένων.

Η ερευνητική προσέγγιση αυτής της εργασίας έχει ως στόχο να διεξάγει κάποια ενδεικτικά συμπεράσματα για τα πληροφοριακά συστήματα του e ΕΦΚΑ σε σχέση με την πολιτική ασφαλείας τους.

Αναλυτικά η εργασία μας διαρθρώνεται σε 5 κεφάλαια: το πρώτο κεφάλαιο αποτελεί μία εισαγωγή όπου αναλύονται οι όροι και οι έννοιες της κυβερνοασφάλειας στο διαδίκτυο, οι στόχοι της κυβερνοασφάλειας, οι μέθοδοι και οι τρόποι των κυβερνητικών επιθέσεων και οι λόγοι που η ταχύτατη εξάπλωση της πανδημίας επέβαλλε την άμεση εφαρμογή μέτρων, το δεύτερο κεφάλαιο αναλύει τα πληροφοριακά συστήματα ήτοι τους ορισμούς, την λειτουργία τους, την σημαντικότητά τους για τον δημόσιο τομέα, την διαλειτουργικότητα τους, την ηλεκτρονική διακυβέρνηση στην Ελλάδα και την θέση της Ελλάδας στην Ευρώπη σε σχέση με αυτό καθώς και την πολιτική ασφαλείας που απαιτείται να εφαρμόζεται στα πληροφοριακά συστήματα προκειμένου να αναπτυχθούν με βάση τον κύκλο ζωής τους, το τρίτο κεφάλαιο εκτιμά και αξιολογεί ως μελέτη περίπτωσης τα πληροφοριακά συστήματα του Ηλεκτρονικού Ενιαίου Φορέα Κοινωνικής Ασφάλισης- e ΕΦΚΑ ήτοι την πληθώρα των πληροφοριακών συστημάτων καθώς και την πολιτική ασφαλείας του φορέα αναφερόμενο συνοπτικά και στα πληροφοριακά συστήματα άλλων φορέων, το τέταρτο κεφάλαιο ερευνά και μελετά τις απόψεις των υπαλλήλων του e ΕΦΚΑ για τα πληροφοριακά συστήματα και την υφιστάμενη κατάσταση που αντιμετωπίζουν στον φορέα και το πέμπτο κεφάλαιο καταλήγει σε συμπεράσματα και ενδεικτικές προτάσεις που προτρέπουν σε δράσεις και μεθόδους που θα παρακάμψουν πιθανά εμπόδια και θα προσφέρουν εφικτές λύσεις και τέλος αναφέρονται οι πηγές και η βιβλιογραφία.

ΚΕΦΑΛΑΙΟ 1ο

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

1.1. *Η έννοια της κυβερνοασφάλειας*

Όπως με πολλές έννοιες που χρησιμοποιούνται ευρέως, σε πολυάριθμα διαφορετικά συγκείμενα, και άπτονται μεταχείρισης τόσο σε πλαίσια ανεπίσημα και καθημερινά, όσο και σε πλαίσια πολιτικά, δικανικά ή ακαδημαϊκά, δεν είναι εύκολο να δώσει κανείς στην έννοια της *κυβερνοασφάλειας* έναν ορισμό επαρκή, ολοκληρωτικό, έτσι ώστε να αποδοθούν με διαύγεια και σαφήνεια όλες οι πτυχές της συνοπτικά.

Σύμφωνα με τις πιο ακριβείς και σύγχρονες προσεγγίσεις, όπως αυτή των Schatz Daniel et al. [1] της οποίας κάνει χρήση και η Βικιπαίδεια [2] , η κυβερνοασφάλεια μπορεί να οριστεί **ως η προστασία πληροφοριακών συστημάτων και δικτύων από δημοσιοποίηση πληροφοριών, κλοπή ή ζημιά στο υλικό, το λογισμικό ή τα ηλεκτρονικά δεδομένα, όπως επίσης και από την διαταραχή ή την παραπλανητική ανακατεύθυνση των υπηρεσιών που παρέχουν.** Συνοπτικότερα, στο εισαγωγικό, πλην κατά την γνώμη μας εξόχως επεξηγηματικό βιβλίο του το 2021, ο Duane C. Wilson ορίζει την κυβερνοασφάλεια ως την γενικευμένη προσπάθεια με στόχο την προστασία ψηφιακών αγαθών από διάρρηξη. [3]

Εμείς εδώ θα θέλαμε να συμπληρώσουμε το στοιχείο αυτό το οποίο η αναλυτικότερη επέκταση του Wilson, αλλά και άλλοι ορισμοί που συναντήσαμε στην έρευνά μας, καταδεικνύουν ως καίριο για την περιχάραξη των ορίων της έννοιας της κυβερνοασφάλειας: το στοιχείο της μη εξουσιοδοτημένης προσπέλασης. Προς τούτο, μία παρένθεση θα μας βοηθήσει να διαλευκάνουμε τον εννοιολογικό χώρο που ανήκει στην κυβερνοασφάλεια αντιστικτικά. Μια παρεμφερής έννοια με αυτή της κυβερνοασφάλειας είναι η έννοια της επιχειρησιακής ή λειτουργικής ασφάλειας, αναφερόμενη συχνότερα με το ακρωνύμιο OPSEC (Operations Security). Εδώ η λέξη «επιχειρησιακής» δεν παραπέμπει σε φορείς και δραστηριότητες που αφορούν το κεφάλαιο, αλλά σε μία δεδομένη επιχείρηση-αποστολή, ένα εγχείρημα «πολεμικής» κατά κάποιον τρόπο φύσης. Η χρήση της έννοιας αυτής ξεκίνησε από τις

[1] Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law

[2] https://en.wikipedia.org/wiki/Computer_security

[3] Wilson, Duance C. “Cybersecurity”(2021). The MIT Press Essential Knowledge Series, MIT Press

στρατιωτικές επιχειρήσεις κρατών, αλλά πλέον χρησιμοποιείται ευρέως από οποιονδήποτε πράκτορα δεν φέρει αξιώσεις εγκυρότητας ή εξουσιοδότησης για τα εγχειρήματά του[4] . Όσον αφορά τον κυβερνοχώρο, στις αρμοδιότητες της έννοιας εμπίπτουν ο εντοπισμός των κρίσιμων πληροφοριών, η ανάλυση των απειλών αλλά και των ευάλωτων σημείων ενός εγχειρήματος, και τέλος, η εφαρμογή κατάλληλων μέτρων που εξασφαλίζουν την προστασία από εχθρικές εξωτερικές παρεμβάσεις.

Παρότι είναι εμφανές ότι η έννοια του OPSEC στην πράξη φαίνεται να επικαλύπτεται με αυτή της κυβερνοασφάλειας, τουλάχιστον όσο η πρώτη αφορά τον κυβερνοχώρο, η κρίσιμη διαφορά είναι η εξής: η απουσία της έννοιας της εξουσιοδότησης, της έγκυρης ή μη έγκυρης χρήσης δεδομένων, της νόμιμης ή παράνομης πρόσβασης.

Τόσο οι κρατικές επιχειρήσεις στην σύγκρουση των συμφερόντων τους με άλλα κράτη και τις στρατιωτικές ή πληροφοριακές υπηρεσίες τους, όσο και οι κυβερνοεγκληματίες και άλλοι μεμονωμένοι πράκτορες που λειτουργούν στον κυβερνοχώρο εκτός των πλαισίων της νομιμότητας χωρίς απαραίτητα να λειτουργούν εκπεφρασμένα εναντίον της, χρησιμοποιούν αυτή την έννοια, και όχι την έννοια της κυβερνοασφάλειας, για να περιγράψουν την προστασία των δεδομένων τους, διότι, και στις δύο περιπτώσεις, δεν υφίσταται φορέας που μπορεί να νομιμοποιήσει ή όχι τις δραστηριότητες τους. Δεν υπάρχει, λοιπόν, ως φιγούρα ο «εγκληματίας» από τον οποίον το εγχείρημα προστατεύεται, παρά μόνο ο «εχθρός».

Γίνεται εμφανές, λοιπόν, ότι η έννοια της κυβερνοασφάλειας εγγενώς στηρίζεται σε ένα νομιμοποιητικό πλαίσιο, με φορείς οι οποίοι μπορούν να φέρουν αξιώσεις νομιμοποίησης, να κρίνουν δικαιούχους, να διακρίνουν μεταξύ δίκαιης και μη δίκαιης χρήσης ψηφιακού υλικού, και έτσι να διαχωρίσουν την χρήση από την κατάχρηση, να ορίσουν το περιχαρακωμένο έδαφος της νομιμότητας και της εγκυρότητας. Άρα, η κυβερνοασφάλεια αφορά *νομικά πρόσωπα*, πολιτικά αναγνωριζόμενα υποκείμενα, και όχι απλώς άτομα ή οργανισμούς, και αυτά μπορούν να είναι πολίτες, τόσο με την ιδιότητά τους ως ιδιώτες όσο και με την ιδιότητά τους ως μέλη που απαρτίζουν φορείς και οργανισμούς, ιδιωτικές και δημόσιες επιχειρήσεις, κρατικές οργανώσεις εφόσον αυτές αφορούν την εσωτερική συγκρότηση του κρατικού μηχανισμού, ή/και αποτελούν επιφάνειες διεπαφής με πολίτες στις διάφορες ιδιότητες τους.

Η κυβερνοασφάλεια *δεν* αφορά όμως, κρατικούς φορείς εφόσον η δραστηριότητά τους ανήκει στη σφαίρα του μη νομιμοποιήσιμου, αλλά στη σφαίρα των

[4] https://en.wikipedia.org/wiki/Operations_security

συμφερόντων του ως κράτος ανάμεσα σε άλλα κράτη, όπως στρατιωτικές ή πληροφοριακές επιχειρήσεις. Δεν αφορά ακόμη άτομα των οποίων η δραστηριότητα δεν αφορά μια ιδιότητα τους που κατοχυρώνεται από ένα πλαίσιο νόμου, είτε αυτό είναι το πλαίσιο του κράτους εντός του οποίου δραστηριοποιούνται, είτε διακρατικά και διεθνή πλαίσια, συνθήκες κ.ο.κ.

Έχοντας υπόψη τα παραπάνω, και κλείνοντας την παρένθεσή μας, μπορούμε να προχωρήσουμε την εννοιολογική διερεύνηση, αναλύοντας τους έξι στόχους της κυβερνοασφάλειας όπως απαριθμούνται στο μοντέλο του Wilson και καλύπτοντας εν συντομία τις πρακτικές που εμπίπτουν σε αυτό το στόχο. [5]

i. Εμπιστευτικότητα (Confidentiality)

Ο στόχος της εμπιστευτικότητας αφορά τον έλεγχο της πρόσβασης σε ευαίσθητα δεδομένα, τις διαδικασίες κατά τις οποίες εξασφαλίζεται πως οι εξουσιοδοτημένοι χρήστες έχουν εύκολη και εγγυημένη πρόσβαση σε συγκεκριμένα ψηφιακά αγαθά, ενώ παράλληλα οι μη εξουσιοδοτημένοι χρήστες αποτρέπονται ενεργητικά και συστηματικά από την απόκτηση τέτοιας πρόσβασης. Πρόκειται για έναν στόχο που μπορεί να γίνει εύκολα αντιληπτός χάριν της αναλογίας με πρακτικές που αφορούν μη ψηφιακά αγαθά και δεδομένα, όπως ο έλεγχος της πρόσβασης στην προσωπική ή ιδιωτική ιδιοκτησία με τη χρήση κλειδιού στο οποίο έχουν πρόσβαση οι δικαιούχοι του εν λόγω αγαθού. Στην κυβερνοασφάλεια, αντίστοιχα, η εμπιστευτικότητα εξασφαλίζεται με τη βοήθεια της κρυπτογραφίας, στη βάση της οποίας κατασκευάζονται ψηφιακά κλειδιά. Έτσι, τα ψηφιακά αγαθά μπορούν να μετασχηματιστούν σε μορφή τέτοια που τα κάνει μη αναγνώσιμα ή γενικώς μη προσπελάσιμα σε όλους εκτός από τους δικαιούχους, οι οποίοι μπορούν να «αποκωδικοποιούν» τα δεδομένα με το ψηφιακό τους κλειδί, δηλαδή τα μετασχηματίζουν πάλι στην αρχική, προσπελάσιμη μορφή τους. Τα ψηφιακά κλειδιά μπορεί να κατασκευάζονται μεμονωμένα, όπως στην παραπάνω περίπτωση, για την προστασία της εμπιστευτικότητας ενός ψηφιακού αγαθού, είτε σε ζεύγη, όταν αυτό που καλείται να παραμείνει εμπιστευτικό είναι ένα κανάλι επικοινωνίας μεταξύ δύο κόμβων σε ένα δίκτυο (εκεί και χρησιμοποιείται ευρύτερα το πρωτόκολλο των δημοσίων και ιδιωτικών κλειδιών, δηλαδή, της ασύμμετρης κρυπτογράφησης). Όταν οι παραπάνω πρακτικές αφορούν ιδιωτικά πρόσωπα, τότε συχνότερα μιλάμε για ιδιωτικότητα, μία έννοια που συμπεριλαμβάνεται στην έννοια της εμπιστευτικότητας.

[5] Wilson, Duance C. “Cybersecurity”(2021). The MIT Press Essential Knowledge Series, MIT Press

ii. Αξιοπιστία (Integrity)

Η αξιοπιστία αφορά την ακεραιότητα και την ταυτότητα των δεδομένων και των συστημάτων. Ένας χρήστης, ή ένας φορέας, απαιτεί ότι τα δεδομένα που αποθηκεύει και προσπελαύνει θα παραμείνουν ασφαλή και αναλλοίωτα, ότι οποιοσδήποτε τα αλλάζει ή παραμορφώνει έχει την κατάλληλη εξουσιοδότηση, και ότι μπορεί με εύκολο και αξιόπιστο τρόπο να ταυτοποιηθεί. Προς τούτο χρησιμοποιούνται συνήθως οι **συναρτήσεις κατακερματισμού (hashing functions),** εργαλείο βασισμένο και αυτό στις αρχές τις κρυπτογραφίας. Πρόκειται για μονόδρομες συναρτήσεις που σε κάθε κομμάτι ή πακέτο δεδομένων, αυθαίρετου μεγέθους, που τους εισάγεται, αντιστοιχούν κάποια πεπερασμένη τιμή, ιδανικά χρησιμοποιώντας επιπλέον μηχανισμούς που βεβαιώνουν ότι αυτή η τιμή είναι μοναδική. Το γεγονός ότι η συνάρτηση είναι μονόδρομη σημαίνει πως κάθε φορά που το ίδιο στοιχείο εισάγεται στη συνάρτηση, θα δίνει απευθείας και γρήγορα το ίδιο αποτέλεσμα, αλλά η αντίστροφη διαδικασία δεν μπορεί να πραγματοποιηθεί από αλγόριθμο σε πεπερασμένο χρόνο. Έτσι μπορεί ένας χρήστης, για παράδειγμα, να επιβεβαιώσει ότι ένα αρχείο είναι όντως αυτό που ισχυρίζεται ότι είναι, και όχι κάποιο κακόβουλο αρχείο μεταμφιεσμένο. Η πιο ευρεία χρήση αυτής της αρχής και των συναρτήσεων κατακερματισμού είναι στους **κωδικούς πρόσβασης (passwords),** οι οποίοι δεν αποθηκεύονται από το εκάστοτε σύστημα ολογράφως, αλλά τροφοδοτούνται σε μία συνάρτηση κατακερματισμού κάθε φορά που απαιτείται επαλήθευση, και το αποτέλεσμα της συνάρτησης συγκρίνεται με την αποθηκευμένη τιμή.Άλλα παραδείγματα είναι η επαλήθευση της γνησιότητας εφαρμογών που μεταφορτώθηκαν από το διαδίκτυο, αλλά και η εφαρμογή tripwire που ελέγχει την αξιοπιστία των αρχείων ενός συστήματος.

iii. Διαθεσιμότητα (Availability)

Η διαθεσιμότητα αφορά την ανάγκη να είναι προσβάσιμα τα δεδομένα στον χρόνο που κανείς τα χρειάζεται. Δεδομένης της αυξανόμενης εξάρτησης και των ιδιωτικών χρηστών, αλλά ιδιαίτερα των επιχειρήσεων και των φορέων, από το **cloud computing** (υπολογιστικό νέφος), οφείλει να διασφαλιστεί η άμεση και συνεχόμενη διαθεσιμότητα των δεδομένων προς χρήση, και να μειωθεί στο ελάχιστο ο χρόνος που το σύστημα «πέφτει» (**downtime)**. Οι εταιρείες που χρησιμοποιούν για την διάθεση των προϊόντων τους ιστοτόπους ηλεκτρονικών αγορών (**e-commerce**), επί παραδείγματι, έχουν ανάγκη να διασφαλίσουν ότι οι πιθανοί πελάτες μπορούν να

επισκεφθούν ανά πάσα στιγμή τα ηλεκτρονικά τους καταστήματα, ειδάλλως θα διακινδύνευαν ζημία.

Οφείλουμε εδώ να σημειώσουμε πως οι παραπάνω στόχοι δεν αποτελούν εύρημα του συγγράμματος από το οποίο τους αντλήσαμε, αλλά συνιστούν ευρέως αναγνωρισμένους από τη βιομηχανία στόχους, και κατονομάζονται με το ακρωνύμιο **CIA Triad.** Το μοντέλο του Wilson, όμως, προσθέτει επιπλέον τρεις στόχους, χτισμένους από τους θεμέλιους λίθους των παραπάνω, που θεωρεί πως η βιομηχανία συχνά παραγνωρίζει.

iv. Αυθεντικοποίηση (Authentication)

Η αυθεντικοποίηση αφορά την επαλήθευση της ταυτότητας ενός χρήστη, η βεβαίωση πως ένας χρήστης είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Η πρόσβαση στα περισσότερα ψηφιακά συστήματα στην εποχή μας διασφαλίζεται με **αυθεντικοποίηση πολλαπλών παραγόντων (multifactor authentication, MFA**). Αυτοί οι παράγοντες αφορούν κάποιο ιδιαίτερο χαρακτηριστικό που αφορά τον χρήστη μοναδικά, επί παραδείγματι: η γνώση ενός κωδικού πρόσβασης, η κατοχή κάποιου πιστοποιητικού αντικειμένου, η εγγραφή σε κάποιον τηλεφωνικό πάροχο με μοναδική κάρτα SIM στην οποία επικοινωνεί το σύστημα επιπλέον προσωρινούς κωδικούς μίας χρήσης, ή τα βιομετρικά δεδομένα του χρήστη (δακτυλικό αποτύπωμα, αναγνωριστικά χαρακτηριστικά του προσώπου).

v.Εξουσιοδότηση(Authorization)

Η εξουσιοδότηση λειτουργεί ακολουθώντας, και σε σύζευξη με την αυθεντικοποίηση. Αφορά τον προσδιορισμό της εμβέλειας της πρόσβασης του κάθε χρήστη στους διαφόρους πόρους ενός συστήματος (αρχεία, φάκελοι,εφαρμογές κ.λπ.). Ανάλογα με το αν ένας χρήστης έχει πρόσβαση διαχειριστή ή ιδιοκτήτη του συστήματος ή του αρχείου, αν πρόκειται για χρήστη με υπηρεσιακή πρόσβαση σε ένα σύστημα ή δίκτυο, ή αν πρόκειται για έναν απλό επισκέπτη, θα πρέπει να καθοριστεί σωστά από το σύστημα το επίπεδο και το εύρος των δυνατοτήτων του για προσπέλαση, αλλαγή και διαμόρφωση των πόρων. Οι **Λίστες Ελέγχου Πρόσβασης** (Access Control Lists), για παράδειγμα, είναι λίστες που αντιστοιχούν σε κάθε αρχείο, και καθορίζουν τα δικαιώματα που το χαρακτηρίζουν, δηλαδή ποιος μπορεί να εκτελέσει κάποια ενέργεια πάνω σε αυτό το αρχείο, και τι είδους ενέργεια θα είναι αυτή. Ακόμη, τα **Firewalls** (Τείχη Προστασίας) καθορίζουν αν θα επιτρέψουν εισερχόμενες ή

εξερχόμενες συνδέσεις μεταξύ κόμβων ενός δικτύου, χρησιμοποιώντας αντίστοιχες λίστες ελέγχου που εξαρτώνται από την εξουσιοδότηση των εκάστοτε κόμβων για τις συνδέσεις που επιχειρούν (π.χ. το τείχος προστασίας ενός σχολικού δικτύου δεν θα επιτρέπει σε υπολογιστές που χρησιμοποιούνται από μαθητές να συνδεθούν σε ιστοσελίδες που καθορίζονται ως επικίνδυνες ή ακατάλληλες).

vi. Μη αποποίηση (Non-repudiation)

Η μη αποποίηση αφορά την διατήρηση της υπευθυνότητας και της ταυτότητας στον ψηφιακό κόσμο. Το ζήτημα είναι η αποτροπή της αποποίησης ευθύνης από τον χρήστη για κάποια δραστηριότητα, όπως η αποστολή ενός μηνύματος ή η εξουσιοδότηση κάποιας πράξης, και συνήθως πραγματοποιείται με τη χρήση κάποιου είδους **ψηφιακής υπογραφής** (digital signature). Στην ηλεκτρονική αλληλογραφία, μπορούν να χρησιμοποιηθούν υπογραφές που κατασκευάζονται επί τη βάσει ψηφιακών κλειδιών κατά τις αρχές της ασύμμετρης κρυπτογραφίας (όπως αναφέραμε παραπάνω) για να καθορίζεται με βεβαιότητα, και ημιμονιμότητα σε βάθος χρόνου, η προέλευση του μηνύματος και η ταυτότητα του αποστολέα. Οι χρηματοοικονομικές επιχειρήσεις, ακόμη, που παρέχουν τις υπηρεσίες τους διαδικτυακά, χρησιμοποιούν μεθόδους ταυτοποίησης των χρηστών τους, απαιτώντας διαπιστευτήρια και δικαιολογητικά, ώστε να εξασφαλίσουν ότι έχουν πράγματι την δικαιοδοσία να πραγματοποιήσουν τις εκάστοτε συναλλαγές, αλλά και να προστατευτούν ενάντια σε ψευδείς διεκδικήσεις επιστροφής χρημάτων και λοιπές απόπειρες εξαπάτησης. Τέλος, συχνά χρησιμοποιούνται εξωτερικοί συνεργάτες, ουδέτεροι προς τις συναλλαγές και διαπραγματεύσεις, ώστε να διασφαλίσουν την συμμόρφωση και των δύο μερών στην εκάστοτε συμφωνία και να επιτηρήσουν την εγκυρότητά της. Τέτοιο παράδειγμα είναι οι αρχές έκδοσης ψηφιακών πιστοποιητικών (certificate authority) που επιβεβαιώνουν την αντιστοίχιση δημόσιων κλειδιών με τα νομικά πρόσωπα φερόμενα ως ιδιοκτήτες τους, επιτρέποντας σε άλλους φορείς και χρήστες να εμπιστευτούν τα κλειδιά και τις υπογραφές αυτές (όπως συμβαίνει με το, πλέον ευρύτατα σε χρήση, διαδικτυακό πρωτόκολλο **HTTPS**).

Με τα παραπάνω, πιστεύουμε πως έχουμε δώσει μία επαρκή, παρότι μη εξαντλητική ανάπτυξη και επεξήγηση της έννοιας της κυβερνοασφάλειας, του εύρους και της εμβέλειας της, αλλά και των προβλημάτων στα οποία καλείται να απαντήσει, καθιστώντας εφικτή, καθότι ευνομούμενη, τη χρήση των πληροφοριακών

συστημάτων σε εγχειρήματα αστείρευτης πολυπλοκότητας, και την διαπραγμάτευση των συμφερόντων πολλαπλών δικαιούχων και μερών.

1.2. *Μέθοδοι και τρόποι κυβερνητικών επιθέσεων*

Οι τρόποι διεκπεραίωσης μίας επίθεσης σε μία κυβερνητική επιφάνεια είναι πολυάριθμοι, και συχνά αλληλοεπικαλύπτονται. Κατά τη γνώμη μας, ο παραδοσιακός τρόπος ταξινόμησης εξαντλείται στην απαρίθμηση εργαλείων και τεχνικών, αποκομμένων από τα κατάλληλα συγκείμενα της χρήσης και εκμετάλλευσής τους. Μπορούμε να δούμε όμως πως την στείρα αυτή απαρίθμηση διαπερνά ένα κοινό νήμα εννοιών, που θα μας βοηθήσουν να συνθέσουμε μία περισσότερο συνεκτική κατανόηση της ενορχήστρωσης και εκπόνησης διαφορετικών ειδών επίθεσης σε ένα κυβερνητικό σύστημα.

Θα ακολουθήσουμε και εμείς, λοιπόν, για αρχή, την συμβατική αυτή απαρίθμηση, με την αξίωση να συνάγουμε ύστερα μία επαρκή και συμπαγή θεώρηση της πορείας μιας επίθεσης, την οποία καλείται να ανταγωνιστεί η πρακτική της κυβερνοασφάλειας.
Για αρχή, θα εξετάσουμε τα διάφορα είδη **κακόβουλου λογισμικού (malware)**, την έκτασή τους και την χρήση τους. Σύμφωνα με τον τυπικό ορισμό, κακόβουλο λογισμικό θεωρείται οποιοδήποτε λογισμικό έχει εκπεφρασμένα σχεδιαστεί με σκοπό να διαταράξει και να σαμποτάρει έναν υπολογιστή, έναν **εξυπηρετητή (server),** έναν **πελάτη (client),** ή ένα δίκτυο υπολογιστών, ώστε να διαρρεύσει ιδιωτικά δεδομένα, να δώσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή συστήματα, να στερήσει από κάποιον δικαιούχο πρόσβαση σε δεδομένα, ή γενικότερα να παρέμβει, χωρίς συναίνεση ή γνώση, στην ασφάλεια και την ιδιωτικότητα.[6]
Αν επιχειρήσουμε όμως εμείς να εξηγήσουμε το διακριτικό χαρακτηριστικό του κακόβουλου λογισμικού σε ένα πλαίσιο ευρύτερης κατανόησης των κυβερνητικών επιθέσεων, φιλοδοξώντας παράλληλα στην γενικότερη και περιεκτικότερη δυνατή εννοιολόγηση του όρου, θα λέγαμε το εξής: πως πρόκειται για ένα συγκεκριμένο είδος «δοχείου» (συγκεκριμένα, λογισμικού «δοχείου») για την τοποθέτηση και εκτέλεση ενός κακόβουλου **«φορτίου» (payload)**. Το «φορτίο» είναι συχνότερα, αλλά όχι αποκλειστικά, ένα ή περισσότερα κομμάτια κώδικα που στοχεύουν κάποιο **ευάλωτο σημείο (vulnerability)** στο λογισμικό ή το λειτουργικό σύστημα κάποιου

[6] https://en.wikipedia.org/wiki/Malware

υπολογιστή, δικτύου κ.λπ., ή έστω στο σημείο της διεπαφής του χρήστη ή των χρηστών με το λογισμικό ή το λειτουργικό σύστημα, με σκοπό είτε την υποκλοπή δεδομένων, είτε την κατάρρευση του συστήματος, είτε τον εκβιασμό των χρηστών του δικτύου για χρηματικό όφελος—γενικώς, την αδιαπραγμάτευτη παραβίαση του συστήματος προς οποιοδήποτε τέλος στοχεύει ο επιτιθέμενος πράκτορας, όσο φυσικά αυτό αφορά, και επιτρέπεται από, τις δυνατότητες τους συστήματος, και την αξία του τελευταίου για τους χρήστες.

Φυσικά, η ενεργοποίηση κακόβουλου φορτίου σε ένα σύστημα δεν εξαντλείται στην εγκατάσταση κακόβουλου λογισμικού. Όπως εξάλλου αναφέραμε, το κακόβουλο λογισμικό δεν είναι παρά ένας από τους τρόπους που ένα φορτίο μπορεί να τοποθετηθεί και να εκτελεστεί σε ένα σύστημα. Συγκεκριμένα, η μέθοδος αυτή συχνά αφορά την αλληλεπίδραση ενός ανυποψίαστου χρήστη με ένα αρχείο, έναν σύνδεσμο κ.λπ., το οποίο λειτουργεί ως φορέας του κακόβουλου φορτίου, και κατόπιν της αλληλεπίδρασης, εκκινεί την δυνητικά καταστροφική δράση του.

Επί παραδείγματι, το φορτίο μπορεί να κρύβεται σε ένα μέρος του κώδικα ενός χρήσιμου προγράμματος, και κατά την εγκατάσταση του προγράμματος από τον χρήστη (ο οποίος, αγνοώντας την ύπαρξη του φορτίου, έδωσε ενός είδους «συναίνεση» για την εκτέλεσή του, όσον αφορά τους μηχανισμούς άμυνας του υπολογιστή), αυτό εκτελείται στο παρασκήνιο, συχνά χωρίς ο χρήστης να αντιλαμβάνεται οτιδήποτε θα μπορούσε να του εγείρει υποψίες, μέχρι να είναι πολύ αργά. Σε λιγότερο συχνές περιπτώσεις, το φορτίο μπορεί να μην είναι καν ένα κομμάτι εκτελέσιμου κώδικα, αλλά η ίδια η δόμηση ενός αρχείου που καλείται να προσπελαστεί από ένα κατά τα άλλα υγιές πρόγραμμα. Σε μία τέτοια περίπτωση, το αρχείο έχει διαφθαρεί με κατάλληλο τρόπο, έτσι ώστε να παραβιάζει τα πρωτόκολλα προσπέλασής του από το πρόγραμμα που καλείται να το ανοίξει και να «βραχυκυκλώνει» τις εντολές που το υγιές πρόγραμμα είναι εξουσιοδοτημένο να εκτελέσει, φέροντας εις πέρας το αποτέλεσμα που επιθυμεί ο δράστης.

Αναλυτικότερα, τα είδη κακόβουλου λογισμικού ταξινομούνται στις κατηγορίες και υποκατηγορίες που θα αναφέρουμε αμέσως παρακάτω, αφού παρεμβάλλουμε μία παρατήρηση και διευκρίνισή μας. Δυστυχώς, το πρόβλημα που συναντάμε τόσο στον συμβατικό ορισμό όσο και στον παρακάτω τρόπο ταξινόμησης είναι μία σύγχυση του κακόβουλου φορτίου με την μέθοδο τοποθέτησης και ενεργοποίησής του, ενώ παράλληλα, παρατάσσονται οι διαφορετικές κατηγορίες κακόβουλου λογισμικού υπό

καθεστώς σύγχυσης ως προς το κριτήριο διάκρισης. Όπως εξηγήσαμε όμως παραπάνω, νιώθουμε το καθήκον να ακολουθήσουμε το συμβατικό πρότυπο, τουλάχιστον ως εφαλτήριο για τους προβληματισμούς μας, και έτσι η ταξινόμηση ακολουθεί ως εξής:[7][8][9]

a) **Ιοί (Viruses):**Οι ιοί μεταφέρουν ένα κακόβουλο φορτίο συνήθως (αν και όχι αποκλειστικά) με δύο τρόπους: είτε μολύνουν μία κατά τα άλλα υγιή εφαρμογή (π.χ. Microsoft Word, Excelκ.λπ.) επισυναπτόμενοι στην **ακολουθία αρχικοποίησης (initializations equence)** της εφαρμογής, εκτελώντας το φορτίο κατά την εκκίνηση της εφαρμογής, μεταφέροντας κατόπιν τα ηνία στον υγιή κώδικα του προγράμματος **(macroviruses)**, είτε επισυνάπτονται σε ένα εκτελέσιμο αρχείο **(π.χ. .exe)**, και εκτελούνται κατά την εγκατάσταση ή την εκτέλεση του εκτελέσιμου αρχείου, ή μεταμφιέζουν ένα εκτελέσιμο αρχείο που περιέχει τον κώδικα του φορτίου ως κάποιο μη εκτελέσιμο αρχείο **(fileinfectors)**. Οι ιοί έχουν στόχο τη μόλυνση του συστήματος στο οποίο εκτελούνται **(host)**, και αναπαράγονται ώστε να μολύνουν όσο το δυνατόν περισσότερα μέρη του συστήματος είναι εφικτό. Υπάρχουν και είδη ιών με πιο περίπλοκους μηχανισμούς, αλλά κρίνουμε πως δεν είναι σκόπιμο να τους αναφέρουμε στα πλαίσια της παρούσας ανάλυσης.
b) **Δούρειος Ίππος (Trojan):** ο όρος Trojan παίρνει το όνομά του από τον «Δούρειο Ίππο», διότι στην ευρύτερη του χρήση αφορά οποιοδήποτε λογισμικό εξαπατά ως προς την ταυτότητα και την πρόθεσή του [10] . Συνήθως υφέρπουν στον κώδικα κάποιου χρήσιμου προγράμματος και κάτω από την αντίληψη του χρήστη, ανοίγουν ένα δίαυλο επικοινωνίας με τον επιτιθέμενο πράκτορα, μία «πίσω πόρτα» (backdoor) στο μολυσμένο σύστημα, επιτρέποντας την μη εξουσιοδοτημένη πρόσβαση στο σύστημα κατά βούληση. Ο επιτήδειος πράκτορας υποκλέπτει πληροφορίες, συλλέγει δεδομένα που μπορεί να είναι απαραίτητα για μία δυνητικά σοβαρότερη και

[7] https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

[8]https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks

[9]https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

[10] https://en.wikipedia.org/wiki/Trojan_horse_(computing)

πιο κερδοφόρα επίθεση, ή/και διατηρεί το «δικαίωμα» να αναλάβει δυνατότητες και εξουσίες διαχειριστή στο σύστημα όποτε θελήσει (rootkits). Σημαντική διάκριση τους από τους ιούς είναι πως δεν αναπαράγονται ούτε εξαπλώνονται.

c) **Σκουλήκι (worms):** σε αντίθεση με τους ιούς, τα worms δεν επιτίθενται στο σύστημα που προσβάλλουν. Είναι αυτόνομα προγράμματα που επιζητούν να πολλαπλασιαστούν, να εξαπλωθούν και να διασπαρθούν μέσω του συστήματος σε άλλα συστήματα, και προς τούτο εκμεταλλεύονται ελαττώματα σε κάποιο δίκτυο. Είναι μοναδικοί μέσα στο φάσμα του κακόβουλου λογισμικού, διότι τυπικά δεν φέρουν κάποιο κακόβουλο φορτίο—το δοχείο είναι το ίδιο το φορτίο, και ο μόνος σκοπός της δράσης του είναι να μεταδοθεί και να διασκορπιστεί. Συχνά, η μόλυνση επιτυγχάνεται μέσω συνημμένων αρχείων ηλεκτρονικής αλληλογραφίας. Παρότι σπανίως προκαλεί στοχευμένα βλάβη στα συστήματα τα οποία μολύνει, τείνουν να υπερφορτώνουν τα δίκτυα από τα οποία μεταδίδονται, καταναλώνοντας εύρος ζώνης (bandwidth).

d) **Λογισμικό Κατασκοπείας (Spyware):**[11] λογισμικό κατασκοπείας θεωρείται οποιοδήποτε λογισμικό στοχεύει στην συλλογή πληροφοριών για κάποιο άτομο ή οργανισμό, και στέλνει τα δεδομένα αυτά σε κάποιον φορέα με τρόπο τέτοιο που ζημιώνει τον χρήστη. Αν και παραδοσιακά, ο όρος αναφερόταν σε εκπεφρασμένα κακόβουλο και μη νόμιμο λογισμικό, πλέον αναγνωρίζεται πως χρησιμοποιούνται τέτοιες πληροφοριακές πρακτικές και από έγκυρους και νόμιμους φορείς, με σκοπό την εξατομικευμένη διαφήμιση (όπως, για παράδειγμα, το Facebook). Τυπικά, αφορά ένα φάσμα από διαφορετικά είδη λογισμικού, από τα keyloggers (λογισμικό που καταγράφει κρυφά ό,τι πληκτρολογεί ο χρήστης) έως τα adware (λογισμικό που εγκαθίσταται λαθραία σε έναν περιηγητή ή σε ένα σύστημα με σκοπό να προωθήσει στον χρήστη διαφημίσεις και να τον ανακατευθύνει παραπλανητικά σε ιστοτόπους κερδοφόρους για τον επιτιθέμενο). Η χρήση του όρου έχει φθίνει τα τελευταία χρόνια, δεδομένης της κοινοτοπίας και της διάδοσης της παρακολούθησης των χρηστών στην πορεία τους στο διαδίκτυο από μείζονες εταιρίες, με την υποτιθέμενη, τυπικά νόμιμη, συναίνεση τους.

[11] https://en.wikipedia.org/wiki/Spyware

e) **Ransomware** [12]: πρόκειται για είδος κακόβουλου λογισμικού που υφαρπάζει την κατοχή των αρχείων και δεδομένων στο σύστημα ενός χρήστη ή φορέα, είτε απλώς αφαιρώντας την πρόσβαση από τον τελευταίο, δηλαδή κλειδώνοντας τον εκτός δικαιωμάτων ανάγνωσης και χρήσης, είτε, όπως είναι συνηθισμένο, κρυπτογραφώντας τα αρχεία του και, σε κάθε περίπτωση, ζητώντας λύτρα (εξού και η ονομασία ransomware) για να δώσουν πίσω στον χρήστη ή φορέα τα δεδομένα του. Μέχρι την συμμόρφωση του, τα δεδομένα παραμένουν πίσω από τείχος κρυπτογράφησης επ' αόριστον ή απειλείται η ακεραιότητά τους. Ενίοτε, απειλείται και η δημοσίευσή τους. Συνήθως πρόκειται για φορτίο που μεταφέρεται και εκτελείται μέσα σε ένα δοχείο trojan. Χάρη στα κρυπτονομίσματα, οι επίδοξοι δράστες μπορούν να διασφαλίσουν την ανωνυμία τους στις συναλλαγές, ενώ οι φορείς και οι χρήστες συχνά δεν έχουν καμία επιλογή παρά να ενδώσουν στις απαιτήσεις των εγκληματιών, δεδομένου του μεγέθους του διακυβεύματος. Το λογισμικό ransomware αποτελεί από τους πλέον σημαντικούς κινδύνους για οργανισμούς, φορείς και επιχειρήσεις στον τομέα της κυβερνοασφάλειας ακόμη και τη σημερινή εποχή.

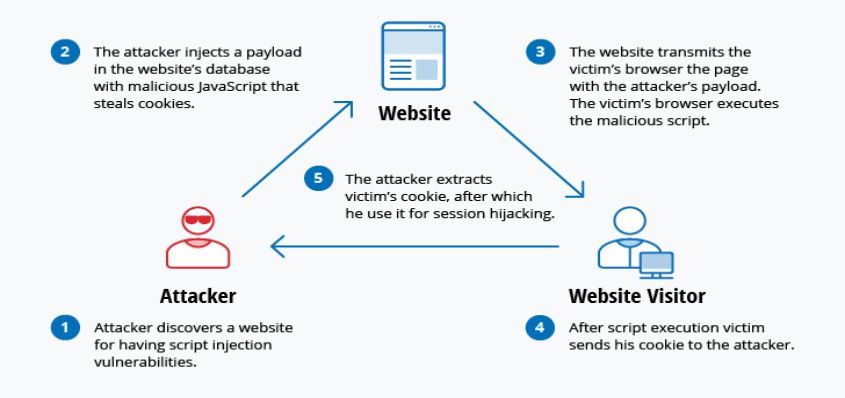
Αυτά ως προς το κακόβουλο λογισμικό, τη βασική εργαλειοθήκη ενός κυβερνοεγκληματία. Όπως γίνεται κατανοητό από τα παραπάνω, τα διαφορετικά είδη κακόβουλου λογισμικού επικαλύπτονται εννοιολογικά και δεν επιδέχονται σαφή και επαρκή ορισμό, ούτε μαρτυρούν ένα σαφές κριτήριο διάκρισης, προσδιοριζόμενα άλλοτε από την λειτουργία τους και άλλοτε από τον σκοπό και το είδος επίθεσης. Αρκετές από τις πιο ύπουλες χρήσεις λογισμικού κατασκοπείας χρησιμοποιούν εξειδικευμένους trojans, όπως η πλειοψηφία των επιθέσεων τύπου ransomware.

Θα προχωρήσουμε τώρα σε τύπους επιθέσεων που αφορούν την ανάπτυξη ιστοσελίδων. Μία «αρχαία» τακτική που χρησιμοποιούταν ευρέως για την παραβίαση ιστοσελίδων και θα φανεί σχετική στην έρευνά μας, είναι η έγχυση SQL (SQL injection).Η έγχυση SQL αφορά ιστοσελίδες που χρησιμοποιούν βάσεις δεδομένων, και τις διαχειρίζονται χρησιμοποιώντας γλώσσα SQL (πλέον η συντριπτική πλειοψηφία ιστοσελίδων απαιτεί κάποιου είδους βάση δεδομένων). Σε πεδία εισαγωγής (π.χ. πεδία αναζήτησης, πεδία πιστοποίησης όνομα χρήστη-κωδικού

[12] https://en.wikipedia.org/wiki/Ransomware

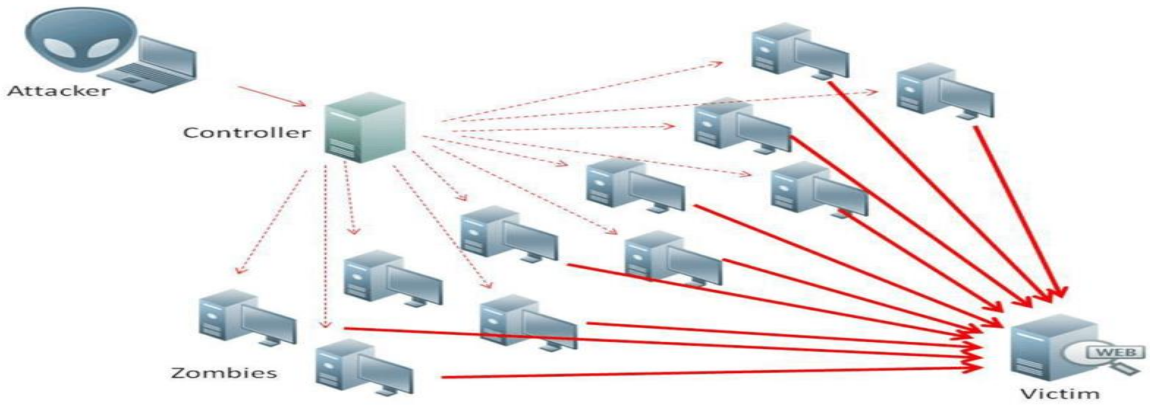
πρόσβασης) ο δράστης εισάγει εμβόλιμα εντολές SQL παραβιάζοντας την αναμενόμενη από το πρόγραμμα σύνταξη και εκμεταλλευόμενος ειδικούς χαρακτήρες όπως τα εισαγωγικά (‘’, “”). Τα δεδομένα που εισάγονται θα είναι μέρος μίας εντολής SQL που θα εκτελεστεί, και παραβιάζοντας την αναμενόμενη σύνταξη, ο εισβολέας αποκτά αυθαίρετα δικαιώματα τροποποίησης της εκάστοτε βάσης δεδομένων, κάτι που μπορεί να αποβεί εξαιρετικά ζημιογόνο για τους χρήστες που έχουν εμπιστευτεί τον ιστότοπο με τα δεδομένα τους. Οι εγχύσεις SQL θεωρούνται ευρέως παρωχημένες, αφού πλέον οι περισσότεροι γνωρίζουν πως αυτό συνιστά ευάλωτο σημείο, και φροντίζουν για την κατάλληλη «απολύμανση» των δεδομένων που εισάγονται στα διάφορα πλαίσια της ιστοσελίδας, πριν δοθεί σε αυτά η άδεια να τρέξουν σε κώδικα SQL (input sanitization).

Αντίστοιχο και πιθανώς πιο επικίνδυνο είδος επίθεσης σε ιστοσελίδες είναι το cross-site scripting ή XSS. Η επίθεση βασίζεται στην έγχυση ενός κακόβουλου φορτίου Javascript στον κώδικα κάποιας ιστοσελίδας, και την εκμετάλλευση της «αφελούς» προθυμίας που δείχνουν οι φυλλομετρητές να εκτελέσουν άκριτα κώδικα Javascript, όταν μία ιστοσελίδα (η οποία εδώ έχει παραβιαστεί) τους ζητήσει να τον εκτελέσει για την υποτιθέμενη ορθή λειτουργία της. Αφότου το φορτίο κώδικα έχει τοποθετηθεί στην ιστοσελίδα, ο φυλλομετρητής εκτελώντας τις νόμιμες εντολές της ιστοσελίδας, εκτελεί και το φορτίο, με ό,τι αυτό μπορεί να συνεπάγεται. Οι επιθέσεις cross-site scripting μπορεί να έχουν αποτέλεσμα την διαρροή των cookies περιήγησης, τα οποία αποστέλλονται στον κυβερνοεγκληματία, με αποτέλεσμα ο τελευταίος να πλαστογραφεί τα δεδομένα μίας συνεδρίας και να φέρεται ηλεκτρονικά ως τα θύματα. Σε περιπτώσεις όπου το διακύβευμα είναι τραπεζικά δεδομένα, ή άλλες ευαίσθητες συναλλαγές, είναι εξαιρετικά σημαντικό να χρησιμοποιηθούν μέθοδοι που αποτρέπουν κάθε τέτοια επίθεση, όπως τα προσωρινά και μοναδικά tokens συνεδρίας.



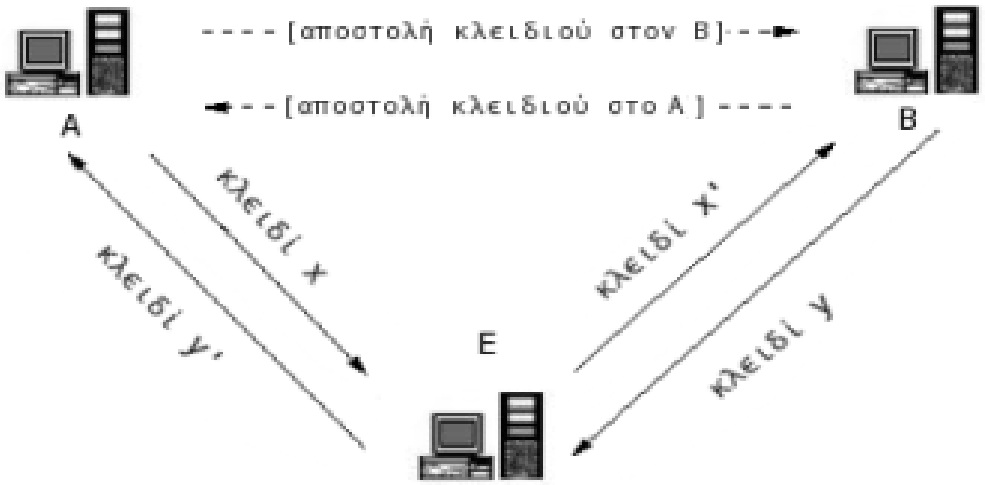
Εικόνα 1: Επίθεση τύπουCross-Site Scripting (https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks)

Ακόμη, υφίστανται οι επιθέσεις που έχουν ως σκοπό το σπάσιμο (cracking) των κωδικών πρόσβασης (passwords), επιθέσεις που μπορούν να αφορούν οποιαδήποτε επιφάνεια επίθεσης (attack surface) που κάνει χρήση αυθεντικοποίησης τέτοιου είδους. Προς τούτο, η πλέον αξιόπιστη, πλην χρονοβόρα και άκομψη, είναι η τεχνική brute-force attack, κατά την οποία ένας αλγόριθμος δοκιμάζει όλους τους πιθανούς συνδυασμούς από διαθέσιμα πλήκτρα διαδοχικά, με την μαθηματική βεβαιότητα ότι μέχρι να τελειώσουν οι δυνατοί συνδυασμοί, ο κωδικός θα έχει βρεθεί. Ο παραπάνω αλγόριθμος όμως σύντομα γίνεται μη ρεαλιστικός, καθώς ο χρόνος που χρειάζεται για να τρέξει αυξάνεται εκθετικά, και όχι πολυωνυμικά, καθώς αυξάνεται το μήκος του κωδικού σε ψηφία, αλλά και η δεξαμενή των δυνατών ψηφίων που θα πρέπει να δοκιμαστούν για κάθε θέση. Πρακτικά, χρησιμοποιούνται βάσεις δεδομένων ή λίστες με γνωστούς κωδικούς, οι οποίοι έχουν γίνει γνωστοί από παρελθοντικές διαρροές και επιθέσεις σε δημοφιλείς ιστοτόπους (dictionary attacks, credential stuffing). Στις γνωστές μεθόδους επίθεσης μέσω διαδικτύου ανήκουν και οι επιθέσεις άρνησης εξυπηρέτησης (Denial-of-Service attacks or DoS) ή/και διασκορπισμένης άρνησης εξυπηρέτησης (Distributed DoS). Οι επιθέσεις (D) DoS δουλεύουν πλημμυρίζοντας συστήματα, εξυπηρετητές ή/και δίκτυα με αιτήματα εξυπηρέτησης, με σκοπό να υπερφορτώσουν το εύρος ζώνης και γενικότερα τους πόρους διαχείρισης αιτημάτων του. Το σύστημα-θύμα, ως συνέπεια του κορεσμού του, καθίσταται ανίκανο να ανταπεξέλθει στα νόμιμα αιτήματα για εξυπηρέτηση, και έτσι η φυσιολογική του λειτουργία παύει. Η διαθεσιμότητα του συστήματος στο Διαδίκτυο θίγεται, και ο κυβερνοεγκληματίας μπορεί είτε να κλιμακώσει την επίθεσή του εκμεταλλευόμενος την κατάσταση αυτή, είτε να ζητήσει τα αιτήματά του να εκπληρωθούν για να ανακαλέσει τα ασταμάτητα αιτήματα που φράσσουν το δίκτυο.



Εικόνα 2: Μία επίθεση Distributed Denial of Service (DDoS). (https://el.safetydetectives.com/blog/τι-είναι-μια-επίθεση-ddos/

Αρκετά κοινές και σημαντικές ώστε να παρουσιαστούν εδώ είναι και οι επιθέσεις man-in-the-middle. Ένας επιτιθέμενος παρεμβάλλει τον εαυτό του και το σύστημά του ανάμεσα σε δύο νόμιμα επικοινωνούντες χρήστες/συστήματα, και είτε υποκλέπτει/κρυφακούει (eavesdropping)[13] είτε αλλοιώνει το μήνυμα που μεταφέρεται,υφαρπάζοντας τα κλειδιά που ανταλλάσσονται και υποσκάπτοντας την λειτουργία της κρυπτογραφικής συνάρτησης.

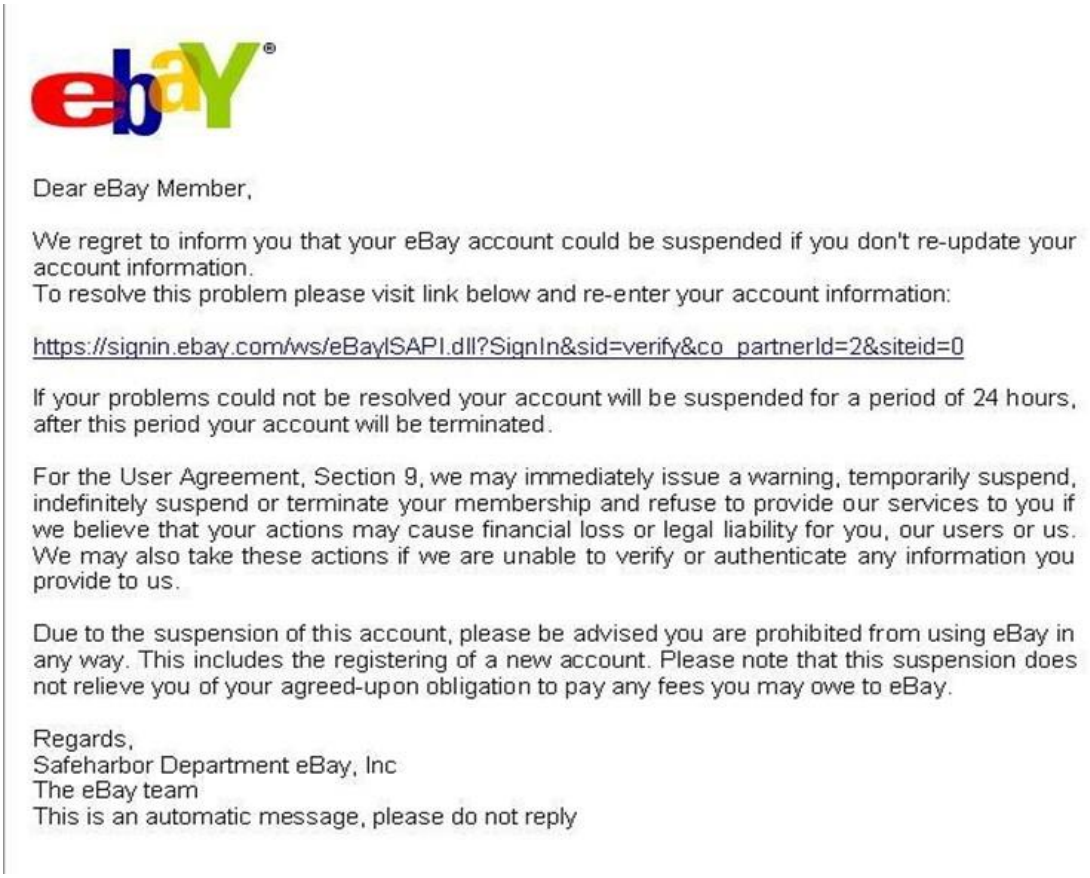


Εικόνα 3: ΕπίθεσηMan-in-the-Middle (MitM) (https://el.wikipedia.org/wiki/Επίθεση_man-in-the-middle)

Μία τέτοια επίθεση μπορεί να λάβει πολλές μορφές και να πραγματοποιηθεί σε πολλά διαφορετικά πλαίσια και συγκείμενα. Μία τέτοια μορφή είναι το session hijacking, κατά το οποίο ο δράστης αντικαθιστά τη δική του διεύθυνση IP για την διεύθυνση ενός πιστοποιημένου πελάτη (client), και πραγματοποιεί όλες τις συναλλαγές με τον εξυπηρετητή στην θέση του. Οι επιθέσεις MitM ήταν αρκετά συχνές στις εποχές που τα κοινά ασύρματα δίκτυα, όπως τα δημόσια WiFi σε καφετέριες, δεν ήταν ασφαλισμένα κατάλληλα, και ένας κακόβουλος πράκτορας μπορούσε να προσποιηθεί πως ο υπολογιστής του ήταν ο ίδιος ο κόμβος του δικτύου και έτσι να υποκλέψει όλα τα πακέτα που αποστέλλονταν μέσα από αυτόν. Είναι ιδιαίτερα δύσκολο να ανιχνευτούν, διότι τα μέλη που προσπαθούν να επικοινωνήσουν νόμιμα συχνά δεν έχουν τρόπο να εξετάσουν αν παρεμβάλλεται κάποιος στην επικοινωνία τους. Τέλος, θα πρέπει να αναφέρουμε τις επιθέσεις phishing. Πρόκειται

[13] https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle

ίσως για το πιο διαδομένο και επιτυχημένο είδος επίθεσης στις μέρες μας, και είναι ένα ιδιόμορφο social engineering («κοινωνική μηχανική), εξαρτάται δηλαδή από την εκμετάλλευση και την εξαπάτηση των ανθρώπινων αδυναμιών σε ένα κυβερνητικό σύστημα, και όχι τις αδυναμίες λογισμικού ή υλισμικού. Γενικότερα, κατά το phishing ο δράστης κατασκευάζει παραπλανητικά μηνύματα ηλεκτρονικής αλληλογραφίες και ιστοσελίδες, τα οποία μιμούνται την διαμόρφωση, τις εικόνες, το κείμενο κ.ο.κ. ενός έγκυρου φορέα με σκοπό την εξαπάτηση χρηστών σε μαζική κλίμακα, οι οποίοι, χάριν αφέλειας, δεν θα είναι σε θέση να διακρίνουν τις όποιες διαφορές από τον πραγματικό, έγκυρο φορέα. Ακόμη, τα μηνύματα συνοδεύονται με συγκαλυμμένες απειλές που παροτρύνουν το θύμα να δράσει άμεσα.[14]



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Εικόνα 4: Παράδειγμα παραπλανητικού phishingemail που προσποιείται πως εκπορεύεται από το E-bay (https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing)

Συχνά, οι κυβερνοεγκληματίες στέλνουν εκατομμύρια μηνύματα ηλ. ταχυδρομείου με την αξίωση ότι αντιπροσωπεύουν π.χ. τράπεζες, ή έγκυρους φορείς ενημέρωσης, και ανακατευθύνουν ύστερα τους ανυποψίαστους χρήστες σε ιστοσελίδες δικής τους

[14] https://el.wikipedia.org/wiki/Phishing

κατασκευής, όπου αυτοί καλούνται να εισάγουν τους κωδικούς πρόσβασής τους και άλλα δεδομένα αυθεντικοποίησης, τα οποία από εκείνη τη στιγμή και ύστερα, βρίσκονται στην διάθεση του δράστη να τα χειριστεί προς ίδιον όφελος. Τύποι phishing είναι το spear phishing (phishing με στόχο συγκεκριμένες επιχειρήσεις και άτομα) και το whaling (phishing με στόχο υψηλόβαθμα στελέχη μίας επιχείρησης ή οργάνωσης).

Θεωρούμε πως τα παραπάνω συνιστούν μία επαρκή, παρότι και πάλι μη εξαντλητική, απαρίθμηση των εργαλείων που οι κυβερνοεγκληματίες έχουν στη διάθεσή τους για την πραγματοποίηση των σκοπών τους. Μένει μόνο να δούμε πώς τα ετερογενή εργαλεία αυτά συντίθενται για να πραγματοποιηθεί μία ρεαλιστική επίθεση. Προς τούτο, θα παραθέσουμε το μοντέλο Cyber Kill Chain, που αναπτύχθηκε αρχικά από την εταιρεία Lockheed Martin [15] ως το αντίστοιχο του στρατιωτικού μοντέλου kill chain[16] στο κυβερνοχώρο, και περιγράφει την πορεία και τα στάδια μίας κυβερνοεπίθεσης.

Σύμφωνα με την Lockheed Martin, τα 7 στάδια μίας κυβερνοεπίθεσης έχουν ως εξής:

1) Αναγνώριση (Reconnaissance): Αρχικά, ο επίδοξος εισβολέας επιλέγει τον στόχο του και διεξάγει την κατάλληλη έρευνα που θα καταστήσει δυνατή την επίθεση. Συλλέγει στοιχεία για την διαρρύθμιση και την οργάνωση του στόχου, τα μέτρα προστασίας του και τις πολιτικές ασφαλείας του, και αποπειράται να ανιχνεύσει ευάλωτα σημεία σε κάθε βαθμίδα της διάρθρωσής του.

2) Κατασκευή όπλου (Weaponization): Ο εισβολέας, χρησιμοποιώντας τα στοιχεία που έχει συλλέξει, κατασκευάζει κάποιου είδους κακόβουλο λογισμικό, με φορτίο και δοχείο κατάλληλα σχεδιασμένα και προσαρμοσμένα να διαρρήξουν τα ευάλωτα σημεία του συστήματος-στόχου.

3) Παράδοση (Delivery): Ο εισβολέας μεταδίδει το κακόβουλο λογισμικό στον στόχο του, με όποια μέσα κρίνει κατάλληλα. Τέτοιοι φορείς είναι μηνύματα ηλ. ταχυδρομείου (phishing), αποσπώμενο μονάδες υλισμικού (USB, CD), και πλαστογραφημένες ιστοσελίδες.

[15] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[16] https://en.wikipedia.org/wiki/Kill_chain

4)Εκμετάλλευση (Exploitation): Σε αυτό το στάδιο, το κακόβουλο φορτίο εκτελείται στο σύστημα του θύματος, εκμεταλλεύεται τα ευάλωτα σημεία, πολλαπλασιάζει τις αδυναμίες του, ώστε να καταστήσει το σύστημα πλήρως τρωτό.

5) Εγκατάσταση (Installation): Επιπλέον, το κακόβουλο λογισμικό εγκαθιστά κάποιο σημείο απομακρυσμένης πρόσβασης (π.χ. backdoor), ώστε ο εισβολέας να έχει ανοιχτό κανάλι ελέγχου και επικοινωνίας με το σύστημα ανά πάσα στιγμή.

6) Διεύθυνση και Έλεγχος (Command and Control): Το κακόβουλο λογισμικό κλιμακώνει τα δικαιώματα πρόσβασης του εισβολέα, ώστε ο τελευταίος αποκτά πλήρες έλεγχο του συστήματος και του δικτύου. Αποπειράται ηπαραβίαση περαιτέρω διαπιστευτηρίων που θα δώσουν στον εισβολέα τα προσδοκώμενα δεδομένα.

7) Εκτέλεση Στόχων (Actions on Objective): Εφόσον τα παραπάνω έχουν πραγματοποιηθεί, ο εισβολέας προχωρά στις επιθυμητές ενέργειες, όπως η εκμαίευση και υποκλοπή δεδομένων, η καταστροφή δεδομένων ή η κρυπτογράφηση δεδομένων με σκοπό τον εκβιασμό του θύματος για λύτρα ή οποιονδήποτε άλλο επιθυμητό σκοπό.

Το παραπάνω μοντέλο θεωρούμε πως δίνει μία καθαρή εικόνα για το πώς τα εργαλεία, οι τεχνικές και οι μέθοδοι που είχαμε απαριθμήσει, συνδράμουν για να επιτευχθεί ένα συμπαγές και ενιαίο σχέδιο, από την γωνία θέασης του κυβερνοεγκληματία, και ελπίζουμε πως διαλευκάνει τη σύγχυση που προκύπτει από την αλληλοεπικάλυψη των διαφορετικών μεθόδων και τεχνικών.

1.3. *Οι συνέπειες της πανδημίας στην κυβερνοασφάλεια*

Η πρωτοφανής και απρόβλεπτη έκρηξη και εξάπλωση της πανδημίας COVID-19 από τις αρχές του 2020 έως και σήμερα, είχε αναπόφευκτο αποτέλεσμα την ριζική αναδιάρθρωση της καθημερινής μας ζωής, και ως εκ τούτου, του τρόπου που τόσο ο ιδιωτικός όσο και ο δημόσιος τομέας διαπραγματεύονται και διαχειρίζονται τις συνθήκες υπό τις οποίες η εργασία καθίσταται ανέφικτη. Το διακύβευμα, η συνέχιση της ομαλότητας της διεκπεραίωσης των επιχειρηματικών και κρατικών δραστηριοτήτων, φέρει τη βαρύτητα ενός είδους φυσικής επιλογής για τις Δυτικές κοινωνίες. Η διατήρηση μιας διαμεσολαβημένης κανονικότητας μέσω του Διαδικτύου

και των πολύμορφων μέσων και εργαλείων που έχει στη διάθεση του, ήταν μη διαπραγματεύσιμη ανάγκη, και συνέβη με ρυθμούς ραγδαίους, ανώμαλα, μη προγραμματισμένα.

Είναι εμφανές πώς μια τέτοια κατάσταση εξαίρεσης και ανωτέρας βίας, οδηγεί οργανικά στην υιοθέτηση όχι συστηματοποιημένων, οργανωμένων, προγραμματισμένων πληροφοριακών συστημάτων και πρωτοκόλλων αλληλεπίδρασης, αλλά σε ένα αυθόρμητα συναρμολογημένο «κολλάζ» από ετερογενείς, μη εσωτερικά συνεχείς και αφομοιωμένες, τεχνολογίες, τις οποίες κλήθηκαν να χρησιμοποιήσουν μη προετοιμασμένοι εργαζόμενοι. Η προτεραιότητα ήταν η επιβίωση και η προστασία της κοινωνίας, της συμπαγούς λειτουργίας του κράτους, και της διατήρησης του κεφαλαίου στην επιφάνεια.

Μία τέτοια κατάσταση αποδιοργάνωσης εμφανίζεται ως ελκυστική ευκαιρία για έναν κυβερνοεγκληματία. Χωρίς αμφιβολία, υπό κανονικές συνθήκες, τόσο οι επιχειρήσεις, όσο και οι κρατικοί μηχανισμοί, έχουν πολλαπλές δικλείδες ασφαλείας και οδηγίες χρήσης προς τους εργαζομένους, έχοντας συνήθως συνάψει συνθήκες με εταιρίες που ειδικεύονται στην κυβερνοασφάλεια, ώστε να μειωθούν στο ελάχιστο οι ρωγμές και πληροφοριακές διαρροές που θα μπορούσαν να καταστήσουν το σύστημα τους ευάλωτο, έτσι ώστε ακόμη και αν η προοπτική της επίθεσης δεν δύναται να εξουδετερωθεί πλήρως, η πιθανή ζημιά ελαχιστοποιείται, και η «δουλειά» του εγκληματία δυσχεραίνεται εκθετικά, τόσο ώστε το κόστος του εγχειρήματος να είναι αποτρεπτικό στην πλειοψηφία των περιπτώσεων.

Όπως αρκετοί ειδικοί στον χώρο της κυβερνοασφάλειας επισημαίνουν, το ζήτημα και το αντικείμενο της κυβερνοασφάλειας δεν ήταν ποτέ η τεχνολογία και η αλγοριθμική θωράκισή της, αλλά ο ανθρώπινος παράγοντας. Οι συνθήκες υπό τις οποίες εμφανίζονται ρωγμές σε μία κυβερνητική επιφάνεια, γόνιμες προς εκμετάλλευση, είναι συνάρτηση αφελούς εμπιστοσύνης, παραμέλησης και άγνοιας στους ανθρώπους ως προς την κίνησή τους στον κυβερνοχώρο. Το έγκλημα στον κυβερνοχώρο μπορεί να παρομοιαστεί με ένα ιδιόμορφο είδος ταχυδακτυλουργικής: βασίζεται στον αντιπερισπασμό της προσοχής του χρήστη όσο ο επιτιθέμενος πράκτορας εισβάλλει ακριβώς στο «τυφλό» σημείο του. Επιστρέφοντας, όμως, στο πρόσφατο παρελθόν, η αναγκαιότητα της επείγουσας εύρεσης καινούριων και μη δοκιμασμένων πληροφοριακών υποδομών, σε συνδυασμό με την περιρρέουσα ατμόσφαιρα σύγχυσης και υπαρξιακής αγωνίας που καταλύει την εσωτερική οργάνωση της

καθημερινότητας και της ψυχικής ζωής του εργαζομένου, απέκλεισε την σωστή και εύρυθμη εφαρμογή διαδικασιών όπως οι παραπάνω, που θα μπορούσαν να εξασφαλίσουν ένα εύρωστο τείχος προστασίας στον πλέον απεδαφικοποιημένο χώρο εργασίας. Ακόμη, οι φορείς και οι επιχειρήσεις δεν είναι οι μόνοι πιθανοί στόχοι κυβερνοεγκληματιών που έμειναν ξαφνικά ευάλωτοι. Η απομόνωση των ατόμων στο σπίτι έχει ως άμεσο αποτέλεσμα την δραματική αύξηση του χρόνου παραμονής και περιήγησης στο Διαδίκτυο. Έτσι, οι πιθανότητες το ίδιο το άτομο να πέσει θύμα μιας μαζικής εκστρατείας phishing, για παράδειγμα, που έχει ακριβώς στοχαστική φύση, και όχι συγκεκριμένο στόχο, συλλέγοντας δεδομένα όσων χρηστών εξαπατηθούν, ενώ απαιτεί ελάχιστη προσπάθεια, αυξάνονται εξίσου δραματικά. Πράγματι, παρατηρήθηκε πως το 47% των ατόμων που δούλευαν από το σπίτι, έπεσαν θύματα phishing, κατά τη διάρκεια της εργασίας. Συγκεκριμένα, η ανάγκη για συνεχείς ενημερώσεις ως προς την εξέλιξη της πανδημίας, οδήγησε σε πολλαπλές απάτες, που χρησιμοποιούσαν, ως δόλωμα, ειδήσεις σχετικά με τον COVID-19. Επί παραδείγματι, η Αστυνομία της Πόλης του Λονδίνου δήλωσε πως από τον Ιανουάριο του 2020, 11 εκατομμύρια λίρες έχουν απολεσθεί, αποκλειστικά εξαιτίας κάποιας παραλλαγής της παραπάνω απάτης. Παραβιάσεις που στοχεύουν ακριβώς στην διασταύρωση του διαδικτυακού χώρου εργασίας με τους εργαζόμενους ως ιδιωτικοί χρήστες, επίσης πολλαπλασιάστηκαν. Αρκεί να εξετάσουμε, και πάλι, σε θεωρητικό επίπεδο την φύση της μετάβασης για να «προβλέψουμε» και εκ των υστέρων τι ήταν αναπόφευκτο να συμβεί στο σημείο αυτής της διασταύρωσης. Όταν οι διάφορες δραστηριότητες των ατόμων ήταν χωρικά διακεκριμένες, τα milieu της κάθε αλληλεπίδρασης χωρισμένα, διαθέτοντας εσωτερική ενότητα και συμπάγεια το καθένα, με τους δικούς τους μηχανισμούς προστασίας, θα ήταν δύσκολο να αποσπαστούν χρήσιμα δεδομένα για τα άτομα που απαρτίζουν αυτούς τους χώρους και δραστηριοποιούνται εκεί, με τέτοιο τρόπο ώστε επιθέσεις είτε στοχευμένες είτε στοχαστικές να μπορέσουν να πραγματοποιηθούν με όφελος. Στην εποχή του COVID-19, όμως, με την μεταφορά των περισσότερων δραστηριοτήτων που προϋποθέτουν κοινωνική αλληλεπίδραση στον κυβερνοχώρο, ο τελευταίος γίνεται μία οριζόντια και ομοιογενής επιφάνεια, πάνω στην οποία τα εδάφη των διαφορετικών αλληλεπιδράσεων χάνουν τα σαφή όρια τους και «διαρρέουν» το ένα μέσα στο άλλο.

Οι ετερογενείς χώροι με τα όρια τους και τις αποστάσεις που τους χώριζαν, σε αυτή τη νέα επιφάνεια γίνονται απλώς πόλοι ή επιμέρους κέντρα σημασιοδότησης και

έλξης, και το έδαφος τους κινείται και μεταμορφώνεται σε συστοιχία με την κίνηση και τις μεταμορφώσεις της επιφάνειας. Έτσι *ο κυβερνοχώρος ο ίδιος* μετατρέπεται κατά ένα τρόπο σε ένα «μοναδικό σημείο αποτυχίας» (single point of failure) και έτσι η διάρρηξη ενός μόνο σημείου του δύναται να προκαλέσει σεισμικές δονήσεις σε οτιδήποτε άλλο κατανέμεται πάνω σε αυτή την επιφάνεια.

Μπορούμε εύκολα να δούμε, και συγκεκριμένα, πώς πράγματι ακριβώς η ευαλωτότητα αυτής της διάρθρωσης των αλληλεπιδράσεων υπήρξε καταστροφική. Υπέρογκες βάσεις δεδομένων από παρελθοντικές διαρροές δεδομένων χρηστών (της τάξης των εκατομμυρίων ή και δισεκατομμυρίων) από δημοφιλείς ιστοσελίδες (π.χ. κοινωνικής δικτύωσης), που ενίοτε πωλούνται σε κυβερνο-εγκληματίες ή και διατίθενται δωρεάν, αξιοποιήθηκαν πλέον σε κλίμακα άνευ προηγουμένου από επιτιθέμενους. Το ευάλωτο σημείο που διαρρηγνύεται εδώ (η μέθοδος είναι γνωστή ως credential stuffing) είναι η τάση της πλειοψηφίας των χρηστών να ανακυκλώνουν τα στοιχεία και τους κωδικούς τους, να χρησιμοποιούν δηλαδή, για την πρόσβαση στον διαδικτυακό χώρο εργασίας ή σε πλατφόρμες τηλεδιάσκεψης, τα ίδια στοιχεία με τις ιστοσελίδες που επισκέπτονται με προσωπικό λογαριασμό για ιδιωτικούς σκοπούς. Έτσι οι επιτιθέμενοι μπορούν τόσο να αποκτήσουν πρόσβαση στο εσωτερικό της πλατφόρμας μιας εταιρίας μέσα από λογαριασμούς εργαζομένων, και να προκαλέσουν αξιοσημείωτη, ακόμη και μη επιδιορθώσιμη ζημιά. Ακόμη, μπορούσαν να εισβάλλουν στην ιδιωτική ζωή των εργαζομένων και να τους ηχογραφήσουν ή να τους βιντεοσκοπήσουν, ώστε να πουλήσουν αυτές τις καταγραφές στο dark web.[17]

1.4. *Επιβολή μέτρων ασφαλείας και σύσταση νέων οργανισμών στην μετά-COVID εποχή*

Από τα ανωτέρω συμπεραίνουμε ότι η αυστηρότερη επιβολή μέτρων ασφαλείας στην μετά covid εποχή ήταν επιτακτική ανάγκη για κάθε οργανισμό δημόσιο ή ιδιωτικό.

[17] https://eurozoi.gr/2022/01/%ce%b7-%ce%ba%cf%85%ce%b2%ce%b5%cf%81%ce%bd%ce%bf%ce%b1%cf%83%cf%86%ce%ac%ce%bb%ce%b5%ce%b9%ce%b1-%cf%83%cf%84%ce%b7%ce%bd-%ce%b5%ce%b5-%cf%84%ce%b7%ce%bd-%cf%80%ce%b5%cf%81%ce%af%ce%bf%ce%b4%ce%bf/

Η αυξημένη μεταδοτικότητα του ιού άλλαξε την καθημερινότητά μας, μετέβαλλε το εργασιακό περιβάλλον αυξάνοντας το ποσοστό της εξ αποστάσεως εργασίας,[18] επηρέασε τις εμπορικές συναλλαγές με πληθώρα αγορών μέσω διαδικτύου, μας υποχρέωσε να συναλλαχτούμε με την δημόσια ψηφιακή διοίκηση και τελικά μας ανάγκασε να αλλάξουμε την οπτική μας και την κουλτούρα μας.

Η έξαρση της πανδημίας, με σύμμαχο την ραγδαία εξέλιξη της τεχνολογίας της πληροφορίας και των τηλεπικοινωνιών, βοήθησε τον υπό εξέλιξη παγκόσμιο μετασχηματισμό.

Τα αυξημένα ποσοστά κυβερνοεγκλημάτων[19] επέβαλλαν και ταυτόχρονη αύξηση μέτρων ασφαλείας για επαρκή προστασία και μείωση των αρνητικών επιπτώσεων.

Από τα στοιχεία που αντλήσαμε από την 'Ευρωπαική 'Ενωση και αναφέρονται κατωτέρω προκύπτει ότι υπάρχει ανησυχία, πρόβλεψη αλλά και μέριμνα και ενισχυμένα μέτρα ασφαλείας που επιβάλλεται να εφαρμόσουν τα κράτη μέλη προκειμένου να αντιμετωπισθούν οι ορατοί κίνδυνοι στο κυβερνοχώρο.

«*Ο αριθμός, η πολυπλοκότητα και η κλίμακα των περιστατικών στον κυβερνοχώρο αυξάνονται, όπως και ο οικονομικός και κοινωνικός αντίκτυπός τους. Η πανδημία του κορωνοϊού έχει προκαλέσει μια απρόβλεπτη επιτάχυνση στον ψηφιακό μετασχηματισμό του κοινωνίες σε όλο τον κόσμο. Ωστόσο, έχει επίσης επιδεινώσει τα υπάρχοντα προβλήματα, όπως το ψηφιακό χάσμα, και συνέβαλε στην παγκόσμια αύξηση των περιστατικών κυβερνοασφάλειας. Σε αυτή την πρωτόγνωρη κατάσταση, υπήρξε αύξηση της κακόβουλης διαδικτυακής δραστηριότητας στα κράτη μέλη, όπως αποκαλύπτεται από πρόσφατη Έκθεση Europol. Τα θέματα κυβερνοασφάλειας γίνονται καθημερινός αγώνας για την ΕΕ. Σύμφωνα με εκθέσεις παρακολούθησης από τον Οργανισμό της ΕΕ για την Ασφάλεια Πληροφοριών Δικτύων (ENISA), το έγκλημα στον κυβερνοχώρο γίνεται ολοένα και περισσότερο αποτιμημένο σε χρήμα, ιδιαίτερα στην περίπτωση μεγάλων επιθέσεων στον κυβερνοχώρο που χρήση ransomware. Ομοίως, το αυξημένο ηλεκτρονικό εμπόριο και οι πληρωμές χωρίς μετρητά ενέχουν αυξημένους κινδύνους επιθέσεις κυβερνοεγκλήματος και παραβιάσεις της ασφάλειας στον κυβερνοχώρο. Καθώς οι πληρωμές γίνονται όλο και περισσότερο χωρίς μετρητά. Η διαδικτυακή κλοπή –χρημάτων αλλά και προσωπικών δεδομένων– έχει αυξηθεί. Η έκθεση του 2020*

[18] https://www.ertnews.gr/eidiseis/oikonomia/ey-i-tacheia-prosarmogi-stin-tilergasia/?fbclid=IwAR0z7sW4ziCCw7V9aVN7LmXRXcgryqYhIyKJLgFwTyY6RCBwQOzA-Jejhh4

[19] https://electronicanto.net/trends/cyber-security-trends-2022/

αποκαλύπτει ότι οι επιθέσεις στον κυβερνοχώρο γίνονται πιο εξελιγμένες, στοχευμένες, διαδεδομένες και δεν ανιχνεύονται και καταλήγει στο συμπέρασμα ότι οι κοινωνίες έχουν μακρύ δρόμο μπροστά προτού μπορέσουν να εξασφαλίσουν περισσότερο ασφαλές ψηφιακό περιβάλλον. Σύμφωνα με τη Verizon, το 86% των παραβιάσεων που διαπράχθηκαν το 2019 ήταν με οικονομικά κίνητρα και 10% από κατασκοπεία. Περίπου το 45% των παραβιάσεων περιείχε hacking, το 17% περιλάμβανε κακόβουλο λογισμικό και το 22% αφορούσε ηλεκτρονικό ψάρεμα. Η τάση αυτή αναμένεται να αυξηθεί περαιτέρω, παράλληλα με τις τεχνολογικές εξελίξεις όπως ο πολλαπλασιασμός συσκευών που συνδέονται με το Διαδίκτυο των Πραγμάτων (IoT). Σε έναν όλο και πιο συνδεδεμένο κόσμο, όπου αναμένεται να χρησιμοποιούνται 22,3 δισεκατομμύρια συσκευές IoT οι αυξανόμενες προκλήσεις στο τοπίο της κυβερνοασφάλειας οδήγησαν την ΕΕ να σκεφτεί πώς να ενισχύσει την προστασία των πολιτών και των εταιρειών της από κυβερνοαπειλές και επιθέσεις.

Εικόνα 5

Η αποτελεσματική υποχρέωση περισσότερων φορέων και τομέων να λάβουν μέτρα, θα βοηθούσε στην αύξηση του επιπέδου της κυβερνοασφάλειας στην Ευρώπη μακροπρόθεσμα. Στο Ευρωπαϊκό Κοινοβούλιο, ο φάκελος έχει ανατεθεί στην Επιτροπή

Βιομηχανίας, Έρευνας και Ενέργεια. Η επιτροπή ενέκρινε την έκθεσή της στις 28 Οκτωβρίου 2021, καθώς και εντολή εισόδου σε διοργανικές διαπραγματεύσεις.

Το 2017, η Cybersecurity Ventures προέβλεψε αυτό το παγκόσμιο ransomware.Το κόστος ζημιών θα έφθανε τα 20 δισεκατομμύρια δολάρια ΗΠΑ έως το 2021, 57 φορές περισσότερο από το ποσό το 2015 ενώ προέβλεψε ότι οι εταιρείες θα υφίσταντο επίθεση ransomware κάθε 11 δευτερόλεπτα μέχρι το 2021 από κάθε 40 δευτερόλεπτα το 2016. Ως αποτέλεσμα, οι επιχειρήσεις πρέπει να επενδύσουν περισσότερα χρήματα για ένα κυβερνοχώρο ασφαλέστερο για τους ίδιους και τους πελάτες τους καθώς όχι μόνο εταιρείες αλλά και πολίτες και ολόκληρες χώρες έχουν επηρεαστεί.

Η παγκόσμια αγορά ασφάλειας σήμερα αξίζει περίπου 150 δισεκατομμύρια δολάρια, αριθμός που πολλοί προβλέπουν ότι θα ανέλθει σε 208 δισεκατομμύρια δολάρια ΗΠΑ το 2023 και 400 δισεκατομμύρια δολάρια το 2026.

Κρίσιμοι τομείς, όπως οι μεταφορές, η ενέργεια, η υγεία και τα οικονομικά, έχουν γίνει ολοένα και πιο εξαρτημένοι σχετικά με τις ψηφιακές τεχνολογίες για τη λειτουργία της βασικής τους δραστηριότητας. Ενώ η αυξανόμενη ψηφιακή συνδεσιμότητα φέρνει τεράστιες ευκαιρίες, εκθέτει επίσης οικονομίες και κοινωνίες σε κυβερνοαπειλές.

Στις 13 Απριλίου 2021, η Ευρωπαϊκή Επιτροπή παρουσίασε τη νομοθετική πρόταση ενώπιον του Κοινοβουλίου. Οι ευρωβουλευτές χαιρέτησαν την προτεινόμενη αναθεώρηση των NIS. Η πιο κοινή ανησυχία που εγείρεται αφορούσε τη συμβατότητά του με άλλη προτεινόμενη ή υφιστάμενη νομοθεσία της ΕΕ, συμπεριλαμβανομένης της DORA, CER, ο νόμος για την ασφάλεια στον κυβερνοχώρο, η EECC και ο GDPR.

Το σχέδιο έκθεσης της ITRE δημοσιεύθηκε στις 3 Μαΐου 2021 και εγκρίθηκαν οι τέσσερις γνωμοδοτήσεις της επιτροπής τον Ιούλιο 2021. Η επιτροπή ITRE ενέκρινε την έκθεσή της στις 28 Οκτωβρίου 2021, με 70 ψήφους υπέρ 3 κατά, με 1 αποχή. Οι ευρωβουλευτές ψήφισαν επίσης για την έναρξη τριμερών διαπραγματεύσεων με το Συμβούλιο, και αυτό επιβεβαιώθηκε στην ολομέλεια τον Νοέμβριο.

Η έκθεση ζητά αυστηρότερες υποχρεώσεις κυβερνοασφάλειας όσον αφορά τη διαχείριση κινδύνων και την υποβολή εκθέσεων και ανταλλαγή πληροφοριών. Αποσκοπεί στη μείωση του διοικητικού φόρτου και στη βελτίωση. Επιπλέον, η έκθεση αναφέρει ότι οι χώρες της ΕΕ θα πρέπει να συστήσουν αυστηρότερα μέτρα εποπτείας και επιβολής και εναρμόνιση των καθεστώτων κυρώσεων.

Η έκθεση αναφέρει επίσης ότι η Επιτροπή πρέπει να διασφαλίσει ότι παρέχεται η κατάλληλη καθοδήγηση σε όλους σε πολύ μικρές και μικρές επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS2. Η έκθεση υποστηρίζει επίσης
πολιτικές που προωθούν τη χρήση εργαλείων κυβερνοασφάλειας ανοιχτού κώδικα, τα οποία είναι εν μέρει πολιτικές που προωθούν τη χρήση εργαλείων κυβερνοασφάλειας ανοιχτού κώδικα, τα οποία έχουν ιδιαίτερη σημασία για τις ΜΜΕ, καθώς αντιμετωπίζουν σημαντικό κόστος για την εφαρμογή εργαλείων κυβερνοασφάλειας.
Μεταξύ άλλων, ο εισηγητής πρόσθεσε την έννοια της «ενεργητικής άμυνας» στο σχέδιο έκθεσης του αναφέρει ότι τα κράτη μέλη πρέπει να υιοθετήσουν πολιτικές για την προώθηση της ενεργού κυβερνο-άμυνας ως μέρος των εθνικών τους στρατηγικών κυβερνοασφάλειας.
Η έκθεση σκοπεύει να διευρύνει το τομεακό πεδίο εφαρμογής, ώστε να συμπεριλάβει επίσης την ακαδημαϊκή, τη γνώση και την έρευνα για ιδρύματα που είχαν αφεθεί εκτός του πεδίου εφαρμογής των NIS2 από την Επιτροπή.
Τα περισσότερα κράτη μέλη δήλωσαν ότι ήταν επιτακτική ανάγκη να θεωρηθεί το NIS2 ως το οριζόντιο πλαίσιο κυβερνοασφάλειας στην ΕΕ και ότι θα πρέπει να χρησιμεύσει ως βασικό πρότυπο για την ελάχιστη εναρμόνιση όλης της σχετικής τομεακής νομοθεσίας στον τομέα αυτό. Άλλες ανησυχίες που διατυπώθηκαν σχετίζονται με τη σημαντική διεύρυνση του πεδίου εφαρμογής των αναθεωρημένων κανόνων, τα κριτήρια ανώτατου ορίου μεγέθους ως το μοναδικό στοιχείο που πρέπει να ληφθεί υπόψη κατά τον προσδιορισμό βασικών και σημαντικών οντοτήτων που πρέπει να καλυφθούν, η προτεινόμενη νομική βάση (δηλαδή ενιαία αγορά) και ανησυχίες για την εθνική ασφάλεια»[20].[21]

Στην Ελλάδα η έξαρση της πανδημίας στάθηκε η αφορμή για να εξελιχθεί η ηλεκτρονική διακυβέρνηση και να δημιουργηθούν νέες ψηφιακές υπηρεσίες όπως η νέα ενιαία Πύλη της Δημόσιας Διοίκησης gov.gr, το μητρώο ασθενών COVID-19, η διαδικτυακή πλατφόρμα για το εμβόλιο κατά της COVID-19 (emvolio.gov.gr), η δήλωση αυτοδιαγνωστικών τεστ COVID-19 - self tests

[20] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[21] https://www.europarl.europa.eu/news/el/headlines/society/20220120STO21428/kuvernoasfaleia-oi-megaluteres-apeiles-gia-to-2021-grafima#missinglink

(self-testing.gov.gr), το egka.gov.gr για ραντεβού με τον φορέα και στην συνέχεια για ηλεκτρονικές υπηρεσίες εξυπηρέτησης των ασφαλισμένων ενώ ταυτόχρονα δρομολογήθηκαν δράσεις για την τηλεσυμβουλευτική και τον Ατομικό Ηλεκτρονικό Φάκελο Υγείας (ΑΗΦΥ),[22]

Η εξέλιξη και βελτίωση των ηλεκτρονικών συναλλαγών στον δημόσιο τομέα απαιτεί και ενίσχυση της Κυβερνοασφάλειας όπως αναφέρει και ο Υπουργός Επικρατείας και Ψηφιακής Διακυβέρνησης Κος Πιερρακάκης αναφερόμενος στον Ευρωπαικό Οργανισμό Κυβερνοασφάλειας ο οποίος πλέον έχει την έδρα του στην Αθήνα[23] «*Όσο ψηφιοποιούμε το κράτος εκ των πραγμάτων, το βλέμμα στρέφεται στην ενίσχυση της κυβερνοαφάλειας. Η αλλαγή στην κυβερνοασφάλεια δεν χρειάζεται μόνο τεχνολογική αλλαγή αλλά και αλλαγή στην κουλτούρα. Είναι τιμή μας που ο ENISA βρίσκεται στη χώρα μας αλλά είναι σημαντικό να γίνουμε εκτός από χώρα που φιλοξενεί τον Οργανισμό και χώρα που τον αξιοποιεί*»[24].

Ο ENISA είναι ο Ευρωπαϊκός Οργανισμός που χαράσσει την πολιτική ασφαλείας που θα πρέπει να εφαρμόσουν τα κράτη μέλη της ΕΕ, συνεργάζεται με τα κράτη μέλη για ανταλλαγή απόψεων, για την ανάπτυξη των ικανοτήτων, για αντιμετώπιση των κινδύνων[25].

Επίσης το Υπουργείο Ψηφιακής Διακυβέρνησης σε μία προσπάθεια ενίσχυσης της Κυβερνοασφάλειας εξέδωσε εγχειρίδιο κυβερνοασφάλειας με τις βέλτιστες πρακτικές για την προστασία και ανθεκτικότητα των πληροφοριακών συστημάτων.

Το εγχειρίδιο χωρίζεται σε 2 μέρη:το πρώτο μέρος περιλαμβάνει αρχιτεκτονικές ασφαλείας για τα σύγχρονα πληροφοριακά συστήματα και βασικά βήματα διαχείρισης ασφαλείας με βάση το βαθμό του κινδύνου και το δεύτερο μέρος αναπτύσσει βέλτιστες πρακτικές σε τεχνικά και οργανωτικά μέτρα προστασίας.

Ενδεικτικά αναφέρουμε: Περιορισμοί πρόσβασης (need-to-know κ.α), ασφάλεια δικτύων με τμηματοποίηση δικτύων, firewall, VPN κ.α , προστασία συσκευών με antivarious, application whitelisting κ.α., προστασία εφαρμογών και δεδομένων με

[22] https://www.dianeosis.org/wp-content/uploads/2021/09/e-gov_policy-paper.pdf

[23] https://www.ethnos.gr/technology/article/166472/enisahkardiathskybernoasfaleiasthseyrophsxtypasthnellada

[24] https://www.fpress.gr/ellada/story/86189/egkainiasthike-i-edra-toy-enisa-stin-athina

[25] https://www.enisa.europa.eu/about-enisa/about/el

κρυπτογράφηση κ.α., αξιολόγηση κινδύνου, ορισμός υπευθύνου ασφαλείας πληροφοριακών συστημάτων[26].

Συγχρόνως το Υπουργείο διοργανώνει εκστρατεία ευαισθητοποίησης για την κυβερνοασφάλεια, προκειμένου να ενημερώσει τους πολίτες και να προωθήσει με οδηγίες και κατευθυντήριες πληροφορίες[27].

Τα δεδομένα από το **Microsoft Security Intelligence Report** πιστοποιούν ότι η Ελλάδα βρίσκεται στη **13η θέση** της κατάταξης 32 χωρών της Ευρώπης που είναι πιο πιθανό να πληγούν από ποικίλες κυβερνοαπειλές.[28][29]

ΚΕΦΑΛΑΙΟ 2ο

Ο ΣΗΜΑΝΤΙΚΟΣ ΡΟΛΟΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΤΠΕ) ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ (eGoverment) ΚΑΙ Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΩΣ ΑΝΑΓΚΑΙΑ ΣΥΝΘΗΚΗ

«Στον 21ο αιώνα η πληροφορική αναδύεται ως θεμελιώδης τεχνολογία των επιχειρήσεων. Όπως ακριβώς η ενέργεια ήταν η κινητήρια δύναμη στην βιομηχανική κοινωνία έτσι και η πληροφορία είναι η βασική πηγή μεταμόρφωσης στις νέες κοινωνικές και οικονομικές σχέσεις»[30].

2.1.Ορισμοί και Βασικά Χαρακτηριστικά

2.1.1.*Ορισμός των Τεχνολογιών της Πληροφορίας και των Επικοινωνιών (ΤΠΕ)*

[26] https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf?fbclid=IwAR0JDJGj5D5H6-DfmMqsc_Sw2x4bVGXrhaaHdlhzYfldW8FqQUiQaN1EUDA

[27] https://www.enisa.europa.eu/news/ecsm-2021-pr/cnect-2021-00359-02-00-el-tra-00.pdf?fbclid=IwAR2_-QUwGISf0foyQnvkl4_3fzVziQYTtuG6oMzE_I0S7UCzPNm5u7y9U68

[28] https://www.fortunegreece.com/article/i-evropaikes-chores-me-ti-megaliteri-kivernoasfalia-i-thesi-tis-elladas/

[29] https://www.kathimerini.gr/economy/561723097/pempti-pagkosmios-i-ellada-stis-psifiakes-epitheseis-phishing/

[30] Δουκίδης Γ. (2011) Καινοτομία Στρατηγική Ανάπτυξη και Πληροφοριακά Συστήματα Εκδόσεις Σιδέρη, Αθήνα

Μέσω δικτύων και κατάλληλων λογισμικών εγκατεστημένων σε υπολογιστές, τηλέφωνα ή άλλες συσκευές εξυπηρετείται ένα ευρύ φάσμα υπηρεσιών πληροφόρησης (συλλογή, επεξεργασία και μετάδοση πληροφοριών) σε διάφορους τομείς. Τα πληροφοριακά συστήματα (που είναι οι εφαρμογές των ΤΠΤ στους οργανισμούς) εξυπηρετούν την αυτοματοποίηση και απλοποίηση των συναλλαγών.

2.1.2 *Βασικές 'Εννοιες Πληροφοριακών συστημάτων*

«***Πληροφοριακό Σύστημα:*** *Ως Πληροφοριακό Σύστημα ορίζεται ένα σύστημα το οποίο αποτελείται από ανθρώπους, διαδικασίες και μηχανές (διάφορα στοιχεία υλικού και λογισμικού) και έχει ως στόχο την συλλογή αποθήκευση, επεξεργασία και διανομή για την υποστήριξη των διαφόρων λειτουργιών του δημόσιου οργανισμού.*

Βασικές Συνιστώσες:

'Ανθρωποι: διοικητικοί υπάλληλοι διαφόρων ιεραρχικών επιπέδων και καθηκόντων οι οποίοι ασχολούνται με την συλλογή, αποθήκευση επεξεργασία και διανομή πληροφοριών και στα πλαίσια αυτών των εργασιών χρησιμοποιούν το ΠΣ ως εργαλείο.Επίσης εξειδικευμένο προσωπικό ΤΠΕ το οποίο ασχολείται με την υποστήριξη της ομαλής λειτουργίας και την διαχείριση των ΠΣ.

Διαδικασίες: Χρησιμοποιούνται από τους ανωτέρω άλλες φορές χειρόγραφα και άλλες φορές ηλεκτρονικά

Υλικό (hardware): Σύνολο από σταθμούς εργασίας (PC, κεντρικούς υπολογιστές), εξυπηρετητές (servers), βάσεις δεδομένων, εκτυπωτές, scanners κλπ

Λογισμικό (software): Κάθε υπολογιστής ενός ΠΣ διαθέτει λογισμικό δηλαδή ένα σύνολο προγραμμάτων το οποίο είναι οργανωμένο σε επίπεδα (layers) λειτουργικό σύστημα, σύστημα βάσης δεδομένων (ΣΔΒΔ), λογισμικό εφαρμογών (π.χ.δημιουργίας κειμένων, μισθοδοσίας, κ.λπ.)

Δικτυακές Διασυνδέσεις (networks): *ένα ΠΣ γενικά περιλαμβάνει ένα αριθμό τοπικών δικτύων (LAN) τα οποία διασυνδέουν υπολογιστές που βρίσκονται σε μικρή απόσταση μεταξύ τους καθώς επίσης και έναν αριθμό δικτύων ευρείας περιοχής (WAN)*

Δεδομένα – Πληροφορίες: *Τα δεδομένα (data) ενός ΠΣ ορίζονται τα διάφορα αναλυτικά πρωτογενή στοιχεία που εισάγονται σε αυτό ενώ πληροφορίες (information) ορίζονται τα αναλυτικά δεδομένα τα οποία έχουν υποστεί επεξεργασία*

Πληροφοριακές Ροές*: Σε κάθε δημόσιο οργανισμό εισρέουν πληθώρα πληροφοριών από το εξωτερικό περιβάλλον π.χ.πολίτες, επιχειρήσεις, συλλογικά όργανα κλπ., από τους βασικούς προμηθευτές π.χ. αγορά υλικών, από άλλους δημόσιους οργανισμούς, εσωτερικού και εξωτερικού, αλλά και μεταξύ των διαφόρων οργανωτικών μονάδων με στόχο την ανάδραση και το συντονισμό μεταξύ τους. Για την υλοποίηση των λειτουργιών ενός δημοσίου οργανισμού πραγματοποιούνται εκτενείς τόσο θεσμοθετημένες όσο και άτυπες πληροφοριακές ροές οι οποίες είναι ζωτικής σημασίας.*

Λειτουργική Δομή Πληροφοριακού Συστήματος : *Ορίζεται το σύνολο των δυνατοτήτων που παρέχει στους διάφορους χρήστες του. Οι δυνατότητες αυτές υποβοηθούν τους χρήστες για να εκτελέσουν κάποιες λειτουργίες σχεδιασμού υλοποίησης, διοικητικής υποστήριξης κ.λ.π. καθώς επίσης και για να λάβουν αποφάσεις. Οι προαναφερόμενες δυνατότητες ενός ΠΣ είναι οργανωμένες με την μορφή ενός αριθμού «Υποσυστημάτων» κάθε ένα από τα οποία παρέχει ένα σύνολο συναφών δυνατοτήτων που συνήθως αφορούν την υποστήριξη της εκτέλεσης κάποιας βασικής λειτουργίας του δημοσίου οργανισμού π.χ. το ΠΣ ενός ασφαλιστικού ταμείου γενικά περιλαμβάνει κάποια υποσυστήματα όπως Υποσύστημα Εσόδων, Υποσύστημα συντάξεων κ.λ.π..*

Τεχνολογική Δομή Πληροφοριακού Συστήματος

Η τεχνολογική δομή ορίζεται ως η διασύνδεση μεταξύ των συνιστωσών υλικού, λογιστικού και διασυνδέσεων»[31]

Τα πληροφορικά συστήματα προσφέρουν δυνατότητες άμεσης και ανέξοδης επικοινωνίας μεταξύ οργανισμών και πολιτών σε οποιοδήποτε χρόνο και τόπο μέσω email, παρέχουν ανταλλαγή και πρόσβαση σε τεράστιο όγκο πληροφοριών μέσω πλατφόρμας όπως e-efka.gov.gr, διευκολύνουν και αυτοματοποιούν γραφειοκρατικές διαδικασίες π.χ.για κατάθεση συνταξιοδοτικών αιτήσεων, δίνουν δυνατότητα

[31] Αποστολάκης Ι., Λουκής Ε., Χάλαρης Ι. (2008) Ηλεκτρονική Δημόσια Διοίκηση Εκδόσεις Παπαζήση Αθήνα

αποθήκευσης και ταξινόμησης πληθώρας πληροφοριών στα πληροφοριακά συστήματα των δημοσίων υπηρεσιών όπως μητρώα πολιτών κλπ, εκτελούν αυτόματα αριθμητικούς υπολογισμούς π.χ. για υπολογισμός ασφαλιστικών εισφορών και γενικά αυξάνουν την ταχύτητα και την αποτελεσματικότητα των υφιστάμενων διαδικασιών αφού δρούν σε πραγματικό χρόνο.

Για να είναι όμως αποτελεσματικά τα πληροφοριακά συστήματα θα πρέπει να εφαρμόζονται κάποιοι παράμετροι ήτοι ο σχεδιασμός τους να πραγματοποιείται σε αντιστοιχία με τον επιχειρησιακό σχεδιασμό του οργανισμού ή να ελέγχεται ο ανασχεδιασμός τους εάν προϋπάρχουν. Στην συνέχεια σε τακτά διαστήματα επιβάλλεται να αξιολογούνται και να επανασχεδιάζονται προκειμένου να επιτευχθεί ο στόχος της επιτυχούς χρήσης τους στο οργανισμό.

Για την αξιολόγησή τους χρησιμοποιούνται τεχνικές που σχετίζονται με τα στάδια ανάπτυξής τους: Αρχικά εξοπλίζουμε τους οργανισμούς και αυτοματοποιούμε τις απλές λειτουργίες για μείωση του λειτουργικού κόστους και στην πορεία ενισχύουμε τα πληροφοριακά συστήματα με περισσότερες on line εφαρμογές ικανοποιώντας τις προσδοκίες για την αποτελεσματικότητά τους.

Η ανάπτυξη προτύπων και μεθοδολογιών και η πλήρης εφαρμογή και αξιολόγηση των δυνατοτήτων των ΠΣ μας παρέχει ολοκληρωμένα πληροφοριακά συστήματα. Στην συνέχεια καθώς η απλή επεξεργασία των δεδομένων γίνεται πλέον αξιοποίηση πληροφορίας και διαχείριση δεδομένων επενδύουμε στην ενοποίηση των υπαρχόντων συστημάτων μέσω τηλεπικοινωνιών και βάσεων δεδομένων και αλλάζει η πληροφοριακή μας προσέγγιση, εξελίσσεται.

Η πληροφορική είναι πλέον ο στρατηγικός σύμμαχος κάθε οργανισμού και το πληροφοριακό του σύστημα αποτελεί την σημαντικότερη υποδομή λειτουργίας του .

Η επιτυχία ή η αποτυχία ενός ΠΣ εξαρτάται από την δομή του, την εναρμόνισή του με το οργανωσιακό σχέδιο του οργανισμού καθώς και την συνεχή εξέλιξή του.

Αναφέρουμε ενδεικτικά κάποιες απαραίτητες ενέργειες για την επίτευξη του στόχου:

- Συνεχής κατάρτιση των χρηστών προκειμένου να αποκτήσουν τις απαραίτητες δεξιότητες διαχείρισης των ΠΣ,

- Συμμετοχή των χρηστών στο σχεδιασμό και την ανάπτυξη του ΠΣ καθώς θα υπάρξει αλληλεπίδραση μεταξύ τους.
- Υποστήριξη και διάθεση από την διοίκηση των απαραίτητων πόρων για πλήρως ολοκληρωμένα ΠΣ, νέα συστήματα και διαχείριση των διαδικασιών αλλαγής.

‘Εάν παρόλα αυτά διακρίνουμε χαμηλή χρηστικότητα στα ΠΣ, χαμηλή ποιότητα συστήματος και δεδομένων, χαμηλή ποιότητα παρεχόμενων πληροφοριών και πληθώρα λειτουργικών προβλημάτων τότε ενδέχεται να υπάρχουν μεγάλες αποκλίσεις σε χρονοδιαγράμματα και κόστη και απαιτείται επαναξιολόγηση του σχεδιασμού.

Σε περίπτωση που δεν υπάρχει ιδία δυνατότητα του οργανισμού για βελτίωση μία εναλλακτική επιλογή για την απόκτηση ΠΣ είναι η αγορά ΠΣ και υπηρεσιών από τρίτους παρόχους. Αυτό σημαίνει ότι ο οργανισμός αναθέτει σε τρίτους (outsourcing) εξ ολοκλήρου την ανάπτυξη κάποιων λειτουργιών των ΠΣ ή την εκτέλεση μιας οργανωσιακής λειτουργίας ή μιας διεργασίας π.χ.ανάθεση του Ολοκληρωμένου Πληροφοριακού Συστήματος του τ.ΙΚΑ εξ ολοκλήρου στην Intracom (ανάδοχος).
Αυτή η επιλογή απαιτεί όρους και αυστηρές συμβάσεις με προϋποθέσεις προκειμένου να προστατευθούν τα μακροπρόθεσμα συμφέροντα του οργανισμού και να θεωρείται επιτυχημένη η ανάθεση. Επειδή μία μακροπρόθεσμη συμφωνία επηρεάζει τις λειτουργίες του οργανισμού η σύμβαση της εξωτερικής ανάθεσης θα πρέπει να πραγματοποιηθεί μετά από ενδελεχή νομικό έλεγχο και να δύναται η ανάκληση σε ενδεχόμενη αθέτηση συμφωνίας.

Επίσης με ταχύς ρυθμούς αναπτύσσονται και οι υπηρεσίες του «υπολογιστικού νέφους» ή cloud computing.Το cloud που βρίσκεται σε μία διαρκή εξελικτική πορεία δίνει την δυνατότητα στους οργανισμούς να αγοράσουν παροχές υπηρεσιών αποθηκευτικών χώρων, βάσεων δεδομένων, λογισμικού κ.λ.π. μέσω διαδικτύου. Αυτό πρακτικά σημαίνει μείωση κόστους για υλικοτεχνική υποδομή, αύξηση ταχύτητας, απόδοσης και αξιοπιστίας αφού οι παροχές προέρχονται από μία καλά οργανωμένη εταιρεία η οποία χρεώνει αντίστοιχα τις υπηρεσίες της με τρόπο παρόμοιο με την χρέωση της ηλεκτρικής ενέργειας[32] πχ.corpmail.

[32] https://www.csc.com.gr/cloud-computing/

2.1.3 *Διαλειτουργικότητα*

Επικοινωνία και διεπαφή πληροφοριακών συστημάτων (ίδιων στον ίδιο οργανισμό ή διαφορετικών και σε διαφορετικούς οργανισμούς) για συνεργασία και ανταλλαγή πληροφοριών και καλύτερη οργανωτική απόδοση. Η διαλειτουργικότητα εξυπηρετεί την διασύνδεση για διαμοιρασμό της πληροφορίας με αποτέλεσμα την βελτίωση της αποτελεσματικότητας. Τα λειτουργικά συστήματα σπάνια λειτουργούν από μόνα τους, συνήθως υποστηρίζονται οι λειτουργίες τους. Η επίτευξη της διαλειτουργικότητας των πληροφοριακών συστημάτων στην δημόσια διοίκηση είναι ένα δύσκολο, αλλά πολύ σημαντικό εγχείρημα, το οποίο θα στηρίξει ουσιαστικά τις συναλλαγές με τους πολίτες και θα εξυπηρετήσει στο έπαρκο τον θεσμικό ρόλο των υπηρεσιών.

Στην Ελλάδα η προσπάθεια για δημιουργία πλαισίου διαλειτουργικότητας βρίσκεται σε διαρκή μετασχηματισμό καθώς αντιμετωπίζει εμπόδια και προβλήματα που σχετίζονται με τις ελλιπής υποδομές και τις καθυστερήσεις του παρελθόντος.

«Τα *υπάρχοντα πληροφοριακά συστήματα στην ελληνική δημόσια διοίκηση έχουν υλοποιηθεί σε διάφορα περιβάλλοντα προγραμματισμού και παρουσιάζουν αυξημένη τεχνολογική και αρχιτεκτονική ανομοιογένεια μεταξύ τους ενώ σε μερικές περιπτώσεις χρησιμοποιούν ξεπερασμένες πλατφόρμες και απαρχαιωμένες τεχνολογίες. Χρησιμοποιούν διαφορετικά λειτουργικά συστήματα και διαφορετικά κατά περίπτωση συστήματα διαχείρισης βάσεως δεδομένων. Επί πρόσθετα οι διαφοροποιημένες ανάγκες του κάθε οργανισμού καθιστούν αυτά τα πληροφοριακά συστήματά τους ακόμα περισσότερα ανομοιογενή από λειτουργικής άποψης, παρά το γεγονός ότι ακολουθούν ενιαίο θεσμικό και λειτουργικό πλαίσιο για την υποστήριξη των διαδικασιών που αυτοματοποιούν»*[33]

Η δύσκολη επίτευξη της διασύνδεσης των ΠΣ σε εθνικό και σε ευρωπαικό επίπεδο οφείλεται αφ’ενός στις σύνθετες νομικές διαδικασίες και αφ’ετέρου στις τεχνικές διαδικασίες.

---

[33] Αποστολάκης Ι., Λουκής Ε., Χάλαρης Ι. (2008) Ηλεκτρονική Δημόσια Διοίκηση Εκδόσεις Παπαζήση Αθήνα

‘Οσον αφορά το νομικό επίπεδο η απουσία ενιαίου νομοθετικού πλαισίου ανάμεσα στους φορείς καθιστά μη εφικτό τον διαμοιρασμό και την επεξεργασία της πληροφορίας. Συγχρόνως επιβάλλεται να εξασφαλίζεται η προστασία και η ασφάλεια των προσωπικών δεδομένων καθώς η μεταφορά, επεξεργασία και χρήση των δεδομένων ενέχει κινδύνους διαρροής και εκμετάλλευσης από τις κυβερνοαπειλές στο διαδίκτυο.

Ταυτόχρονα η υλοποίηση της διαλειτουργικότητας ανάμεσα σε ΠΣ προϋποθέτει και τις κάτωθι διαδικασίες:

Οργανωσιακή διαλειτουργικότητα

Αυτό σημαίνει ότι τα συνεργαζόμενα πληροφοριακά συστήματα θα πρέπει να διαθέτουν ίδιες διαδικασίες, ίδιες οργανωτικές δομές για να αναγνωρίζονται και να υπάρχει επικοινωνία μεταξύ τους. Επίσης να διαθέτουν κοινό επίπεδο διεπαφών και κοινά επίπεδα ασφάλειας.

Σημασιολογική διαλειτουργικότητα

Αυτό σημαίνει ότι η συνεργασία ανάμεσα στα πληροφοριακά συστήματα θα γίνεται με όρους ίδιας σημασίας, η ανταλλαγή πληροφοριών είναι εφικτή όταν η πληροφορία είναι κατανοητή εκατέρωθεν, όταν υπάρχει κοινή γλώσσα επικοινωνίας και κοινές έννοιες.

Τεχνολογική Διαλειτουργικότητα

Η τεχνολογική διαλειτουργικότητα θα πρέπει να υποστηρίζει το front office και το back office δηλαδή τις βασικές αρχές σχεδίασης των διεπαφών, την παρουσίαση και ανταλλαγή δεδομένων, τον τύπο αρχείων, την ενοποίηση δεδομένων, υπηρεσίες διασύνδεσης και δικτύου, υπηρεσίες αποθήκευσης δικτύου κλπ.

Εν τω μεταξύ η Ευρωπαική ‘Ενωση προκειμένου να εξασφαλίσει την διαλειτουργικότητα των πληροφοριακών συστημάτων ανάμεσα στις χώρες της Ευρωπαικής ‘Ενωσης έχει επιβάλλει δράσεις που εντάσσονται στο Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας.

«*Για τους παραπάνω λόγους πολλές χώρες (π.χ.Μ.Βρετανία, Γαλλία, Γερμανία, ΗΠΑ κ.λ.π.αλλά και η Ευρωπαική ‘Ενωση) έχουν αναπτύξει και έχουν θέσει σε εφαρμογή*

«Πλαίσια Διαλειτουργικότητας», ορισμένα ως σύνολα προτύπων και οδηγιών, τα οποία περιγράφουν τον τρόπο με τον οποίο τα πληροφοριακά συστήματα διαφορετικών οργανισμών θα αλληλεπιδρούν και θα συνεργάζονται .

Σε αρκετές περιπτώσεις μία υπηρεσία ηλεκτρονικής δημόσιας διοίκησης, την οποία χρησιμοποιεί ένας πολίτης σε ένα κράτος-μέλος της Ε.Ε. καθιστά αναγκαία την πρόσβαση σε πληροφοριακά συστήματα πολλών δημοσίων οργανισμών, είτε από το ίδιο κράτος είτε από άλλα κράτη-μέλη. Παραδείγματος χάριν, μία ηλεκτρονική αίτηση για συνταξιοδότηση που υποβάλλεται από κάποιον πολίτη σε ένα κράτος –μέλος μπορεί να καθιστά αναγκαία την πρόσβαση σε πληροφοριακά συστήματα διάφορων ασφαλιστικών οργανισμών τόσο στο συγκεκριμένο κράτος-μέλος με στόχο την άντληση δεδομένων σχετικά με τους χρόνους απασχόλησης του πολίτη σε διάφορες προηγούμενες φάσεις της επαγγελματικής του διαδρομής, τις ασφαλιστικές εισφορές που έχει πληρώσει κλπ. Τα παραπάνω καθιστούν αναγκαία τη διαλειτουργικότητα μεταξύ των πληροφοριακών συστημάτων και την ομοιογένεια των δεδομένων που αντλούνται από αυτά. Επισημαίνεται όμως ότι αυτή η ανταλλαγή πληροφοριών γίνεται με βάση σαφείς κανόνες ώστε να διασφαλίζεται η καλή και επωφελής για την κοινωνία χρήση των πληροφοριών αυτών καθώς επίσης και η προστασία των προσωπικών δεδομένων.
Μία άλλη πτυχή της διαλειτουργικότητας αποτελεί το ζήτημα της ασφάλειας και τη παροχής απονομής ψηφιακών πιστοποιητικών. Σύμφωνα με το Π.Δ.150/2001 «Προσαρμογή στην Οδηγία 99/96/ΕΚ του Ευρωπαικού Κανονισμού και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές», ορίζεται η ΕΕΤΤ ως η αρμόδια αρχή για τον έλεγχο και την εποπτεία των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής καθώς επίσης και για την διαπίστωση της συμμόρφωσής τους προς της διατάξεις δημιουργίας ασφαλούς υπογραφής » [34] .

Η σημαντικότητα λοιπόν της διαλειτουργικότητας και της ανάδρασης μεταξύ των πληροφοριακών συστημάτων στην ίδια υπηρεσία αλλά και ανάμεσα στους φορείς είναι αδιαμφισβήτητη και αναγκαία για την ποιότητα των υπηρεσιών του δημοσίου τομέα.

[34] Αποστολάκης Ι., Λουκής Ε., Χάλαρης Ι. (2008) Ηλεκτρονική Δημόσια Διοίκηση Εκδόσεις Παπαζήση Αθήνα

2.1.4 *Ηλεκτρονική διακυβέρνηση (e Government)*

Ηλεκτρονική Διακυβέρνηση είναι ο τρόπος ή η μέθοδος που μπορούμε να χρησιμοποιήσουμε τους υπολογιστές για να κάνουμε την ζωή μας καλύτερη.

Ηλεκτρονική Διακυβέρνηση είναι ο τρόπος ή η μέθοδος που μπορούμε να χρησιμοποιήσουμε τους υπολογιστές για να κάνουμε την ζωή μας καλύτερη.

Η ηλεκτρονική διακυβέρνηση προωθεί τον εκσυγχρονισμό του κράτους χρησιμοποιώντας τις νέες τεχνολογίες της επιστήμης των υπολογιστών αλλά και της διοικητικής επιστήμης. Ο συγχρονισμός και η σύμπλευση των επιστημών θα βοηθήσουν προς την σωστή κατεύθυνση.

‘Όμως σε αυτό το εγχείρημα δεν αρκούν μόνο οι πρωτοβουλίες του κράτους απαιτείται εγρήγορση και αντανακλαστικά και από την κοινωνία. Οι επιρροές της εξέλιξης μας αφορούν όλους και οι προσπάθειες που καταβάλλει το κράτος για αλλαγές και αναβάθμιση θα πρέπει «βρούν» ανταπόκριση και συνεργασία από τους πολίτες. Σε διαφορετική περίπτωση δεν θα μπορέσει να ολοκληρωθεί η προσπάθεια για διεύρυνση των ΤΠΕ και για υλοποίηση των προγραμματισμένων σχεδιασμών.

Επειδή ο μετασχηματισμός της παραδοσιακής δημόσιας διοίκησης σε ηλεκτρονική δημόσια διοίκηση δεν μετασχηματίζει συγχρόνως και την κουλτούρα και την λανθασμένη νοοτροπία των πολιτών απαιτείται χρόνος προσαρμογής στις αλλαγές και στα νέα δεδομένα. Σε αυτό θα βοηθούσε η ενημέρωση, η εκπαίδευση σε νέες δεξιότητες, η συμμετοχή στις νέες μορφές οργάνωσης, η συνεργασία με τον ιδιωτικό τομέα που θα μπορούσε να θεωρηθεί σύμμαχος και αρωγός στις αλλαγές. Είναι αξιοσημείωτο ότι ο ιδιωτικός τομέας ως πιο απαιτητικός δημιουργεί και προετοιμάζει τις αλλαγές καθώς δέχεται πιέσεις από την παγκοσμιοποίηση και τις κλίμακες οικονομίας που αναπτύσσονται.

Επιτυχημένη ηλεκτρονική διακυβέρνηση σημαίνει ότι το κράτος φροντίζει για τον πολίτη πριν το χρειαστεί ο ίδιος ο πολίτης, σημαίνει ότι ο πολίτης εξυπηρετείται ηλεκτρονικά μέσω διαδικτύου χωρίς φυσική του παρουσία στις υπηρεσίες, χωρίς γραφειοκρατία και περιττές διαδικασίες. Ως χαρακτηριστικό παράδειγμα θα μπορούσαμε να αναφέρουμε την αίτηση και το δικαίωμα συνταξιοδότησης που ταλαιπωρεί τους πολίτες ενώ θα μπορούσε να απονέμεται αυτεπάγγελτα από το ίδιο κράτος μετά τον έλεγχο των προϋποθέσεων όπως συμβαίνει σε άλλες χώρες της Ευρωπαικής ‘Ενωσης, Εσθονία, Δανία, Αυστρία, Σουηδία που βρίσκονται στα υψηλότερα επίπεδα του δείκτη DESI. Οι χώρες αυτές έχουν καταφέρει να

εφαρμόσουν την τεχνογνωσία τους με τρόπο αποτελεσματικό, αποδοτικό και επιτυχημένο.

Για να αντιμετωπίσει η χώρα μας αυτή την πρόκληση-πρόσκληση για εξέλιξη και άμεση πρόοδο θα πρέπει να χρησιμοποιήσει οργανωμένα και με βέλτιστο τρόπο την αλματώδη ανάπτυξη της ΤΠΕ, τις απεριόριστες δυνατότητες των πληροφοριακών συστημάτων όπως αναφέρονται ανωτέρω μέσω της διαλειτουργικότητάς τους και να ενισχύσει την πολιτική ασφαλείας τους. Η δυσαρέσκεια και το χαμηλό επίπεδο ικανοποίησης των πολιτών δημιουργεί την αναγκαιότητα των άμεσων και ορθά μεθοδευμένων εξελίξεων.

Η υλοποίηση βέλτιστης ηλεκτρονικής δημόσιας διοίκησης δύναται να πραγματοποιηθεί μέσα από μία σειρά πολυάριθμων διαδικασιών και δράσεων.

Αναφέρουμε ενδεικτικά τις πιο σημαντικές:

- ◊ Υποστήριξη από την Διοίκηση του κάθε οργανισμού των εσωτερικών διαδικασιών και του υπαρχουσών πληροφοριακών συστημάτων,
- ◊ Απαραίτητη διασύνδεση μεταξύ των πληροφοριακών συστημάτων του κάθε φορέα ή και μεταξύ διαφορετικών δημοσίων οργανισμών,
- ◊ Εκπαίδευση δημοσίων υπαλλήλων σε ουσιαστικές γνώσεις και δεξιότητες σε σχέση με το αντικείμενο που εξυπηρετούν
- ◊ Επαναξιολόγηση και αντικειμενικά κριτήρια στις θέσεις ευθύνης
- ◊ Πλήρη εφαρμογή πολιτικής ασφαλείας στα ΠΣ
- ◊ Διαρκή συνεργασία διοίκησης με υπαλλήλους
- ◊ Πολλαπλά κανάλια επικοινωνίας και κεντρικός συντονισμός

Η εύστοχη και επιτυχημένη ηλεκτρονική διακυβέρνηση μπορεί να προσφέρει πολλαπλά οφέλη στον πολίτη όπως:

- o Ποιότητα εξυπηρέτησης
- o Αξιοπιστία στις πληροφορίες και στις διαδικασίες,
- o Εξοικονόμηση χρόνου
- o Άμεση απάντηση και ενημέρωση
- o ‘Αμεσες πληρωμές μέσω τράπεζας
- o Ισότιμη πρόσβαση στην δημόσια διοίκηση
- o Πληρέστερη πληροφόρηση
- o Διαφάνεια και έλεγχος στις υπηρεσίες του

- Δημοκρατική συμμετοχή στην διαμόρφωση δημόσιων πολιτικών

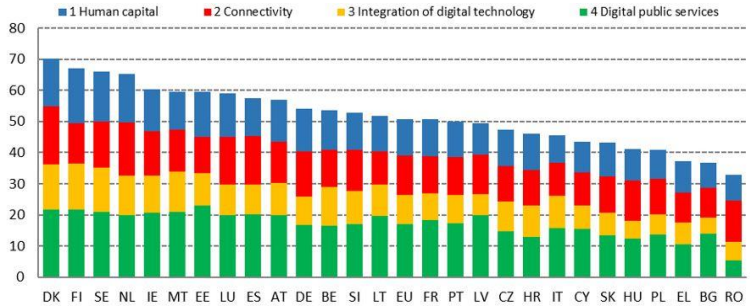
Αλλά ταυτόχρονα να ωφελήσει και το δημόσιο αφού:

- Απλοποιούνται και εκσυγχρονίζονται διαδικασίες
- Αυξάνεται η αποδοτικότητα των υπαλλήλων
- Μειώνεται το λειτουργικό κόστος και εξοικονομούνται πόροι
- Μειώνεται ο χρόνος για περιττές διαδικασίες
- 'Αμεση ενημέρωση για κατανόηση και υλοποίηση νόμων

Συμπερασματικά οι τεχνολογικές εξελίξεις υποχρεώνουν για επαναστατικά βήματα, για δράσεις που η πληροφορική δεν θα έχει διεκπεραιωτικό ρόλο αλλά καταλυτικό[35].

2.1.5 *Ψηφιακές δημόσιες υπηρεσίες στην Ευρωπαική 'Ενωση-Θέση της Ελλάδας*

«Η Ψηφιακή πυξίδα θέτει τον στόχο όλες οι βασικές δημόσιες υπηρεσίες για τους πολίτες και τις επιχειρήσεις να είναι πλήρως διαδικτυακές έως το 2030. Ο DESI παρακολουθεί τη διαδικτυακή παροχή δημόσιων υπηρεσιών βαθμολογώντας κάθε κράτος μέλος ανάλογα με το κατά πόσον είναι δυνατό να ολοκληρωθεί το κάθε στάδιο των βασικών υπηρεσιών εντελώς διαδικτυακά. Η Εσθονία, η Δανία, η Φινλανδία και η Μάλτα έχουν την υψηλότερη βαθμολογία στον DESI όσον αφορά τις ψηφιακές δημόσιες υπηρεσίες, ενώ η Ρουμανία και η Ελλάδα έχουν τη χαμηλότερη.Το 2020, το 64 % των χρηστών του διαδικτύου επικοινώνησαν με τη δημόσια διοίκηση διαδικτυακά, έναντι 58 % το 2015. Η διαδικτυακή διαθεσιμότητα δημόσιων υπηρεσιών αυξάνεται σταθερά την τελευταία δεκαετία, ενώ επιταχύνθηκε σημαντικά ως αποτέλεσμα της πανδημίας COVID-19, κατά την οποία επικράτησε η ψηφιακή αλληλεπίδραση. Ορισμένα κράτη μέλη βρίσκονται ήδη κοντά στον στόχο αυτόν, αλλά η πρόοδος είναι άνιση τόσο μεταξύ όσο και εντός των κρατών μελών, καθώς οι υπηρεσίες για τους πολίτες είναι λιγότερο πιθανό να είναι διαθέσιμες διαδικτυακά σε σύγκριση με τις υπηρεσίες για τις επιχειρήσεις».



Εικόνα 6 ΔΕΙΚΤΗΣ DESI ΓΙΑ ΤΗΝ ΘΕΣΗ ΤΗΣ ΕΛΛΑΔΑΣ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ-
ΔΕΙΚΤΕΣ: 1.ΑΝΘΡΩΠΙΝΟ ΚΕΦΑΛΑΙΟ 2.ΣΥΝΔΕΣΙΜΟΤΗΤΑ 3.ΕΝΣΩΜΑΤΩΣΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ 4.ΨΗΦΙΑΚΕΣ ΔΗΜΟΣΙΕΣ ΥΠΗΡΕΣΙΕΣ»[36]

[35] Λαζακίδου (2019) Α. Ηλεκτρονική Διακυβέρνηση και Ηλεκτρονικές Υπηρεσίες προς Πολίτες και Επιχειρήσεις Εκδόσεις Δίσιγμα

2.2 *Πολιτική Ασφαλείας Δημοσίων Υπηρεσιών*

Η Πολιτική Ασφαλείας σε μία Δημόσια Υπηρεσία είναι μία από τις συνιστώσες που υποστηρίζουν την διαλειτουργικότητα αφού είναι προϋπόθεση για το διαμοιρασμό των δεδομένων και την ασφάλεια τους.

Η αυτοματοποίηση των διαδικασιών και η άμεση διασύνδεση συσκευών επιτάσσει διαφάνεια, εμπιστοσύνη και προστασία προσωπικών δεδομένων σύμφωνα με τον Γενικό Κανονισμό (GDPR).Η εφαρμογή κανόνων προστασίας δεδομένων, ευάλωτων στην ΤΠΕ, ονομάζεται πολιτική ασφαλείας στο κυβερνοχώρο και εφαρμόζεται ως αντίμετρο προκειμένου να μειωθεί η επικινδυνότητα.

Για να προσδιορίσουμε τα μέτρα που θα χρησιμοποιήσουμε θα πρέπει να εντοπίσουμε τις αδυναμίες και τις ανάγκες, και να σχεδιάσουμε τον τρόπο αντιμετώπισης τους με επιχειρησιακές διεργασίες. Απαιτείται στρατηγική με στόχο, ήτοι διακυβέρνηση ασφάλειας πληροφοριών.

Η εφαρμογή τεχνολογιών και εργαλείων προστασίας καθώς και η υλοποίηση πολιτικών και διαδικασιών θα εξασφαλίσει ευελιξία και αυξημένη προστασία στον οργανισμό. Η ηγεσία κάθε οργανισμού θα πρέπει να αναπτύξει στρατηγικό σχεδιασμό για την διαμόρφωση κατάλληλης οργανωσιακής υποδομής και να ενσωματώσει συστήματα διαχείρισης ασφαλείας στον αρχιτεκτονικό σχεδιασμό με τεκμηρίωση και καθοδήγηση για καθορισμό ρόλων και αρμοδιοτήτων σε υπευθύνους.

‘Όμως όπως έχει αναφερθεί και παραπάνω (κεφάλαιο κυβερνοασφάλειας) το αντικείμενο της κυβερνοασφάλειας δεν ήταν ποτέ η τεχνολογία και η αλγοριθμική θωράκισή της, αλλά ο ανθρώπινος παράγοντας αφού οι κυριότερες αδυναμίες εντοπίζονται σε ζητήματα όπως εκπαίδευση προσωπικού, επιβολή κανόνων , έλεγχος συμμόρφωσης με τις πολιτικές ασφαλείας οπότε θα πρέπει να υπάρξει κατάλληλη ισορροπία μεταξύ της προστασίας των πληροφοριών και της ευκολίας στην εργασία του χρήστη που υπαγορεύει αδύναμους κωδικούς. ‘Αλλωστε έχει διαπιστωθεί ότι συχνά στις κυβερνοεπιθέσεις οι κωδικοί ασφαλείας είναι ένα από τα ευάλωτα σημεία που διεισδύουν οι επιτιθέμενοι.

[36] https://ec.europa.eu/commission/presscorner/detail/el/QANDA_21_5483

Το Σύστημα Διαχείρισης Ασφαλείας Πληροφοριών σύμφωνα με το πρότυπο ISO/IEC 27001 θα πρέπει να καλύπτει σε γενικές γραμμές τους βασικούς τομείς:

1.*Πολιτικές ασφαλείας πληροφοριών, 2.Οργάνωση και ασφάλεια πληροφοριών, 3.Ανθρώπινου δυναμικού, 4.Διαχείρισης περιουσιακών στοιχείων, 5.'Ελεγχο πρόσβασης, 6. Κρυπτογραφία, 7.Φυσικής και περιβαλλοντικής ασφάλειας, 8.Λειτουργική ασφάλεια, 9.Ασφάλεια επικοινωνιών, 10.Προμήθεια ανάπτυξη και συντήρηση συστημάτων, 10.Σχέσεις με προμηθευτές 12.Διαχείριση επεισοδίων ασφαλείας πληροφοριών, 13.Ασφάλεια πληροφοριών και επιχειρησιακή συνέχεια, 14.Συμμόρφωση*[37]

Οι βασικές αρχές είναι:

α)Οργανωτικά μέτρα ασφαλείας τα οποία σχετίζονται με τον καθορισμό των ρόλων, του εσωτερικού ελέγχου, των αρμοδιοτήτων, της κανονιστικής συμμόρφωσης (GDPR), της εκπαίδευσης προσωπικού, της διαχείριση των περιστατικών ασφαλείας, της καταστροφής δεδομένων και αποθηκευτικών μέσων κ.λ.π

β)Τεχνικά μέτρα ασφαλείας που σχετίζονται με τον έλεγχο πρόσβασης, την κρυπτογράφηση, διαμόρφωση υπολογιστών, τα αντίγραφα ασφαλείας, ασφάλεια επικοινωνιών, internet, τηλέφωνα, διαχείριση αλλαγών κ.λ.π

γ)Μέτρα φυσικής ασφάλειας που σχετίζονται με περιβαλλοντική ασφάλεια, έλεγχο φυσικής πρόσβασης, φωτισμό, φύλαξη εγγράφων, προστασία και αποθήκευση φορητών μέσων, προστασία οθονών, αντίγραφα ασφαλείας, data room κλπ [38]

Για να εφαρμοσθούν επιτυχημένα πολιτικές ασφαλείας σε ένα οργανισμό απαιτείται οι διοικητικές διαδικασίες να συγχρονίζονται με τις βασικές αρχές και στόχους των πληροφοριακών συστημάτων, οι κανόνες να εφαρμόζονται απόλυτα και με σεβασμό σε κοινωνικοπολιτικές αξίες με συμμετοχή και ενδιαφέρον όλων των οντοτήτων.

Η πολιτική ασφαλείας είναι η δέσμευση κάθε διοίκησης για την προστασία των Πληροφοριακών και Επικοινωνιακών Συστημάτων και Δικτύων και των Προσωπικών Δεδομένων γι αυτό είναι αναγκαία πρόδηλη[39].

[37] Κάτσικας Σ. Γκρίτζαλης Σ. Λαμπρινουδάκης Κ. (2021) Ασφάλεια Πληροφοριών και Συστημάτων στο Κυβερνοχώρο Εκδόσεις Νέων Τεχνολογιών Αθήνα
[38] https://mindigital.gr/kyvernoasfaleia

ΚΕΦΑΛΑΙΟ 3ο

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΟΝ *e-ΕΦΚΑ*

Για να μπορέσουμε να χρησιμοποιήσουμε τους υπολογιστές απαιτείται αλλαγή σε νομικό και θεσμικό πλαίσιο με συναίνεση και συνεργασία σε ένα διαφορετικό επίπεδο. Προκειμένου να είναι εφικτή η εξυπηρέτηση των πολιτών με όρους ηλεκτρονικής διακυβέρνησης επιβάλλεται να αλλαχθούν και να σχεδιασθούν εκ νέου οι διαδικασίες και να δοθούν οδηγίες προσαρμογής. Το επιχείρημα είναι σύνθετο και πολύπλοκο καθώς το κράτος εγκλωβισμένο σε γραφειοκρατικές αγκιστρώσεις καλείται να προσεγγίσει το καινούργιο, και να αντιμετωπίσει μία εξελίξιμη τεχνολογία προσαρμοσμένη και εναρμονισμένη στις ανάγκες της σημερινής κοινωνίας.

Για να κατανοήσουμε τις δυσκολίες και τα προβλήματα που δημιουργούνται στα πληροφοριακά συστήματα του e-ΕΦΚΑ κρίνουμε σκόπιμο αρχικά να ανατρέξουμε σε μία συνοπτική ιστορική αναδρομή της προγενέστερης κατάστασης των φορέων κοινωνικής ασφάλισης και στην συνέχεια να παραθέσουμε την υπάρχουσα κατάσταση με τα πολλαπλά πληροφοριακά συστήματα, την έλλειψη διαλειτουργικότητας και την ελλιπή κυβερνοασφάλεια.

3.1 Ιστορική Αναδρομή του e-ΕΦΚΑ

Ο ΕΦΚΑ είναι ο Ενιαίος Φορέας Κοινωνικής Ασφάλισης που προήλθε από την ενοποίηση των υπαρχόντων ταμείων κοινωνικής ασφάλισης.

. Όπως αναφέρεται στο βιβλίο του Κουβεριανού Βαγγέλη:

«*Η διοικητική και λειτουργική ενοποίηση του ΕΦΚΑ μαζί με την ενιαιοποίηση των κανόνων εισφορών όλων των ασφαλισμένων είναι απαραίτητη για την πρώτη εφαρμογή της νέας δομής της σύνταξης και την συνολική αναδιάταξη του συνταξιοδοτικού τοπίου.*»

Ο Ν.5733/1932 καθιέρωνε το ΙΚΑ ως γενικό ασφαλιστικό ταμείο μισθωτών και απαγόρευε τη σύσταση νέων οργανισμών κοινωνικής ασφάλισης, αλλά δεν εφαρμόστηκε λόγω της ασυντόνιστης εργατικής δυναμικής και της πελατειακής κρατικής πολιτικής. Το ζήτημα της ενοποίησης τίθεται ήδη από την δεκαετία του 1950,

[39] https://www.reporter.gr/Eidhseis/technologia/462967-H-kyberno-asfaleia-allazei-to-dhmosio

ουσιαστικά όμως είναι οι επιτακτικές και συντονισμένες πιέσεις προσαρμογής στην οικονομική κρίση της δεκαετίας του 1990 που θα οδηγήσουν στην πρώτη φάση των ενοποιήσεων. Επιχειρώντας, για τις ανάγκες της κατανόησης των αλλαγών, μία τυπολογία των ενοποιήσεων φορέων κοινωνικής ασφάλισης, μπορούμε να διακρίνουμε μεταξύ διοικητικής και λειτουργικής ενοποίησης (ΚΕΠΕ 2014). Η διοικητική ενοποίηση αποτελεί ενοποίηση διοικητικών δομών σε αντιδιαστολή με την λειτουργική ενοποίηση που συνιστά ενοποίηση των κανόνων που διέπουν άμεσα ή έμμεσα τις υποχρεώσεις και τα δικαιώματα των ασφαλισμένων. Επομένως, η ενοποίηση του 2008 συνιστά κυρίως διοικητική ενοποίηση. Από τους 120 οργανισμούς κοινωνικής ασφάλισης και τα 54 ταμεία αλληλοβοήθειας προκύπτουν 19 οργανισμοί (Καλλιαντέρης), αλλά αυξάνεται η πολυπλοκότητα του συστήματος, διότι εντός των νέων Οργανισμών Κοινωνικής Ασφάλισης ιδρύονται τόσοι τομείς και συνυπάρχουν τόσα ασφαλιστικά καθεστώτα όσοι και οι καταργηθέντες ΟΚΑ.

Η λειτουργική ενοποίηση ενοποιεί τους εφαρμοζόμενους κανόνες, το επίπεδο υποχρεώσεων και δικαιωμάτων των ασφαλισμένων συγκλίνοντας τα επίπεδα κοινωνικοασφαλιστικής προστασίας. Χαρακτηριστικά παραδείγματα λειτουργικών ενοποιήσεων είναι η ίδρυση του ΕΟΠΥΥ για την ενοποίηση του κλάδου υγείας, των ΚΕΠΑ για την ενοποίηση της πιστοποίησης αναπηρίας, του ΚΕΑΟ για την ενοποίηση του εισπρακτικού μηχανισμού και ασφαλώς η πρώτη ενοποίηση της επικουρικής σύνταξης στο ΕΤΕΑ.

Βασικές στιγμές στην πορεία ενοποίησης των οργανισμών κοινωνικής ασφάλισης στον κλάδο σύνταξης είναι ο νόμος Σιούφα το 1992, και ο νόμος Πετραλιά το 2008.

Το 1992 με το ν.3029/2002, γνωστό έκτοτε ως νόμο Σιούφα από τον εισηγητή Υπουργό, υλοποιείται η πρώτη μεγάλη ενοποίηση ασφαλιστικών καθεστώτων, όχι απλά διοικητικών μηχανισμών αλλά και κανόνων για τους ασφαλισμένους που πρωτοασφαλίζονται μετά το 1992. Η ενοποίηση αυτή, σαφώς δυσμενής για τους νέους ασφαλισμένους, προετοιμάζει μία ουσιαστική ενοποίηση των ασφαλιστικών καθεστώτων με ορίζοντα αποτελεσμάτων τις επόμενες δεκαετίες, αλλά ταυτόχρονα δημιουργεί έναν επιπλέον διαχωρισμό μεταξύ ασφαλισμένων με βάση το χρόνο πρώτης ασφάλισης, έναν διαχωρισμό που δύσκολα δικαιολογείται με βάση τις αρχές κοινωνικής ασφάλισης.

Από το 2008 και μετά, το ελληνικό Σύστημα Κοινωνικής Ασφάλισης χαρακτηρίζεται από μία σταδιακή αλλά σταθερή μετάβαση προς ένα σύστημα συνταξιοδοτικής

προστασίας τύπου Beveridge, δηλαδή ένα σύστημα που προσανατολίζεται κυρίως σε μία βασική συνταξιοδοτική προστασία με ενιαία οργάνωση και κανόνες για όλες τις κατηγορίες εργαζομένων (Παπαρρηγοπούλου Πεχλιβανίδη 2016). Το 2008 με το ν.3655/2008 επί Υπουργίας Πετραλιά επιχειρείται μία κυρίως διοικητικής φύσης ενοποίηση. Η ιδιορρυθμία της ενοποίησης του 2008 έγκειται στο γεγονός ότι δεν ενοποιούνται οι καταστατικές ρυθμίσεις των ενοποιούμενων ταμείων, οι οποίες ισχύουν παράλληλα.

Από το 2010, τίθεται ο -μνημονιακός πια- στόχος ενοποίησης των οργανισμών κοινωνικής ασφάλισης σε τρεις μεγάλους οργανισμούς για τον κλάδο κύριας σύνταξης με την ένταξη ομοειδών ΟΚΑ και σε έναν ενιαίο οργανισμό επικουρικής σύνταξης για τον επικουρικό κλάδο(ν.3845/2010).

Από το 2012, με το ν. 4052/2012 δημιουργείται το Ενιαίο Ταμείο Επικουρικής Ασφάλισης όλων των κλάδων, των ταμείων και των τομέων επικουρικής ασφάλισης με σκοπό την παροχή επικουρικής σύνταξης. Από το άρθρο 39 του ανωτέρω νόμου και τον νέο Κανονισμό Παροχών προκύπτει ξεκάθαρα ότι δεν έχουμε ενοποίηση υπαρχόντων κανόνων για υποχρεώσεις και δικαιώματα ασφαλισμένων στον κλάδο επικουρικής ασφάλισης. Η ενοποίηση με τη δημιουργία του ΕΤΕΑ συνιστά ταυτόχρονα αλλαγή της φυσιογνωμίας της κοινωνικής ασφάλισης, παραμένοντας στη δημόσια σφαίρα ως προς την οργάνωση, όχι όμως και ως προς την λογική της (Στεργίου 2014, σ. 68,71).

Η διοικητική διάσπαση του ασφαλιστικού συστήματος είναι εντυπωσιακή. Ενδεικτικό είναι ότι το 1990 λειτουργούσαν 327 φορείς κύριας και επικουρικής ασφάλισης, λοιπών παροχών και περιορισμένος αριθμός υπηρεσιών ασφάλισης καθώς και κρατικές υπηρεσίες για την συνταξιοδότηση και υγειονομική περίθαλψη των δημοσίων υπαλλήλων, πολιτικών και στρατιωτικών. Το 1997 υφίστανται 28 φορείς κύριας ασφάλισης και παραπάνω από 200 φορείς επικουρικής ασφάλισης.

Σύμφωνα με δημοσιευμένα στοιχεία του συστήματος Ήλιος, συντάξεις γήρατος, αναπηρίας, θανάτου ή κάποιας άλλης κατηγορίας δίδονται από 21 φορείς. Οι 21 αυτοί φορείς αποτελούνται από 78 υπό ομάδες ή κλάδους, ορισμένοι εκ των οποίων φαίνεται να εξυπηρετούν μερικές δεκάδες συνταξιούχους. Είναι χαρακτηριστικό το παράδειγμα του ΕΤΑΠ-ΜΜΕ που συνολικά παρέχει 8.208 συντάξεις και αποτελείται από 10 τομείς ασφάλισης.

Σύμφωνα με την Επιτροπή Εμπειρογνωμόνων του 2015 για την μεταρρύθμιση του Συστημάτων Κοινωνικής Ασφάλισης, υπέρ της ενοποίησης προκρίνονται περισσότερο

οικονομικά κριτήρια και κριτήρια λειτουργικότητας και αποδοτικότητας: Το υφιστάμενο σύστημα κοινωνικής ασφάλισης χαρακτηρίζεται από μία πολύπλοκη θεσμική δομή, η οποία, παρ' όλες τις βελτιώσεις που έχει δεχθεί διαχρονικά, δημιουργεί σοβαρά εμπόδια στην αποδοτική λειτουργία του.Ένα βασικό πρόβλημα είναι η εμπλοκή πολλών, διαφορετικών και ορισμένες φορές με διαφορετικές επιδιώξεις, νομικών προσώπων.

Ενδεικτικό είναι ότι η εποπτεία του συστήματος κοινωνικής ασφάλισης μοιράζεται ανάμεσα στα Υπουργεία Εργασίας, Κοινωνικής Ασφάλισης και Πρόνοιας, το Υπουργείο Οικονομικών, το Υπουργείο Εθνικής Άμυνας και το Υπουργείο Προστασίας του Πολίτη. Σύμφωνα με το μητρώο φορέων της Γενικής Κυβέρνησης της ΕΛΣΤΑΤ το Δεκέμβριο του 2012 ήταν καταγεγραμμένοι 41 Φορείς Κοινωνικής Ασφάλισης (ΦΚΑ), χωρίς να υπολογίζεται το Γενικό Λογιστήριο του Κράτους (ΓΛΚ) που είναι υπεύθυνο για τις συντάξεις του Δημοσίου.

Το σύστημα κοινωνικής ασφάλισης είναι όμως ακόμα πιο κατακερματισμένο, αφού κάτω από την ίδια στέγη υπάρχουν παλαιότερα ασφαλιστικά ταμεία που ακόμα και μετά την ενοποίησή τους εξακολουθούν να διατηρούν πλήρη οικονομική και λειτουργική αυτοτέλεια.

Αποτιμώντας τις διαχρονικές ενοποιήσεις των ασφαλιστικών δομών που έλαβαν χώρα τα τελευταία χρόνια, καταλήγουμε στο συμπέρασμα ότι ήταν κυρίως επιφανειακές και ορισμένες φορές, λόγω του ελλιπούς σχεδιασμού τους, βιαστικές. Χωρίς ουσιαστική προετοιμασία και προσαρμογή, αλλά με υποχωρήσεις συχνά σε συνδικαλιστικές πιέσεις, ήταν αναποτελεσματικές και δημοσιονομικά επιβλαβείς»[40].

Παραθέσαμε αυτούσιο απόσπασμα από το βιβλίο του Κουβεριανού Βαγγέλη καθώς η σύντομη ανάλυσή του είναι αρκετά κατατοπιστική για να αντιληφθούμε τον τρόπο που αντιμετωπιζόταν η δημόσια κοινωνική ασφάλιση στην χώρα μας.

Η οικονομική κρίση υπήρξε η αφορμή για ουσιαστικές και οριστικές μεταρρυθμίσεις δημοσιονομικής προσαρμογής και διαρθρωτικών αλλαγών. Στα πλαίσια αυτά με τον Ν.4387/16 (όπως τροποποιήθηκε και ισχύει σήμερα με τον Ν.4445/2016) συστάθηκε ο Ενιαίος Φορέας Κοινωνικής Ασφάλισης (ΕΦΚΑ) ως Νομικό Πρόσωπο Δημοσίου Δικαίου (Ν.Π.Δ.Δ.) με έναρξη λειτουργίας την 1/1/2017 που τελεί υπό την εποπτεία του υπουργείου εργασίας και κοινωνικών υποθέσεων. Στον ΕΦΚΑ τον μεγαλύτερο

[40] https://ejournals.epublishing.ekt.gr/index.php/eekp/article/view/14604

φορέα κλάδου κύριας ασφάλισης εντάχθηκαν αυτοδίκαια σχεδόν όλοι οι φορείς κύριας κοινωνικής ασφάλισης.

‘Όπως αναφέρεται στον Ν.4387/2016 άρθρο 53 ο ΕΦΚΑ πλέον περιλαμβάνει τους κάτωθι φορείς:

1. Ίδρυμα Κοινωνικών Ασφαλίσεων-Ενιαίο Ταμείο Ασφάλισης Μισθωτών (ΙΚΑ-ΕΤΑΜ).

2. Ενιαίο Ταμείο Ασφάλισης Προσωπικού Μέσων Μαζικής Ενημέρωσης (ΕΤΑΠ-ΜΜΕ).

3. Ενιαίο Ταμείο Ανεξάρτητα Απασχολούμενων (ΕΤΑΑ).

4. Οργανισμός Ασφάλισης Ελεύθερων Επαγγελματιών (ΟΑΕΕ).

5. Οργανισμός Γεωργικών Ασφαλίσεων (ΟΓΑ) εκτός του Λογαριασμού Αγροτικής Εστίας.

6. Ναυτικό Απομαχικό Ταμείο (ΝΑΤ).

7. Ταμείο Ασφάλισης Υπαλλήλων Τραπεζών και Επιχειρήσεων Κοινής Ωφέλειας (ΤΑΥΤΕΚΩ).

8. Ενιαίο Ταμείο Ασφάλισης Τραπεζοϋπαλλήλων (ΕΤΑΤ)

9. Γενική Διεύθυνση Χορήγησης Συντάξεων Δημοσίου Τομέα (ΓΛΚ).

Επίσης, στον ΕΦΚΑ μεταφέρθηκε και υπάγεται το Κέντρο Είσπραξης Ασφαλιστικών Οφειλών (ΚΕΑΟ) με τις αρμοδιότητες που προβλέπονται από τη νομοθεσία που το διέπει.

Στην συνέχεια με τον με τον ν.4670/20 από την 1/3/2020 ο Ενιαίος Φορέας Κοινωνικής Ασφάλισης (ΕΦΚΑ) μετονομάστηκε σε Ηλεκτρονικό Εθνικό Φορέα Κοινωνικής Ασφάλισης (e-ΕΦΚΑ). Στον e-ΕΦΚΑ εντάχθηκε από την 1.3.2020 το Ενιαίο Ταμείο Επικουρικής Ασφάλισης και Εφάπαξ Παροχών (Ε.Τ.Ε.Α.Ε.Π.). Με την δημιουργία του e-ΕΦΚΑ ολοκληρώθηκε η μεγαλύτερη διοικητική και οργανωτική ενοποίηση των ασφαλιστικών φορέων απονομής σύνταξης και εφάπαξ παροχής της χώρας.

Τα υπακτέα στην ασφάλιση του e-ΕΦΚΑ πρόσωπα είναι οι ασφαλισμένοι και συνταξιούχοι και τα προστατευόμενα μέλη των οικογενειών τους που υπήχθησαν στην ασφάλιση των εντασσόμενων φορέων, τομέων, κλάδων και λογαριασμών καθώς και τα πρόσωπα που ανέλαβαν ασφαλιστέα εργασία ή απέκτησαν την ασφαλιστέα ιδιότητα από την έναρξη λειτουργίας του e-ΕΦΚΑ και μετά και τα προστατευόμενα μέλη αυτών.

Αρμοδιότητα του e-ΕΦΚΑ είναι η παροχή υπηρεσιών κοινωνικής ασφάλισης στα υπακτέα στην ασφάλισή του πρόσωπα όπως η χορήγηση κύριας σύνταξης (γήρατος, αναπηρίας και θανάτου), προσυνταξιοδοτικών παροχών, παροχών ασθενείας σε χρήμα, ειδικών προνοιακών επιδομάτων και κάθε άλλης παροχής υπηρεσιών σε χρήμα για την οποία καθίσταται αρμόδιος. Πόρους του e-ΕΦΚΑ αποτελούν τα έσοδα από τις ασφαλιστικές εισφορές, οι πρόσοδοι περιουσίας και η απόδοση των κεφαλαίων και των αποθεματικών των φορέων, τομέων, κλάδων και λογαριασμών[41][42]

3.2 *ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΟΝ Ε- ΕΦΚΑ*

Η μετονομασία του φορέα σε Ε-ΕΦΚΑ φιλοδοξεί να σηματοδοτήσει την ηλεκτρονική διακυβέρνηση η οποία θα εξυπηρετείται από την διαλειτουργικότητα των πληροφοριακών συστημάτων.

Στην παρούσα μεταβατική φάση όμως αυτό σημαίνει ότι οι πολίτες εξυπηρετούνται από πληθώρα πληροφοριακών συστημάτων των ενταχθέντων Φορέων Κοινωνικής Ασφάλισης (ΦΚΑ) που δεν συνδέονται μεταξύ τους όπως αναλύονται κατωτέρω.

Η Πληροφοριακή Υποδομή του Ηλεκτρονικού Εθνικού Φορέα Κοινωνικής Ασφάλισης (e-ΕΦΚΑ), αποτελείται από τα διαφορετικά πληροφοριακά συστήματα των συγχωνευθέντων Φορέων Κοινωνικής Ασφάλισης (ΦΚΑ) και τις Ηλεκτρονικές Υπηρεσίες που παρέχονται μέσω διαδικτύου σε πολίτες, επιχειρήσεις και φορείς που εξυπηρετούν την συναλλαγή με τους πολίτες και χρησιμοποιούνται στην υφιστάμενη κατάσταση:[43][44]

- **Ολοκληρωμένο Πληροφοριακό Σύστημα Μισθωτών (ΟΠΣ-ΕΦΚΑ Μισθωτών-τ.ΟΠΣ-ΙΚΑ ΕΤΑΜ)**

  Το ΟΠΣ-ΕΦΚΑ Μισθωτών είχε εγκατασταθεί αρχικά σε περίπου 300 σημεία εγκατάστασης (μεταξύ των οποίων 164 Υποκ/τα και 127 Παρ/τα), με περίπου 9.000 χρήστες, οι οποίοι εκτελούσαν περίπου 120.000 συναλλαγές ημερησίως.

---

[41] https://www.e-nomothesia.gr/kat-ergasia-koinonike-asphalise/nomos-4387-2016-phek-85a-12-5-2016.html

[42] Τεχνικές και Λειτουργικές προδιαγραφές. Διασύνδεση του ΕΦΚΑ με το Ευρωπαϊκό Σύστημα Ηλεκτρονικής Ανταλλαγής Πληροφοριών για την Κοινωνική Ασφάλιση (EESSI)

[43] https://www.ieidiseis.gr/oikonomia/134998/efka-9-asyndetes-psifiakes-platformes-talaiporoyn-tous-asfalismenous?fbclid=IwAR3ixzQex3ZnOen4__mpGGFL1C4RG-vASATv_gFSc8_twdfWx8XHh0gp_Ao

[44] https://www.dikastiko.gr/eidhsh/sfodri-antidrasi-tis-olomeleias-ston-efka-me-apeili-lipsis-metron-quot-dekades-dikigoroi-vrethikan-paranomos-anasfalistoi-quot/

Σήμερα το ΟΠΣ ΕΦΚΑ Μισθωτών (πρώην ΟΠΣ-ΙΚΑ) λειτουργεί πλέον των 200 σημείων εγκατάστασης με 6.000 χρήστες.

Το ΟΠΣ-ΕΦΚΑ Μισθωτών είναι **ένα ιδιαίτερα πολύπλοκο έργο πληροφορικής**. Για την υλοποίηση του λογισμικού του ΟΠΣ-ΕΦΚΑ Μισθωτών, έχουν δημιουργηθεί περίπου 15.000 προγραμματιστικά αντικείμενα (πίνακες της βάσης δεδομένων, όψεις της βάσης δεδομένων, συναρτήσεις και triggers).

Το υφιστάμενο ΟΠΣ, το οποίο στηρίζεται στις υποδομές του πρώην ΙΚΑ-ΕΤΑΜ, με τις όποιες παρεμβάσεις, τροποποιήσεις, επεκτάσεις έχουν υλοποιηθεί, προκειμένου να υποστηρίξει τις απαιτήσεις λειτουργίας του ΕΦΚΑ, για την εγγραφή των εργοδοτών, τις εισφορές για τους Μισθωτούς, τις συντάξεις και την οικονομική διαχείριση. Το ***«Υφιστάμενο ΟΠΣ ΕΦΚΑ»*** υποστηρίζει, επιπλέον, τη λειτουργία του Κέντρου Είσπραξης Ασφαλιστικών Οφειλών [ΚΕΑΟ] και του Κέντρου Πιστοποίησης Αναπηρίας [ΚΕ.Π.Α].

Η υποδομή ηλεκτρονικών υπηρεσιών του ΕΦΚΑ, στηρίζεται σε υποδομές του πρώην ΙΚΑ-ΕΤΑΜ και υποστηρίζει την παροχή ηλεκτρονικών υπηρεσιών στους εργοδότες, τους ασφαλισμένους και άλλους φορείς. Η διαδικτυακή πύλη του ΙΚΑΝΕΤ είναι εξωτερική διεπαφή αυτής της υποδομής.

Πέραν του σημερινού ***«Υφιστάμενου ΟΠΣ ΕΦΚΑ»***, για την εξυπηρέτηση των ασφαλισμένων του ΕΦΚΑ, κατά τη μεταβατική λειτουργία του ΕΦΚΑ, χρησιμοποιούνται πληροφοριακά συστήματα που έχουν υλοποιηθεί από την ΗΔΙΚΑ Α.Ε. ή από τους πρώην ΦΚΑ. Τα συστήματα αυτά υποστήριζαν λειτουργίες των Φ.Κ.Α πριν την ενοποίηση, βάσει σχετικής νομοθεσίας. Με την κατάλληλη τροποποίηση τα συστήματα αυτά υποστηρίζουν τον ΕΦΚΑ κατά τη μεταβατική περίοδο λειτουργίας του.

- **Πληροφοριακό Σύστημα τ.ΟΑΕΕ** που εξυπηρετεί τους ασφαλισμένους του τ.ΟΑΕΕ
- **Πληροφοριακό Σύστημα τ.ΟΓΑ** που εξυπηρετεί τους ασφαλισμένους του τ.ΟΓΑ
- **Πληροφοριακό Σύστημα τ.ΤΣΑΥ** που εξυπηρετεί τους ασφαλισμένους του τ.ΤΣΑΥ
- **Πληροφοριακό Σύστημα** τ.**ΤΣΜΕΔΕ** που εξυπηρετεί τους ασφαλισμένους του τ.ΤΣΜΕΔΕ

- Το σύστημα του **Web Μητρώου** που διαχειρίζεται από την ΗΔΙΚΑ Α.Ε. (Μητρώο Ασφαλισμένων).
- Το σύστημα πληροφορικής για τις εισφορές των **Μη-Μισθωτών** (διαχειρίζεται από την ΗΔΙΚΑ Α.Ε.).
- Το Ενιαίο Σύστημα Ελέγχου και Πληρωμών Συντάξεων (**ΕΣΕΠΣ**).
- Το Σύστημα **ΑΤΛΑΣ,** που στόχος του είναι να ενσωματώσει σταδιακά το χρόνο ασφάλισης όλων των πολιτών της χώρας.

Οικονομική Διαχείριση

- Για τη μηχανογραφική κάλυψη των εργασιών των οικονομικών υπηρεσιών του e ΕΦΚΑ, χρησιμοποιείται το υπάρχον Πληροφοριακό Σύστημα Οικονομικής Διαχείρισης του **ΟΠΣ τ.ΙΚΑ-ΕΤΑΜ**, αναπτύσσοντας τις απαραίτητες τροποποιήσεις λογισμικού εφαρμογών.

Διαχείριση Προσωπικού και Μισθοδοσίας

- Για την μηχανογραφική κάλυψη των αναγκών της διαχείρισης προσωπικού και μισθοδοσίας του e ΕΦΚΑ, χρησιμοποιείται το Ολοκληρωμένο Πληροφοριακό Σύστημα Διαχείρισης Ανθρώπινου Δυναμικού «**COMPASS**». Το σύστημα έχει εγκατασταθεί και λειτουργεί σε υποδομές του e ΕΦΚΑ.

Διαχείριση συντονισμού και Υποστήριξης

- Για την μηχανογραφική κάλυψη των αναγκών της διαχείρισης συντονισμού και Υποστήριξης χρησιμοποιείται η Ενιαία Ανεξάρτητη Αρχή Δημοσίων Συμβάσεων (ΕΑΔΗΣΗ), το Εθνικό Σύστημα Ηλεκτρονικών Δημοσίων Συμβάσεων (ΕΣΗΔΗΣ) και Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ), το Κεντρικό Σύστημα Ηλεκτρονικής Ανάρτησης πράξεων στο Διαδίκτυο (ΔΙΑΥΓΕΙΑ) και το Πληροφοριακό Σύστημα Ηλεκτρονικής Διαχείρισης Εγγράφων (ΣΗΔΕ-ΙΡΙΔΑ) το οποίο θα αντικατασταθεί με το Σύστημα Ηλεκτρονικής Διαχείρισης Εγγράφων (ΣΗΔΕ-DOCUTRACKS)

EMAIL

- Η εξυπηρέτηση ανάμεσα υπαλλήλων και πολιτών πραγματοποιείται μέσω corpmail

Δίκτυο INTRANET (πρώην ΙΚΑΝΕΤ)

- Το ΙΚΑnet ήταν ένα από τα πιο μεγάλα έργα του δημοσίου στο πλαίσιο του Γ'ΚΠΣ, ύψους περίπου 6,5 εκ.ευρώ.Το έργο περιλαμβάνει το λεπτομερή σχεδιασμό και υλοποίηση τηλεπικοινωνιακού δικτύου που θα ενοποιούσε 425 οργανωτικές μονάδες και γραφεία του οργανισμού και θα διευκόλυνε σε πλήρη ολοκλήρωση, σε συνδυασμό τόσο με την υπάρχουσα όσο και με την υπό διαμόρφωση μηχανογραφική υποδομή του οργανισμού, την αποτελεσματική και ασφαλή μεταφορά δεδομένων, καθώς και παροχή υπηρεσιών φωνής και εικόνας (IP-VPN)[45].Πλέον μετονομάστηκε σε INTRANET το οποίο συνδέει τις μονάδες του e ΕΦΚΑ μισθωτών, με τις κεντρικές υπηρεσίες του ΕΦΚΑ. Η σχεδίαση και υλοποίηση του δικτύου έχει γίνει με τον κανόνα παροχής υπηρεσιών μεταγωγής δεδομένων υψηλού επιπέδου (SLA), έτσι ώστε σε κάθε περίπτωση να εξασφαλίζονται υψηλά ποιοτικά χαρακτηριστικά λειτουργίας και η διαθεσιμότητα του δικτύου να είναι τουλάχιστον 99,9%. Σταδιακά και άλλες υπηρεσίες του e ΕΦΚΑ, πέρα από εκείνες των μισθωτών, συνδέονται στο εν λόγω δίκτυο.

Σύζευξις

- Πρόκειται για εθνικό δίκτυο της δημόσιας διοίκησης, το οποίο προσφέρει ευρυζωνικές υπηρεσίες δικτύου και διακίνησης Φωνής-Εικόνας-Δεδομένων σε φορείς του ελληνικού δημοσίου. Περιφερειακές και κεντρικές υπηρεσίες του e ΕΦΚΑ συνδέονται στο δημόσιο δίκτυο Σύζευξις, αξιοποιώντας τις υπηρεσίες που αυτό προσφέρει.
- Διαλειτουργεί επίσης με το Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης και Κοινωνικής Αλληλεγγύης για τη διασύνδεση με το σύστημα ΕΡΓΑΝΗ, με το Υπουργείο Εσωτερικών που λειτουργεί το Μητρώο Πολιτών για την άντληση δημογραφικών και ληξιαρχικών γεγονότων καθώς και προσωπικών στοιχείων των πολιτών, με την Ανεξάρτητη Αρχή Δημοσίων Εσόδων για τη διασύνδεση με το TAXIS, με το Κέντρο Πληροφορικής του Υπουργείου Οικονομικών (ΚΕΠΥΟ), με την Ελληνική Αστυνομία για τη διασταύρωση στοιχείων ταυτοτήτων και διαβατηρίων, με το Υπουργείο Ανάπτυξης, Οικονομίας και

[45] Αποστολάκης Ι., Λουκής Ε., Χάλαρης Ι. (2008) Ηλεκτρονική Δημόσια Διοίκηση Εκδόσεις Παπαζήση, Αθήνα

Τουρισμού, για άντληση στοιχείων εταιρειών από το Γενικό Εμπορικό Μητρώο.

Πλατφόρμα τηλεκπαίδευσης (e-learning)

- Ο e ΕΦΚΑ οργανώνει και πραγματοποιεί διαδικτυακές τηλεδιασκέψεις μέσεω της υπηρεσίας **e:Presence.gov.gr** που δίνει την δυνατότητα στους φορείς του Ελληνικού Δημοσίου

3.2.1 ***Εξέλιξη των λειτουργιών των πληροφοριακών συστημάτων της κοινωνικής ασφάλισης***

Το μοντέλο της αρχιτεκτονικής του ΟΠΣ ΙΚΑ βασίζεται στην αρχή της αποκέντρωσης των λειτουργιών και των δεδομένων, όσον αφορά τις λειτουργίες οι περισσότερες εκτελούνται σε επίπεδο Περιφερειακών και Τοπικών Υποκ/των.

Στις κεντρικές υπηρεσίες εκτελούνται συνήθως batch διαδικασίες αλλά και ορισμένες online διαδικασίες που αφορούν κεντρικά μητρώα (π.χ.ασφαλισμένων).Οι βάσεις δεδομένων τηρούνται τόσο στις Κεντρικές Υπηρεσίες όσο και στα Περιφερειακά Υποκ/τα .Οι Κεντρικές Υπηρεσίες τηρούν τα master files των δεδομένων και συγκεντρωτικά στοιχεία.

Συγχρόνως το τ.ΙΚΑ-ΕΤΑΜ είχε την εποπτεία και τον έλεγχο της εταιρείας «ΚΕΝΤΡΟ ΗΛΕΚΤΡΟΝΙΚΟΥ ΥΠΟΛΟΓΙΣΤΗ ΚΟΙΝΩΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ» (Κ.Η.Υ.Κ.Υ) με σκοπό τον εκσυγχρονισμό και την ψηφιοποίηση των φορέων κοινωνικής ασφάλισης η οποία εντάχθηκε στις διατάξεις των φορέων του Δημοσίου. Στην συνέχεια καταργήθηκε η εταιρεία αυτή και την διαδέχθηκε η «Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης» (Η.ΔΙ.Κ.Α. Α.Ε.) η οποία ανέλαβε έργα πληροφορικής και επικοινωνιών των Φορέων Κοινωνικής Ασφάλισης καθώς και τις επεκτάσεις τους. Το 2008 με την θέσπιση της ασφαλιστικής μεταρρύθμισης δίδεται στην Η.ΔΙ.Κ.Α ο ρόλος της χορήγησης του Αριθμού Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ).

Επίσης μέσω συστήματος «ΑΤΛΑΣ» το 2014 θεσμοθετήθηκε η διαδικασία συγκέντρωσης και τήρησης των στοιχείων ασφάλισης και ασφαλιστικής ικανότητας όλων των ασφαλισμένων της χώρας μέσω της Η.ΔΙ.ΚΑ.Α.Ε

Ειδικότερα, με το σύγχρονο ολοκληρωμένο σύστημα της κοινωνικής ασφάλισης «ΑΤΛΑΣ»: • Συγκροτείται το Εθνικό Μητρώο Ασφαλισμένων στο οποίο καταγράφονται τόσο οι άμεσα όσο και οι έμμεσα ασφαλισμένοι.

• Συγκεντρώνεται για πρώτη φορά η ασφαλιστική ιστορία ανά

ασφαλισμένο δημιουργώντας έτσι τον Ψηφιακό Ατομικό Λογαριασμό Ασφάλισης, μια μορφή ηλεκτρονικού ασφαλιστικού «βιογραφικού».

- Συγκροτείται το Εθνικό Μητρώο Δικαιούχων περίθαλψης και καταργείται η θεώρηση των βιβλιαρίων.
- Ψηφιοποιείται και μηχανογραφείται όλο το κανονιστικό πλαίσιο της θεμελίωσης και απονομής συντάξεων.

Αποτελεί μηχανογραφική εφαρμογή που ενημερώνεται μόνο με αποστολή ασφαλιστικών στοιχείων από τους τέως Φορείς Κοινωνικής Ασφάλισης (νυν ΕΦΚΑ). **Λόγω εργασιών ανασχεδιασμού του συστήματος περιλαμβάνονται ασφαλιστικά στοιχεία από το 1994 μέχρι και το πρώτο τρίμηνο του 2016.** Το χρονικό διάστημα των ασφαλιστικών στοιχείων ενδέχεται να διαφέρει ανάλογα με την τελευταία ενημέρωση του συστήματος από τον εκάστοτε Ασφαλιστικό Φορέα. Ειδικότερα στο υπάρχον σύστημα έχει ενσωματωθεί ο χρόνος ασφάλισης για το τ.ΙΚΑ, τον τ.ΟΑΕΕ, το τ.ΕΤΑΑ, και τον τ.ΟΓΑ, ενώ για το τ.ΕΤΑΠ-ΜΜΕ το 70% περίπου του χρόνου ασφάλισης από τους δύο μεγαλύτερους τομείς του. Δεν έχει ενσωματωθεί χρόνος ασφάλισης για το τ.ΝΑΤ και το τ.Δημόσιο.

Από 01.01.2013 η Η.ΔΙ.Κ.Α. Α.Ε. ανέλαβε επίσης την δημιουργία του ενιαίου συστήματος Ελέγχου & Πληρωμών Συντάξεων-«Σύστημα ΗΛΙΟΣ», με το οποίο συγκέντρωσε για πρώτη τα φορά τα δεδομένα από 92 πληροφοριακά συστήματα των ασφαλιστικών φορέων για 4,5 εκατομμύρια συντάξεις και ταυτοποίησε 2,7 εκατομμύρια συνταξιούχους. Σύμφωνα με τη διαδικασία που προβλέπεται οι ΦΚΑ αποστέλλουν στην Η.ΔΙ.Κ.Α. Α.Ε ηλεκτρονικό αρχείο πληρωμών συντάξεων σε μηνιαία βάση με καταληκτική ημερομηνία την 10η ημέρα κάθε μήνα, στο οποίο περιέχονται αναλυτικά και ανά συνταξιούχο τα ποσά των συντάξεων που καταβάλει κάθε φορέας, ένδειξη εξαίρεσης από τις μειώσεις που προβλέπονται καθώς και περιοδικότητα καταβολής του ποσού της σύνταξης. Στη συνέχεια η Η.ΔΙ.Κ.Α ελέγχει την ορθότητα και την πληρότητα των στοιχείων που εμπεριέχονται στα αρχεία και πραγματοποιεί τους αναγκαίους υπολογισμούς παράγοντας τα τελικά αρχεία προς τη «ΔΙΑΣ». Παράλληλα, επεξεργάζεται στατιστικά τα δεδομένα τα οποία παρουσιάζονται αναλυτικά και με πλήρη διαφάνεια στις μηνιαίες εκθέσεις του Ενιαίου Συστήματος Ελέγχου & Πληρωμών Συντάξεων «ΗΛΙΟΣ» από τον Ιούνιο του 2013.

3.3 *Εφαρμογές στο υφιστάμενο ΟΠΣ e ΕΦΚΑ*

Στην παρούσα μεταβατική φάση, οι λειτουργίες του e ΕΦΚΑ σε επίπεδο Τεχνολογιών Πληροφορικής και Επικοινωνιών υλοποιούνται μετά από την επιλογή, τροποποίηση για τις ανάγκες του e ΕΦΚΑ, και εκμετάλλευση των πληρέστερων πληροφοριακών συστημάτων που προϋπήρχαν και λειτουργούσαν στους ΦΚΑ πριν την ένταξή τους στον ΕΦΚΑ, καθώς και των πληροφοριακών συστημάτων της ΗΔΙΚΑ ΑΕ.

Αναφέρονται ενδεικτικά:

Ενιαίο Μητρώο Ασφαλισμένων (εν ενεργεία και συνταξιούχων):

Πληροφοριακό σύστημα:

Διατηρούνται τα δημογραφικά στοιχεία των ασφαλισμένων σε λατινικά και ελληνικά

- Web Μητρώο: Εφαρμογή Μητρώου που χρησιμοποιείται στον ΕΦΚΑ, παράλληλα με τα Μητρώα των ενταχθέντων στον ΕΦΚΑ Φορέων κατά την μεταβατική περίοδο ομογενοποιώντας τα μητρώα του κάθε Τομέα (τέως Ταμείου).
- Διαχείριση όλου του μητρώου γίνεται από τις αντίστοιχες διευθύνσεις του ΕΦΚΑ μέσω της διαδικτυακής εφαρμογής του Ενιαίου Μητρώου Ασφαλισμένων ΕΦΚΑ
- Εξυπηρετητές βρίσκονται στην κεντρική υπολογιστική υποδομή της ΗΔΙΚΑ για λογαριασμό του ΕΦΚΑ

ΜΗΤΡΩΟ ΑΣΦΑΛΙΣΜΕΝΩΝ
Επιχειρησιακές Λειτουργίες
Εμφάνιση Στοιχείων Ασφαλισμένου
Έντυπα Μητρώου Ασφαλισμένων
Ε.Ε.
Ασφαλιστική Ικανότητα
Ασφαλιστική Ικανότητα Ανέργων
ΟΑΕΔ
Βεβαιώσεις Μητρώου
Ασφαλισμένων

Συντάξεις:

Πληροφοριακό σύστημα :

- στις υφιστάμενες διαδικασίες του ΟΠΣ του τ.ΙΚΑ-ΕΤΑΜ,
- ασφαλισμένοι του Δημοσίου, του τ.ΟΓΑ και του τ.ΝΑΤ εξυπηρετούνται από τα πληροφοριακά συστήματα των αντίστοιχων τ.ΦΚΑ.

- Μηνιαία διαδικασία εκκαθάρισης συντάξεων:
- Πληροφοριακά συστήματα ΟΠΣ-ΙΚΑ,
- Σύστημα Εκκαθάρισης ΟΑΕΕ,

- Σύστημα ΗΔΙΚΑ.

- Διαδικασία τελικής πληρωμής συντάξεων
- Μέσω του συστήματος ΕΣΕΠΣ/ΗΛΙΟΣ που διατηρεί η ΗΔΙΚΑ ΑΕ.

WORKFLOW
ΣΥΝΤΑΞΕΩΝ
Επιχειρησιακές
Λειτουργίες
Πρωτόκολλο Ροής
Εργασιών Συντάξεων
Εισερχόμενο Πρωτόκολλο
Εξερχόμενο Πρωτόκολλο
Διαχείριση Εργασιών

ΚΕΠΑ:

Πληροφοριακό σύστημα :

- στις υφιστάμενες διαδικασίες του ΟΠΣ του τ.ΙΚΑ-ΕΤΑΜ

ΚΕ.Π.Α.
Επιχειρησιακές Λειτουργίες
Διαχείριση Μητρώου Αιτούντων
Πιστοποίησης
Υγειονομικές Επιτροπές
Μητρώο Ιατρών
Πλάνο Εργασιών ΚΕΠΑ
Αιτήσεις Πιστοποίησης Αναπηρίας
Αποφάσεις Πιστοποίησης Αναπηρίας
Διαχείριση Ενστάσεων
ΚΑΤ' ΟΙΚΟΝ ΦΡΟΝΤΙΔΑ
ΣΥΝΤΑΞΙΟΥΧΩΝ
Επιχειρησιακές Λειτουργίες
Αίτηση συμμετοχής Παρόχου
Έλεγχος δικαιολογητικών-κριτηρίων
Συμβάσεις
Αίτηση Συμμετοχής Ωφελούμενου
Έλεγχος Κριτηρίων Ωφελούμενου
Δήλωση Παροχής Υπηρεσιών
Εκκαθάριση Δήλωσης

Παροχές
Πληροφορικό Σύστημα

- Παροχών που υπήρχαν και λειτουργούσαν στους Φορείς που εντάχθηκαν στον ΕΦΚΑ. Η συγκεκριμένη διαδικασία θα εξακολουθήσει να υφίσταται μέχρι τη θέσπιση Ενιαίου Κανονισμού Ασφάλισης και Παροχών του ΕΦΚΑ και τη δημιουργία αντίστοιχου πληροφοριακού συστήματος.

Επιχειρησιακές Λειτουργίες
Έξοδα Κηδείας
Επίδομα Ασθενείας
Επίδομα Μητρότητας

Δώρου Επιδόματος
Ατύχημα - Επαγγελματική Ασθένεια
Αναδρομικά
Καταλογισμός

Εισφορές Μισθωτών-Απογραφή Εργοδοτών

Πληροφοριακό σύστημα:

- Μηχανογραφικά από το ΟΠΣ του τ.ΙΚΑ-ΕΤΑΜ και ειδικότερα από την υπηρεσία υποβολής των Αναλυτικών Περιοδικών Δηλώσεων (ΑΠΔ).

ΕΙΣΦΟΡΕΣ
Επιχειρησιακές Λειτουργίες
Μητρώο Εργοδοτών Κοινών Επιχειρήσεων
Μητρώο Οικοδομοτεχνικών Έργων
Μητρώο Ειδικών Κατηγοριών Ασφάλισης
ΑΠΔ
Έλεγχος Δηλωθέντων Καταβληθέντων
Ουσιαστικός Έλεγχος Εργοδοτών
Ασφαλιστική Ενημερότητα
Καταγγελία Ασφαλισμένου
Πράξεις Επιβολής
Έντυπα Εισφορών ΕΕ
Οικονομικές Κινήσεις Εργοδοτών
Διαχείριση ασφαλιστικής Ιστορίας
Διαχείριση Αποφάσεων Εισφορών
Ασφάλιση Ειδικών Κατηγοριών
Εργόσημο
Είσπραξη Τρεχουσών Εισφορών
Προαιρετική Ασφάλιση
Αναγνώριση Χρόνου Ασφάλισης
Εκθέσεις Επιτόπιων Ελέγχων

Σύστημα Κέντρου Είσπραξης Ανεξόφλητων Οφειλών

- Πρόκειται για το μηχανογραφικό σύστημα που υποστηρίζει τις επιχειρησιακές ανάγκες λειτουργίας του ΚΕΑΟ.

ΚΑΘΥΣΤΕΡΟΥΜΕΝΕΣ ΕΙΣΦΟΡΕΣ – ΟΦΕΙΛΕΣ –
Κ.Ε.Α.Ο.
Επιχειρησιακές Λειτουργίες
Μητρώο Οφειλετών
Οικονομικές Κινήσεις Οφειλέτη
Ρυθμίσεις Οφειλών
Παραγραφόμενες – Παραγραμμένες Οφειλές
Είσπραξη Καθυστερούμενων Οφειλών
Εισπράξεις μέσω Ηλεκτρονικών Κατασχέσεων
Είσπραξη Δόσεων Ρύθμισης
Βεβαίωση Οφειλών
Ατομικές Ειδοποιήσεις
Μηνύσεις –‘Ενδικα Μέσα

Εισφορές Μη Μισθωτών:

Πληροφοριακό Σύστημα:

- Ο υπολογισμός των εισφορών των μη μισθωτών βασίστηκε στην αναβάθμιση του Πληροφοριακού Συστήματος του τ.ΟΓΑ που αναπτύσσει και συντηρεί η ΗΔΙΚΑ ΑΕ.

Ιστότοπος και ηλεκτρονικές υπηρεσίες

- Ο διαδικτυακός τόπος του τ.ΙΚΑ-ΕΤΑΜ ο οποίος δημιουργήθηκε το 2002 δεν ήταν μία συνηθισμένη ιστοσελίδα ενημερωτικού/πληροφοριακού χαρακτήρα, αλλά μία ολοκληρωμένη πλατφόρμα παροχής ηλεκτρονικών υπηρεσιών προς τους πολίτες και διάφορους φορείς. 'Ηταν ένας αυτόνομος ιστότοπος και δεν φιλοξενούνταν από κάποιο πάροχο σχετικών υπηρεσιών. Αυτό σήμαινε εγκατάσταση και λειτουργία συστοιχίας server επαρκούς ισχύος για ταυτόχρονη εξυπηρέτηση μεγάλου αριθμού πιστοποιημένου χρηστών (εργοδότες και ασφαλισμένοι).

  Πλέον έχει μετονομαστεί και λειτουργεί ο ιστότοπος του ΕΦΚΑ (**www.efka.gov.gr**), για την εξυπηρέτηση των πολιτών στον οποίο παρέχονται επί 24ώρου βάσεως ενημερωτικές πληροφορίες και ηλεκτρονικές υπηρεσίες. Ταυτόχρονα, υπάρχουν παραπομπές σε ηλεκτρονικές υπηρεσίες των πρώην ΦΚΑ και της ΗΔΙΚΑ, οι οποίες δεν έχουν ακόμα μεταφερθεί στις υποδομές του ΕΦΚΑ. Το Έργο εκτελείται ήδη με την μορφή Σύμβασης Παροχής Υπηρεσιών Συμφωνημένου επιπέδου (S.L.A), με αντικείμενο την Υλοποίηση ενός VPN δικτύου πολλαπλών υπηρεσιών (διακίνηση δεδομένων, φωνής και εικόνας) σε 362 Σημεία Εγκατάστασης, την Λειτουργία, Συντήρηση και Διαχείριση αυτού. Το δίκτυο συνδέει όλες τις Διοικητικές Μονάδες του ΕΦΚΑ Μισθωτών (Περιφερειακές, Τοπικές, Παραρτήματα) με τις Κεντρικές Υπηρεσίες του e-ΕΦΚΑ. Το δίκτυο είναι τεχνολογίας IP-VPN.
- Επίσης για την 24ωρη τηλεφωνική εξυπηρέτηση λειτουργεί η γραμμή 1555 η οποία εξυπηρετεί και ως οδηγός του πολίτη σε ιστότοπο (https://ticketing.1555.gov.gr/odigosUI/). Εδώ υποβάλλονται ηλεκτρονικά ερωτήματα για θέματα αρμοδιότητας του Υπουργείου Εργασίας και των εποπτευόμενων φορέων.[46][47]

[46] https://www.pagenews.gr/2022/01/30/oikonomia/efka-pente-aksones-pou-allazoun-to-epipedo-ton-parexomenon-ypiresion-tou-infographic/

3.4. ***Επιγραμματικά και ενδεικτικά παρατίθενται κάποιες από τις δράσεις οι οποίες είναι σε εξέλιξη και σχετίζονται άμεσα με τη λειτουργία των συστημάτων του ΕΦΚΑ*** :

- Παροχή υπηρεσιών συμφωνημένου επιπέδου (S.L.A) υποστήριξης παραγωγικής λειτουργίας του ***«Υφιστάμενου ΟΠΣ ΕΦΚΑ»***, των παρεχόμενων ηλεκτρονικών υπηρεσιών μέσω διαδικτύου προς τους πολίτες και φορείς, καθώς και παροχή υπηρεσιών συναφών έργων
- Παροχή τηλεπικοινωνιακών υπηρεσιών συμφωνημένου επιπέδου (SLA) μετάδοσης δεδομένων, φωνής και εικόνας μέσω ιδιωτικού ιδεατού δικτύου
- Εφαρμογή πολιτικής ασφάλειας τ. ΙΚΑ-ΕΤΑΜ
- Αντικατάστασης της κεντρικής υπολογιστικής υποδομής και εκσυγχρονισμού του περιφερειακού εξοπλισμού
- Καταπολέμηση της Εισφοροδιαφυγής και Εισφοροαποφυγής
- Ανάπτυξη συστημάτων και εφαρμογών, υπηρεσίες ψηφιοποίησης, παροχή ηλεκτρονικών υπηρεσιών για την υποστήριξη της άμεσης απονομής σύνταξης
- Διαγωνιστική διαδικασία για την υλοποίηση του **νέου Ολοκληρωμένου Πληροφοριακού Συστήματος** του Ενιαίου Φορέα Κοινωνικής Ασφάλισης, το οποίο θα καλύπτει Μισθωτούς και Μη Μισθωτούς. (Από εδώ και στο εξής θα αναφέρεται σαν «***ΟΠΣ - ΕΦΚΑ***»)
- Ψηφιοποίηση ασφαλιστικού χρόνου
- Διασύνδεση του ΕΦΚΑ στο Ευρωπαϊκό Σύστημα Ηλεκτρονικής Ανταλλαγής Πληροφοριών για την Κοινωνική Ασφάλιση (EESSI)
- **Πλατφόρμα τηλεκπαίδευσης (e-learning)**

  Ο ΕΦΚΑ διαθέτει πλατφόρμα τηλεκπαίδευσης η οποία αποτελείται από 2 επιμέρους συστήματα:

  Σύστημα ασύγχρονης τηλεκπαίδευσης

  Πρόκειται για εγκατάσταση της ανοικτής πλατφόρμας **Open eClass** (http://www.openeclass.org) σε υποδομές του ΕΦΚΑ Η εν λόγω πλατφόρμα αποτελεί ένα ολοκληρωμένο σύστημα διαχείρισης ηλεκτρονικών μαθημάτων.

---

47 https://www.skai.gr/news/greece/kseperasan-to-1-ekatommyrio-oi-apantimenes-kliseis-sto-1555

Η πλατφόρμα Open eClass είναι συμβατή με διεθνή πρότυπα (SCO IMSCP) με τα οποία εξασφαλίζεται η επαναχρησιμοποίηση, η προσβασιμότητα και η ανθεκτικότητα του εκπαιδευτικού υλικού στις τεχνολογικές μεταβολές, καθώς και η διαλειτουργικότητα μεταξύ συστημάτων ηλεκτρονικής μάθησης.

Σύστημα σύγχρονης τηλεκπαίδευσης

Πρόκειται για εγκατάσταση της πλατφόρμας ανοικτού λογισμικού BigBlueButton (http:/www.bigbluebutton.org/) σε υποδομές του ΕΦΚΑ. Η εν λόγω πλατφόρμα προσφέρει τη δυνατότητα άμεσης web-based επικοινωνίας εκπαιδευτών και εκπαιδευόμενων. Η εφαρμογή εκτελείται απευθείας από τον πλοηγό διαδικτύου, ενώ για την αξιοποίηση του συνόλου των δυνατοτήτων της πλατφόρμας, χρησιμοποιείται επιπρόσθετος εξοπλισμός από το τελικό χρήστη (headphones, web κάμερα).

- **Ασφαλής Διάταξη Δημιουργίας Υπογραφής / Κεντρικό ΑΔΔΥ**

  Πρόκειται για την ασφαλή διάταξη ARX Cosign Central FIPS v 7.1, η οποία έχει πιστοποιηθεί κατά ETSI TS 14167-5/Common Criteria EAL4+ καθώς και από την ΕΕΤΤ ότι καλύπτει τις απαιτήσεις των ασφαλών διατάξεων δημιουργίας υπογραφής.

  Η εν λόγω διάταξη έχει τα εξής ελάχιστα χαρακτηριστικά απόδοσης & ασφάλειας:

- Υποστήριξη μέχρι 270 ψηφιακών υπογραφών/sec με κλειδιά 1024 bit
- Εξυπηρέτηση 10.000 χρηστών / Ασφαλή Διάταξη
- Υποστήριξη κλειδιών μήκους 4096 bit
- Υποστήριξη ψηφιακής υπογραφής εγγράφων χωρίς να απαιτείται χρήση άλλων εφαρμογών
- Υποστήριξη της δυνατότητας απομακρυσμένης διασύνδεσης με την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ-ΕΡΜΗΣ).

  Το κεντρικό ΑΔΔΥ παρέχει μία προγραμματιστική διεπαφή CoSign Signature API (SAPI) που παρέχει υπηρεσίες ψηφιακής υπογραφής και λειτουργικότητα διασύνδεσης με εξωτερικά συστήματα και εφαρμογές. Οι προγραμματιστές μπορούν να χρησιμοποιήσουν το SAPI για να ολοκληρώσουν την υποστήριξη ψηφιακών υπογραφών σε προσαρμοσμένες διαδικασίες, εσωτερικά ανεπτυγμένες εφαρμογές, και την ενσωμάτωση του CoSign με τρίτες εφαρμογές, συστήματα και υπηρεσίες καταλόγου. Το SAPI παρέχει την

λειτουργικότητά του σε τρεις τύπους διεπαφών προγραμματισμού:

- C/C++ βιβλιοθήκες για εφαρμογές Microsoft Windows
- COM Objects για προγραμματισμό σε περιβάλλον Microsoft
- Web Services

Στο κεντρικό ΑΔΔΥ βρίσκονται αποθηκευμένα αναγνωρισμένα ψηφιακά πιστοποιητικά για τους υπαλλήλους του e-ΕΦΚΑ, τα οποία έχουν εκδοθεί από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ-ΕΡΜΗΣ). Η διαχείριση χρηστών στο κεντρικό ΑΔΔΥ έχει ολοκληρωθεί με τη διαχείριση χρηστών του e-ΕΦΚΑ (χρήστες εφαρμογής ΟΠΣ Μισθωτών και χρήστες της εφαρμογής ηλεκτρονικών καταθέσεων εις χείρας πιστωτικών ιδρυμάτων).

- **Πλατφόρμα αυθεντικοποίησης με κωδικό πρόσβασης μιας χρήσης (OTP)**

Πρόκειται για την πλατφόρμα Lin OTP v2.8, η οποία επικοινωνεί με το Κεντρικό ΑΔΔΥ μέσω του τυποποιημένου πρωτόκολλου RADIUS, παρέχοντας τη δυνατότητα επέκτασης της πιστοποίησης χρηστών του Cosign με χρήση Two Factor Authentication – One Time Passwords (OTP) – Κωδικός Πρόσβασης Μιας Χρήσης.Για το CoSign Central-FIPS που είναι μια πλατφόρμα κεντρικού εξυπηρετητή ψηφιακών υπογραφών, ο υψηλού επιπέδου έλεγχος ταυτότητας του υπογράφοντος είναι ένας βασικός παράγοντας για την ασφάλεια του όλου συστήματος. Για το λόγο αυτό ο μηχανισμός ταυτοποίησης βασίζεται σε δυο παράγοντες:

1. ένα κωδικό Πρόσβασης μιας χρήσης που παράγεται από μια συσκευή που έχει στην κατοχή του ο χρήστης, π.χ. μια συσκευή παραγωγής κωδικών (OTP hardware token) ή μια εφαρμογή στο κινητό του τηλέφωνο
2. κάποια πληροφορία που γνωρίζει ο χρήστης όπως π.χ. τα στοιχεία πρόσβασης (credentials) σε ένα πληροφοριακό σύστημα.

Μόνο η επιτυχής επικύρωση των δύο στοιχείων παρέχει επαρκείς εγγυήσεις για την ταυτότητα του τελικού χρήστη.

- **Λογισμικό Ανάλυσης Επικινδυνότητας**

Έχει υλοποιηθεί υποδομή Risk Analysis, Business Intelligence και Datawarehouse η οποία αποτελείται από τα ακόλουθα δομικά συστατικά:

- RDBMS Oracle Έκδοση 11g Enterprise Edition
- Oracle Web Logic Suite
- Oracle Business Intelligence Suite

- ESKORT RISK Analysis Engine (υποσύστημα του ESKORT Selection Module
  - **Λογισμικό Ανίχνευσης Ιομορφών**
- Trust Port Antivirus
  Είναι εγκατεστημένο σε θέσεις εργασίας (PC).
  - **Λογισμικό Firewall**
- VPN-1 Enterprise Center[48] [49]

3.5 *ΥΦΙΣΤΑΜΕΝΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ e ΕΦΚΑ*

Δεν έχει κοινοποιηθεί επίσημη πολιτική ασφαλείας στους υπαλλήλους του e ΕΦΚΑ οπότε δεν γνωρίζουμε εάν υπάρχει.

Μετά από τηλεφωνική επικοινωνία με το τμήμα ασφάλειας συστημάτων και εφαρμογών της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνίας ενημερωθήκαμε ότι η πολιτική ασφαλείας του οργανισμού είναι απόρρητη.

Αναφέρουμε τα μέτρα ασφαλείας τα οποία γνωρίζουμε καθώς χρησιμοποιούνται καθημερινά.

3.5.1 *Ασφάλεια Περιμέτρου*

Ένα από τα μέσα προστασίας που εφαρμόζονται στο υφιστάμενο ΟΠΣ ΕΦΚΑ είναι το σύστημα firewall ο μηχανισμός «περιμετρικής άμυνας» που ελέγχει την πρόσβαση στο δίκτυο του ΙΚΑΝΕΤ.

3.5.2 *Κωδικοί ασφαλείας στα συστήματα*

Κάθε υπάλληλος έχει κωδικό πρόσβασης για τα πληροφοριακά συστήματα και συγκεκριμένους ρόλους αντίστοιχα με το αντικείμενο του. Οι κωδικοί πρόσβασης δεν έχουν ελάχιστο ή συγκεκριμένο αριθμό χαρακτήρων, δεν εφαρμόζεται χρήση ισχυρών κωδικών πρόσβασης

3.5.3 *Μεταφορά αρχείων*

48 Παροχή Υπηρεσιών Συμφωνημένου Επιπέδου (SLA) για υπηρεσίες Υποστήριξης Παραγωγικής Λειτουργίας, Διαχείρισης Έργου-Διασφάλισης Ποιότητας, Ασφάλειας σε Συστήματα του e-ΕΦΚΑ και Υπεύθυνου Ασφάλειας, Συντήρησης Λογισμικού Εφαρμογών, On-demand Συμβουλευτικές/Υποστηρικτικές Υπηρεσίες των Πληροφοριακών Συστημάτων

49 Ανοικτά Δεδομένα από e ΕΦΚΑ. Σχέδιο Διακήρυξη Ανοικτού Διαγωνισμού

Δεν υπάρχει δυνατότητα μεταφοράς αρχείων σε υπολογιστές με το υφιστάμενο σύστημα ΟΠΣ ΕΦΚΑ και δεν προβλέπεται διατήρηση αντιγράφων ασφαλείας από τους υπαλλήλους

3.5.4 *Διεύθυνση Ασφάλειας Πληροφοριακών Συστημάτων*

Στην Κεντρική Διεύθυνση υπάρχει Τμήμα Ασφαλείας Συστημάτων και εφαρμογών και υπεύθυνος ασφαλείας DPO καθώς και στις Διευθύνσεις έχει ορισθεί Υπεύθυνος Ασφαλείας

3.5.5 *Διαχείριση email*

Διαχείριση e mail μέσω corpmail σε υπολογιστή που δεν λειτουργεί ΟΠΣ.

Συχνή ενημέρωση και οδηγίες σε σχέση με την διακίνηση κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου και ασφαλή χρήση ηλεκτρονικής αλληλογραφίας.

3.5.6. *Ψηφιακή Υπογραφή*

Ακόμα δεν υπάρχει δυνατότητα ψηφιακής υπογραφής

3.6 *ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΑΛΛΩΝ ΦΟΡΕΩΝ*

Καθημερινά διαβάζουμε δημοσιεύματα τα οποία ονοματίζουν τον e ΕΦΚΑ ως τον φορέα με τα περισσότερα προβλήματα στην ηλεκτρονική διακυβέρνηση[50].

Ο e ΕΦΚΑ είναι ένας οργανισμός που έχει 1,1 εκατομμύρια συναλλαγές online ημερησίως ενώ στοχεύει στον ολοκληρωτικό μετασχηματισμό του.

Πολλά δημοσιεύματα κάνουν λόγο για διαπιστωμένα κενά ασφαλείας στον e ΕΦΚΑ [51]αλλά εξίσου πολλά δημοσιεύματα θίγουν το θέμα τα κυβερνοασφάλειας και σε άλλους φορείς σε ιδιωτικό και δημόσιο φορέα[52] με τελευταίο παράδειγμα στην Ελλάδα τα ΕΛΤΑ[53] και προγενέστερο την ίδια την Βουλή[54].

---

[50] https://www.antinews.gr/action.read/ellada/i-aristi-metatropi-tou-efka-se-upiresia-koinonikis-anaisthisias/4.157063

[51] https://ictplus.gr/sti-bouli-fernei-o-syriza-p-s-ypothesi-kenon-asfaleias-sta-pliroforiaka-systimata-e-efka-kai-ypourgeiou-psifiakis-diakybernisis/?fbclid=IwAR3F5gPd0RQKoCDE1dbYBVgPpV939Hlgpd8yxBNRC28-hTvGYx3akLoYUSo

[52] https://gr.rua.gr/2022/01/21/%CF%87%CE%AC%CE%BA%CE%B5%CF%81-%CE%B5%CF%80%CE%B9%CF%84%CE%AD%CE%B8%CE%B7%CE%BA%CE%B1%CE%BD-%CF%83%CE%B5-%CF%84%CF%81%CE%AF%CE%B1-%CE%BD%CE%BF%CF%83%CE%BF%CE%BA%CE%BF%CE%BC%CE%B5%CE%AF%CE%B1-%CF%84/

[53] https://iguru.gr/elta-dothike-anakoinosi-gia-ton-tropo-tis-kyvernoepithesis/?feed_id=2119&_unique_id=6239719e4a483&fbclid=IwAR3GOBZSnFBYI74pBk7AJ-y8L_TayOeAsDOWBGBHmBqKwHa4K4PDkiJeZaM

Το ίδιο συμβαίνει και σε χώρες του εξωτερικού με πρόσφατο παράδειγμα την μαζική κυβερνοεπίθεση σε ιστοτόπους και τράπεζες στην Ουκρανία λίγο πριν την εισβολή της Ρωσίας[55].

Τα κενά ασφαλείας και η αντιμετώπιση των απειλών είναι ένα σύνθετο παγκόσμιο πρόβλημα το οποίο αναζητά άμεσες λύσεις. Επειδή οι κίνδυνοι συνεχώς αυξάνονται και εξελίσσονται η πολιτική ασφαλείας σε κάθε δυναμικό οργανισμό θα έπρεπε να είναι μία αναγκαία συνθήκη και γι'αυτό να εφαρμόζονται αυστηρότεροι κανονισμοί. Πολλές υπηρεσίες έχουν λάβει υπόψη τους τα συχνά φαινόμενα των κυβερνοαπειλών και έχουν εντάξει στην πολιτική τους κανονισμούς και συνεχής ενημερώσεις προκειμένου να αφυπνίσουν τους υπαλλήλους και να προστατεύσουν τους πολίτες. 'Ενα τέτοιο παράδειγμα μας δίνει η ΑΑΔΕ στην πλατφόρμα της υπηρεσίας της που μας παρέχει χρήσιμες συμβουλές οπότε αντιλαμβανόμαστε ότι η συγκεκριμένη υπηρεσία έχει αξιολογήσει τους ορατούς και σοβαρούς κινδύνους που απειλούν την ασφάλεια των πληροφοριακών της συστημάτων και αυτό εκφράζεται.

https://www.aade.gr/menoy/aade/asfaleia-ilektronikon-ypiresion

Την αξιοσημείωτη αυτή προσπάθεια θα μπορούσαν να υιοθετήσουν και άλλοι φορείς όπως ο e ΕΦΚΑ.

Ενδεικτικά αναφέρουμε κάποια από τα μέτρα που αναφέρονται στην πλατφόρμα:

- Να συνδέεστε με τον επίσημο διαδικτυακό τόπο της Α.Α.Δ.Ε. πληκτρολογώντας απευθείας την ηλεκτρονική διεύθυνση www.aade.gr στον φυλλομετρητή σας (browser), και όχι μέσω συνδέσμων (links) που πιθανόν σας έχουν αποσταλεί ηλεκτρονικά ή έχουν δημοσιευτεί σε ιστοσελίδες τρίτων.
- Όταν κάνετε login στην ιστοσελίδα μιας ηλεκτρονικής υπηρεσίας της Α.Α.Δ.Ε. όπου σας ζητείται να συμπληρώσετε τον λογαριασμό χρήστη (Username) καθώς και τον προσωπικό σας κωδικό πρόσβασης (Password), να ελέγχετε αν η διεύθυνση αρχίζει με https (αντί του http) και υπάρχει εικονίδιο με λουκέτο. Με διπλό κλικ στο λουκέτο, θα εμφανιστούν πληροφορίες που θα σας βοηθήσουν να επιβεβαιώσετε ότι η ιστοσελίδα είναι γνήσια.
- Αφού ολοκληρώσετε τις ενέργειές σας να αποσυνδέστε από τη σελίδα (επιλέγοντας «Αποσύνδεση») πριν την εγκαταλείψετε.

---

[54] https://www.kathimerini.gr/politics/561680272/epithesi-chakers-sti-voyli/

[55] https://www.kathimerini.gr/world/561733171/oykrania-maziki-kyvernoepithesi-se-kyvernitikoys-istotopoys-kai-trapezes/

- Κατά την επιλογή password: Επιλέξτε συνδυασμό γραμμάτων, αριθμών και συμβόλων στο password σας και αποφύγετε τη χρήση απλών λέξεων. Επιπλέον, αποφύγετε τη χρήση σειράς ίδιων χαρακτήρων (π.χ.g177777) ή χαρακτήρων με κάποια λογική συνέχεια (π.χ. 123456, abcde).
- Επιλέξτε μια φράση που μόνο εσείς γνωρίζετε και αποφύγετε τη δημιουργία password με στοιχεία που σας ταυτοποιούν όπως το όνομά σας, η ημερομηνία γέννησης, ο αριθμός ταυτότητας ή το ΑΦΜ σας.

Επίσης η ΑΑΔΕ αφού έχει μεριμνήσει για την πολιτική ασφαλείας των ΠΣ συγχρόνως έχει αναπτύξει και την διαλειτουργικότητα των συστημάτων της https://www.aade.gr/sites/default/files/2020-10/ATT01682.pdf ως αναφέρεται στο link.

Θα μπορούσαμε να πούμε με βεβαιότητα ότι η ΑΑΔΕ ως υποδειγματική υπηρεσία θα έπρεπε να μεταδώσει-μεταφέρει την τεχνογνωσία και στο υπόλοιπο δημόσιο.

3.7 *Ενδεικτικά Δημοσιεύματα από Κυβερνοαπειλές*

«Τα δεδομένα αυτά δείχνουν ότι ένα σημαντικό ποσοστό καταναλωτών έχουν πληρώσει λύτρα για τα δεδομένα τους τελευταίους 12 μήνες. Αλλά η παράδοση χρημάτων δεν εγγυάται την επιστροφή δεδομένων και ενθαρρύνει μόνο τους εγκληματίες του κυβερνοχώρου να συνεχίσουν την πρακτική αυτή. Επομένως, συνιστούμε πάντα εκείνοι που επηρεάζονται από ransomware να μην πληρώνουν, καθώς τα χρήματα υποστηρίζουν τη συνέχιση της συγκεκριμένης πρακτικής. Αντ' αυτού, οι καταναλωτές πρέπει να φροντίζουν να επενδύουν στην αρχική προστασία και ασφάλεια για τις συσκευές τους και να δημιουργούν αντίγραφα ασφαλείας όλων των δεδομένων τους τακτικά. Αυτό θα κάνει την ίδια την επίθεση λιγότερο ελκυστική ή επικερδή για τους εγκληματίες στον κυβερνοχώρο, μειώνοντας τη χρήση της πρακτικής και παρουσιάζοντας ένα ασφαλέστερο μέλλον για τους χρήστες του διαδικτύου».[56]

«Στις κυβερνοεπιθέσεις Τούρκων και Ελλήνων χάκερ με φόντο τη διαμάχη για το φυσικό αέριο αναφέρεται ο γερμανικός τύπος. Ήταν μια επίθεση τεραστίων διαστάσεων, αυτό πρέπει κανείς να το παραδεχθεί. Την Κυριακή οι ιστοσελίδες του

[56] https://www.asfalisinet.gr/%CF%84%CE%B1-%CE%BC%CE%B9%CF%83%CE%AC-%CE%B8%CF%8D%CE%BC%CE%B1%CF%84%CE%B1-ransomware-%CF%80%CE%BB%CE%AE%CF%81%CF%89%CF%83%CE%B1%CE%BD-%CE%BB%CF%8D%CF%84%CF%81%CE%B1-%CE%B3%CE%B9%CE%B1-%CE%B1%CE%BD/

υπ. Εξωτερικών και της Βουλής στην Αθήνα δεν ήταν διαθέσιμες. Δύο μέρες νωρίτερα, Τούρκοι χάκερ ανέφεραν ότι χάκαραν αυτές τις ιστοσελίδες, όπως επίσης και εκείνη της ελληνικής μυστικής υπηρεσίας αλλά και του Χρηματιστηρίου Αθηνών. Ο λόγος για την επίθεση των Τούρκων πολεμιστών του κυβερνοχώρου, οι οποίοι αποκαλούν τους εαυτούς τους σε σελίδα του facebook 'Στρατιώτες του Φοίνικα' είναι η διαμάχη γύρω από τα δικαιώματα γεωτρήσεων για φυσικό αέριο στην ανατολική Μεσόγειο» αναφέρει εκτενές ρεπορτάζ της Süddeutsche Zeitung»[57]

«Σύμφωνα με έκτακτη ενημέρωση που έγινε σήμερα το απόγευμα, το ύποπτο περιστατικό έγινε χθες, Πέμπτη, το μεσημέρι. «Στις 20 Ιανουαρίου 2021 μεσημβρινές ώρες η Διεύθυνση Πληροφορικής διαπίστωσε ότι ήταν σε εξέλιξη προσπάθεια απόκτησης πρόσβασης σε λογαριασμούς του ηλεκτρονικού ταχυδρομείου της Βουλής από εξωτερική IP», σημειώνεται χαρακτηριστικά από κοινοβουλευτικές πηγές.
Αμέσως μόλις έγινε αντιληπτή η κακόβουλη προσπάθεια, «διακόπηκε η λειτουργία του web mail των χρηστών για την προστασία τους και ενημερώθηκαν οι αρμόδιες εποπτικές αρχές». Οι ίδιες πηγές αναφέρουν ότι «η Διεύθυνση Πληροφορικής είναι σε άμεση και στενή συνεργασία με τις αρμόδιες Αρχές προκειμένου να αποτιμηθεί το περιστατικό».[58]

ΚΕΦΑΛΑΙΟ 4ο

ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ

4.1 *Σκοπός και ερευνητικά ερωτήματα*

Ο σκοπός της έρευνας είναι να μελετήσουμε την άποψη των υπαλλήλων του ΕΦΚΑ, από όποια θέση εργάζονται και από όποιο τμήμα της υπηρεσίας, για τα πληροφοριακά συστήματα που χρησιμοποιούν όσον αφορά την διαλειτουργικότητα και την ασφάλεια των δεδομένων αλλά και την αποτελεσματικότητα τους σε μία προσπάθεια να εντοπίσουμε τις αιτίες των προβλημάτων.
Διενεργούμε αυτή την μελέτη επειδή θεωρούμε ότι το ανθρώπινο δυναμικό που στελεχώνει τον φορέα θα βοηθήσει σε μια ποιοτική έρευνα για αξιοπρόσεκτα

[57] https://www.protothema.gr/greece/article/966715/suddeutsche-zeitung-polemos-haker-sto-aigaio/

[58] https://www.kathimerini.gr/politics/561680272/epithesi-chakers-sti-voyli/

συμπεράσματα εκφράζοντας προσωπική άποψη και μεταφέροντας την καθημερινή του εμπειρία.

Τα ερευνητικά μας ερωτήματα εστιάζουν στην λειτουργικότητα των πληροφοριακών συστημάτων, στην διασύνδεσή τους, στην ασφάλεια και γενικότερα στην αξιολόγηση της υφιστάμενης κατάστασης.

Χρησιμοποιούμε την ποιοτική έρευνα αντλώντας πληροφορίες για τον τρόπο διεξαγωγής της από το βιβλίο Ισαρη Φ.- Μπουρκός Μ. (2015) Ποιοτική Μεθοδολογία Ερευνας Εκδόσεις Ελληνικά Συγράμματα.

4.2 *Τρόπος διεξαγωγής της έρευνας*

Η ποιοτική έρευνα «*βοηθά να αναπτύξουμε μια πιο σύνθετη, λεπτομερή περιγραφή και κατανόηση του υπό διερεύνηση ζητήματος. Τις λεπτομέρειες αυτές τις αποκτούμε με την άμεση επαφή με τα πρόσωπα της έρευνας καταγράφοντας τις ιστορίες τους, παρατηρώντας τη συμπεριφορά τους, εντοπίζοντας τις πρακτικές τους στα πλαίσια που ζουν και εργάζονται*».[59]

Με την ποιοτική έρευνα θα αντλήσουμε πληροφορίες για την πραγματική απεικόνιση της καθημερινότητας μέσα από προσωπικές ερμηνείες και εμπειρίες μίας πραγματικής διαχείρισης. *Οι ποιοτικοί ερευνητές, σύμφωνα με την Willing (2001), ενδιαφέρονται για το νόημα, για τον τρόπο που οι άνθρωποι βιώνουν τα γεγονότα.*

Μέσα από συνέντευξη με τους υπαλλήλους, από σημειώσεις και από παρατηρήσεις θα αναλυθούν τα ποιοτικά δεδομένα που θα αντλήσουμε.

Ορισμένοι ερευνητές εδράζονται στη διαισθητική ανίχνευση των συσσωρευμένων δεδομένων, κάποιοι άλλοι στη συστηματική και τυποποιημένη κωδικοποίηση και ανάλυσή τους στη βάση συγκεκριμένων τεχνικών (βλ. Strauss & Corbin, 1990)».

Τα ερευνητικά ερωτήματα προέκυψαν από τις προσωπικές καθημερινές δυσκολίες στο περιβάλλον της εργασίας, μέσα από ένα διαισθητικό προβληματισμό για την αναζήτηση των αιτιών και των λύσεων.

Η μεθοδολογία προσδιορίσθηκε από τον σκοπό της έρευνας και τις απαντήσεις που αναζητούνταν.

Οι Case και Light (2011), βασισμένοι στη διαλεκτική προσέγγιση της Cousin (2009), τονίζουν ότι η σχέση μεταξύ των ερευνητικών ερωτημάτων και της μεθοδολογίας δεν είναι συνήθως μονής κατεύθυνσης αλλά διπλής κατεύθυνσης. Θα μπορούσε κάποιος να

[59]'Ισαρη Φ.- Μπουρκός Μ. Ποιοτική (2015) Μεθοδολογία Ερευνας Εκδόσεις Ελληνικά Συγράμματα

ξεκινήσει με κάποιες ιδέες για το τι θα ήθελε να ερευνήσει, να εντοπίσει τη μεθοδολογία που είναι για την περίπτωση η πιο κατάλληλη και μετά να επιστρέψει πίσω στα ερευνητικά ερωτήματα για να τα εκλεπτύνει. Η διαδικασία μπορεί να επαναληφθεί όσες φορές χρειάζεται μέχρι που ο ερευνητής νιώσει ικανοποιημένος με το αποτέλεσμα.

Εργαλείο της έρευνας είναι οι ερωτήσεις, ο λόγος, η άποψη, η κατανόηση, η ανάλυση και το συμπέρασμα. Οι ερωτηθέντες δεν επηρεάστηκαν από τον ερευνητή ο οποίος υπήρξε απλός παρατηρητής και θα αξιολογήσει τις αντιδράσεις, την ποικιλία των απαντήσεων, την αξιοπιστία τους και την εγκυρότητά τους για να γενικεύσει σε συμπεράσματα.

Ο στόχος είναι μέσα από μία ουσιαστική και τεκμηριωμένη προσέγγιση του θέματος να υπάρξουν νέες πληροφορίες και να διαμορφωθεί ένα αδιαμφισβήτητο συμπέρασμα.

Έτσι, *λαμβάνοντας υπόψη τις ερμηνείες των ερευνητών, των αναγνωστών της έρευνας καθώς και των ίδιων των ερευνητικών υποκειμένων, μπορούμε να έχουμε μια καλύτερη ιδέα για την πολυπλοκότητα του ζητήματος και τις πολλαπλές αντιλήψεις που υπάρχουν γι' αυτό*.[60]

Η θεωρητική δειγματοληψία ήταν ο τρόπος που εξυπηρετούσε για την έρευνά μας καθώς «*ο ερευνητικός σχεδιασμός είναι πιο ευέλικτος, ανοιχτός και καθοδηγούμενος από τα ερευνητικά ερωτήματα, αποσκοπώντας στον εντοπισμό του φαινομένου και των διαστάσεών του. Στη συνέχεια τα δεδομένα συλλέγονται παράλληλα με την ανάλυση, καθώς η θεωρητική δειγματοληψία στοχεύει στο να αναζητήσει περιπτώσεις (ανθρώπους, καταστάσεις, πεδία γεγονότα) που θα επιτρέψουν στον ερευνητή είτε να αποσαφηνίσει και να ενισχύσει τις διαμορφούμενες θεωρητικές κατηγορίες είτε να τις διαφοροποιήσει αναδεικνύοντας νέες όψεις του υπο διερεύνηση φαινομένου (Coyne, 1997 Τσιώλης, 2014· Willig, 2008).*

Με αυτό τον τρόπο συλλέγοντας τα δεδομένα από τους υπαλλήλους-συναδέρφους συγχρόνως εξελισσόταν η έρευνα αντίστοιχα με τα δεδομένα και ολοκληρώθηκε όταν πλέον δεν υπήρχε κάποιο νέο στοιχείο που να προσφέρει στην αναζήτηση. Το μέγεθος του δείγματος υπήρξε αντίστοιχο αφού σύμφωνα με τη Marshall (1996: 523) «το κατάλληλο μέγεθος δείγματος για μια ποιοτική μελέτη είναι αυτό που απαντάει επαρκώς στην ερευνητική ερώτηση».

[60] [60]'Ισαρη Φ.- Μπουρκός Μ. Ποιοτική Μεθοδολογία Ερευνας (2015 Ελληνικά Συγράμματα)

4.3 ***Στοιχεία 'Ερευνας***

Χρόνος:από 08-03-2022 έως 18-03-2022

Χώρος:ΕΦΚΑ.

Δείγμα:8 υπάλληλοι

Α. ΘΕΣΕΙΣ ΕΥΘΥΝΗΣ: 2 άτομα

Β.ΥΠΑΛΛΗΛΙΚΗ ΣΧΕΣΗ: 6 άτομα

Ο οδηγός συνέντευξης περιλαμβάνει 15 κοινές ερωτήσεις :

1.Γνωρίζετε από πόσα πληροφοριακά συστήματα αποτελείται η πληροφοριακή υποδομή του e ΕΦΚΑ;

2.Γνωρίζετε ποιες ηλεκτρονικές υπηρεσίες παρέχονται από τον e ΕΦΚΑ μέσω διαδικτύου σε πολίτες, επιχειρήσεις και φορείς;

3.Ποιο πληροφοριακό σύστημα χειρίζεστε; από ποιο ταμείο;

4.Θεωρείτε ότι υπάρχει διαλειτουργικότητα ανάμεσα:

α)στα διαφορετικά πληροφοριακά συστήματα τουe ΕΦΚΑ;

β)στους φορείς του δημοσίου (π.χ.εφορία, δήμος, περιφέρεια κλπ);

5.Αντιμετωπίζετε συχνά τεχνικά προβλήματα στα πληροφοριακά συστήματα;Υπάρχει αρμόδιο τμήμα επίλυσης προβλημάτων για κάθε τμήμα;

6.Γνωρίζετε τι σημαίνει Κυβερνοασφάλεια;

7.Γνωρίζετε εάν υπάρχει πολιτική ασφαλείας στα πληροφοριακά συστήματα του e ΕΦΚΑ;

8.Εχετε ενημερωθεί για κάποια τεχνικά και οργανωτικά μέτρα που χρησιμοποιούνται στον e ΕΦΚΑ για την ασφάλεια και την εξασφάλιση της επιχειρησιακής συνέχειας των πληροφοριακών του συστημάτων;

9.Θεωρείτε ότι τα προσωπικά δεδομένα των πολιτών είναι ασφαλή;

10.Διαχειρίζεστε email από τον ίδιο υπολογιστή που συναλλάσσεστε με τους ασφαλισμένους;

11.Χρησιμοποιείτε ψηφιακή υπογραφή;

12.Εχει υπάρξει κάποια ενημέρωση ή εκπαίδευση που να αφορά την ασφάλεια των συστημάτων, την προστασία της ακεραιότητας και της διαθεσιμότητας των πληροφοριών, την προστασία των προς επεξεργασία και αποθηκευμένων προσωπικών δεδομένων;

13.Θα επιθυμούσατε να υπάρξει ενημέρωση και εκπαίδευση που να αφορά την ασφάλεια των πληροφοριακών συστημάτων που χειρίζεστε;

14.Θεωρείτε ότι η ανεπαρκής ενημέρωση και εκπαίδευση στα θέματα ασφάλειας των πληροφοριακών συστημάτων επηρεάζει την διαλειτουργικότητα και κατά συνέπεια την αποδοτικότητα των υπαλλήλων ;

15.Πιστεύετε ότι υπάρχει βελτίωση, εξέλιξη και εκσυγχρονισμός λειτουργιών και υποδομών του ΕΦΚΑ και κατ'επέκταση των πληροφοριακών συστημάτων;

16.Θα μπορούσατε να αναφέρετε οποιαδήποτε δική σας παρατήρηση, διαπίστωση και άποψη που θα βοηθούσε προκειμένου να διεξαχθούν κάποια ενδεικτικά συμπεράσματα για τα πληροφοριακά συστήματα του ΕΦΚΑ και την Κυβερνοασφάλεια;

4.4 ***Διαδικασία έρευνας***

Αρχικά ενημερώθηκαν όλοι οι υπάλληλοι - συμμετέχοντες για τον σκοπό της μελέτης, και ότι αυτή διεξάγεται στα πλαίσια διεξαγωγής μεταπτυχιακής διπλωματικής εργασίας στο Πανεπιστήμιο της Πάτρας.

Οι συμμετέχοντες έδωσαν προφορικά την συναίνεση τους για την συμμετοχή τους και ξεκίνησε η συνέντευξη για την οποία έχουν καταγραφεί οι απαντήσεις τους.

Οι συνεντεύξεις έγιναν στο χώρο εργασίας (ΕΦΚΑ) μετά την συναλλαγή με το κοινό, λόγω φόρτου εργασίας. Το υλικό που καταχωρήθηκε επεξεργάστηκε αργότερα για την ανάλυσή του. Η συμμετοχή τους ήταν εθελοντική και ανώνυμη και εξασφαλίστηκε η προστασία των προσωπικών τους δεδομένων .

4.5 ***Ανάλυση των δεδομένων***

Μέσω της ανάλυσης περιεχομένου, οι ερευνητές μπορούν να εξάγουν συμπεράσματα από το κείμενο που αναλύουν και να κάνουν υποκειμενική ανάλυση, με βάση τα όσα αντιλαμβάνονται οι ίδιοι ότι παρουσιάζει το κείμενο (Graneheim&Lundman, 2004).Η διαδικασία της ανάλυσης των συνεντεύξεων βασίστηκε στα 4 βήματα της ανάλυσης περιεχομένου όπως αναφέρονται από τον Τσιώλη (2018). Αρχικά καταχωρήθηκε η συνέντευξη, στη συνέχεια μελετήθηκαν συστηματικά οι απαντήσεις, ώστε η ερευνήτρια να τις κατανοήσει, κατόπιν προσδιορίστηκαν επιμέρους θέματα, ανάλυση και έγινε κωδικοποίηση των απαντήσεων.

Οι υπάλληλοι κωδικοποιήθηκαν με συγκεκριμένο αλφαριθμητικό κωδικό. Αυτός ο κωδικός αποτελούνταν από τα γράμματα «ΕΥΘ», για τους υπαλλήλους στην θέση ευθύνης και από τα γράμματα «ΥΠΑΛ» για τους διοικητικούς υπαλλήλους. Στους υπαλλήλους με θέση ευθύνης ανατέθηκε ένας αριθμός από το 1 μέχρι το 2, με βάση τη σειρά κατά την οποία λήφθηκαν οι συνεντεύξεις οπότε οι κωδικοί είναι ΕΥΘ-1 ΕΥΘ-2 και των Διοικητικών υπαλλήλων είναι ΥΠΑΛ-1, ΥΠΑΛ-2, ΥΠΑΛ-3 και ΥΠΑΛ-4, ΥΠΑΛ-5 ΚΑΙ ΥΠΑΛ-6

4.5.1 ***Ανάλυση αποτελεσμάτων***

Ανάλυση απαντήσεων

1. Στον πρώτο ερώτημα κλήθηκαν να απαντήσουν εάν γνώριζαν από πόσα πληροφοριακά συστήματα αποτελείται η πληροφοριακή υποδομή του e ΕΦΚΑ. Υπήρχε διαφορετική άποψη ανάμεσα στους διοικητικούς υπαλλήλους, ενώ οι υπάλληλοι με θέση ευθύνης γνώριζαν περισσότερα στοιχεία. Για παράδειγμα αναφέρουν χαρακτηριστικά:
   «…Η πληροφοριακή υποδομή του e ΕΦΚΑ αποτελείται από το σύνολο των πληροφοριακών συστημάτων των πρώην φορέων που συγχωνεύθηκαν στο ενιαίο φορέα την 01-01-2017.Κάποια από αυτά επανασχεδιάστηκαν ώστε να εξυπηρετούν με ενιαίο τρόπο» (ΥΠΑΛ-1),
   «…Πληροφοριακό σύστημα ΟΠΣ και Σύζευξις» (ΥΠΑΛ-6).
2. Στην ερώτηση ποιες ηλεκτρονικές υπηρεσίες παρέχονται από τον e ΕΦΚΑ μέσω διαδικτύου σε πολίτες, επιχειρήσεις και φορείς όλοι έδωσαν την ίδια απάντηση, οπότε υπάρχει ενημέρωση.
3. Στην ερώτηση ποιο πληροφοριακό σύστημα χειρίζεστε από τις απαντήσεις κρίνουμε ότι δεν χρησιμοποιούν τα ίδια και δεν γνωρίζουν τα πληροφοριακά συστήματα που χρησιμοποιούν οι συνάδερφοι τους.
4. Στην ερώτηση εάν υπάρχει διαλειτουργικότητα ανάμεσα στα διαφορετικά πληροφοριακά συστήματα του e ΕΦΚΑ και ανάμεσα στους φορείς του δημοσίου απάντησαν διαφορετικές απαντήσεις, οι υπάλληλοι με θέσεις ευθύνης, και διαφορετικές οι διοικητικοί υπάλληλοι οι οποίοι επίσης είχαν διαφορετικές απόψεις.
   Για παράδειγμα αναφέρουν χαρακτηριστικά:

«…Υπάρχει κατά κύριο λόγο ασύγχρονη επικοινωνία μεταξύ των πληροφοριακών υποσυστημάτων του ΕΦΚΑ με αποτέλεσμα να διαστρεβλώνεται η έννοια της διαλειτουργικότητας όπως αυτή καθορίζεται από την επιστήμη της Πληροφορικής. Ωστόσο σε κάποια από τα πληροφοριακά υποσυστήματα έχει καθοριστεί αλγόριθμος ανταλλαγής δεδομένων και συγχρονισμού σε συγκεκριμένες χρονικές περιόδους με time intervals ικανά ώστε να θεωρηθεί η όλη διαδικασία «διαλειτουργικότητα» (ΕΥΘ-1),

«….Μεταξύ των διαφορετικών πληροφοριακών συστημάτων του e ΕΦΚΑ δεν υπάρχει διαλειτουργικότητα, μεταξύ του e ΕΦΚΑ και των υπολοίπων φορέων δημοσίου είναι πολύ περιορισμένη η διαλειτουργικότητα» (ΥΠΑΛ-5).

5. Στην ερώτηση εάν αντιμετωπίζουν τεχνικά προβλήματα στα πληροφοριακά συστήματα και εάν υπάρχει αρμόδιο τμήμα επίλυσης προβλημάτων για κάθε τμήμα επίσης υπήρχαν διαφορετικές απόψεις, καθώς άλλοι υπάλληλοι απάντησαν ότι δεν είχαν τεχνικά προβλήματα, άλλοι πως είχαν, αλλά δεν υπήρχε αρμόδιο τμήμα και άλλοι ότι επιλύονταν άμεσα.
6. Στην ερώτηση εάν γνωρίζουν τι σημαίνει Κυβερνοασφάλεια, κάποιοι γνώριζαν, αλλά οι περισσότεροι δεν ήξεραν.

Για παράδειγμα αναφέρουν χαρακτηριστικά:

«…Οι κυβερνοαπειλές (Cyber Threats) είναι ενέργειες που γίνονται από τρίτους με σκοπό να πάρουν πρόσβαση σε πόρους που δεν έχουν τα κατάλληλα δικαιώματα, να καταστρέψουν ευαίσθητες και σημαντικές πληροφορίες, να αποσπάσουν χρήματα από χρήστες ή να διακόψουν τη ροή εργασιών μιας επιχείρησης. Η Κυβερνοασφάλεια (Cyber Security) είναι ένα σύνολο διαδικασιών και τεχνολογιών με τις οποίες αναγνωρίζουμε τις κυβερνοαπειλές και τις αποτρέπουμε» (ΕΥΘ-1),

«..Δεν έχω άρτια άποψη» (ΥΠΑΛ-2).

7. Στην ερώτηση εάν γνωρίζετε εάν υπάρχει πολιτική ασφαλείας μόνο όσοι έχουν ασχοληθεί οι ίδιοι γνώριζαν

Για παράδειγμα αναφέρουν χαρακτηριστικά:

«…Γνωρίζω ότι η πολιτική ασφαλείας που υπάρχει σε ορισμένα από τα

πληροφοριακά συστήματα του e ΕΦΚΑ είναι σε «εμβρυικό στάδιο» παρωχημένη και ξεπερασμένη από τον χρόνο και τα δεδομένα της επιστήμης της πληροφορικής που υπάρχουν σήμερα» (ΥΠΑΛ-1), «..Ναι» (ΥΠΑΛ-3),

«…Γνωρίζω ότι δεν μπορώ να μοιράζω τον κωδικό προστασίας μου» (ΥΠΑΛ-2),

8. Στην ερώτηση εάν έχετε ενημερωθεί για κάποια τεχνικά και οργανωτικά μέτρα που χρησιμοποιούνται στον e ΕΦΚΑ για την ασφάλεια και την εξασφάλιση της επιχειρησιακής συνέχειας των πληροφοριακών συστημάτων οι περισσότεροι απάντησαν όχι.
9. Στην ερώτηση εάν θεωρούν τα προσωπικά δεδομένα των πολιτών ασφαλή οι περισσότεροι απάντησαν ότι είναι επισφαλή.
10. Στην ερώτηση εάν διαχειρίζονται email από τον ίδιο υπολογιστή που συναλλάσσονται με ασφαλισμένους υπήρξαν διαφορετικές απαντήσεις καθώς άλλοι δεν συναλλάσσονταν, άλλοι απάντησαν θετικά και άλλοι αρνητικά
11. Στην ερώτηση εάν χρησιμοποιούν ψηφιακή υπογραφή όλοι ακόμα και οι υπάλληλοι σε θέσεις ευθύνης απάντησαν αρνητικά λόγω τεχνικής αδυναμίας του φορέα ενώ θεωρούν ότι αυτό έχει προγραμματισθεί να εφαρμοσθεί.
12. Στην ερώτηση εάν έχει υπάρξει κάποια ενημέρωση ή εκπαίδευση που να αφορά την ασφάλεια των συστημάτων, την προστασία της ακεραιότητας και της διαθεσιμότητας των πληροφοριών, την προστασία των προς επεξεργασία και αποθηκευμένων προσωπικών δεδομένων απάντησαν πάλι όλοι αρνητικά .
13. Στην ερώτηση εάν θα επιθυμούσατε να υπάρξει ενημέρωση και εκπαίδευση που να αφορά την ασφάλεια των πληροφοριακών συστημάτων που χειρίζεστε απάντησαν όλοι θετικά με εξαίρεση ένα διοικητικό υπάλληλο που απάντησε ότι «…θα επιθυμούσα να υπάρξει πρώτα ασφάλεια στα πληροφορικά συστήματα και μετά ενημέρωση» (ΥΠΑΛ-1).
14. Στην ερώτηση εάν θεωρείτε ότι η ανεπαρκής ενημέρωση και εκπαίδευση στα θέματα ασφάλειας των πληροφοριακών συστημάτων επηρεάζει την

διαλειτουργικότητα και κατά συνέπεια την αποδοτικότητα των υπαλλήλων απάντησαν διαφορετικά καθώς κάποιοι υπάλληλοι θεωρούν ότι η διαλειτουργικότητα είναι ανεξάρτητη από την απόδοση των υπαλλήλων και ανεξάρτητη από τα εργαλεία που τους δίνονται ενώ αρκετοί απάντησαν θετικά.

15. Στην ερώτηση εάν πιστεύετε ότι υπάρχει βελτίωση, εξέλιξη και εκσυγχρονισμός λειτουργιών και υποδομών του ΕΦΚΑ και κατ'επέκταση των πληροφοριακών συστημάτων εκφράζουν διαφορετική άποψη

Για παράδειγμα αναφέρουν χαρακτηριστικά:

«…..Εξαρτάται με τι τα συγκρίνουμε και από πότε. Γενικότερα όμως αυτό που χρειάζεται εκσυχρονισμό είναι το θεσμικό πλαίσιο λειτουργίας του ΕΦΚΑ πάνω στο οποίο θα στηριχθούν τα πληροφοριακά συστήματα που υλοποιούν τις λειτουργίες του» (ΕΥΘ-1)

«…Υπάρχει βελτίωση και εξέλιξη στις ηλεκτρονικές υπηρεσίες που παρέχονται από τον e ΕΦΚΑ μέσω διαδικτύου σε πολίτες, επιχειρήσεις και φορείς. Όμως όσον αφορά τους υπαλλήλους που χειρίζονται τ.Ο.Π.Σ. (τ. ΙΚΑ –ΕΤΑΜ) η έλλειψη διαλειτουργικότητας και ο περιορισμός της χρήσης απλών εφαρμογών (π.χ. email στον ίδιο υπολογιστή που εργάζεται ο κάθε υπάλληλος) προκειμένου να διασφαλιστεί η ασφάλεια του πληροφοριακού συστήματος περιορίζει: την πρόσβαση στην πληροφορία, την δυνατότητα άρτιας-άμεσης συναλλαγής με τους πολίτες και άλλους φορείς και φυσικά την αποδοτικότητα των υπαλλήλων» (ΥΠΑΛ-5).

16. Στην ερώτηση εάν θα μπορούσατε να αναφέρετε οποιαδήποτε δική σας παρατήρηση, διαπίστωση και άποψη που θα βοηθούσε προκειμένου να διεξαχθούν κάποια ενδεικτικά συμπεράσματα για τα πληροφοριακά συστήματα του ΕΦΚΑ και την Κυβερνοασφάλεια υπάρχουν αρκετοί σχολιασμοί που τους παραθέτω:

«…Η βασική παρατήρηση που θα έκανα είναι ότι εξαιτίας της αδυναμίας εξασφάλισης της Κυβερνοασφάλειας και της εφαρμογής πολιτικής ασφαλείας στα πληροφοριακά συστήματα του e- ΕΦΚΑ (και συγκεκριμένα αναφέρομαι στο σύστημα Ο.Π.Σ. τ. ΙΚΑ –ΕΤΑΜ) οι υπάλληλοι στερούνται απλές και αυτονόητες εφαρμογές(π.χ. email στον

ίδιο υπολογιστή που εργάζεται ο κάθε υπάλληλος) αλλά και την διαλειτουργικότητα μεταξύ των πληροφοριακών συστημάτων του e-ΕΦΚΑ και των φορέων του Δημοσίου» (ΥΠΑΛ-5),

« …Η εκκίνηση του εκσυγχρονισμού γίνεται από το θεσμικό πλαίσιο και τον κανονισμό λειτουργίας του Φορέα, ο οποίος θα αποτελέσει τη βάση για τη δημιουργία ενός ΕΝΙΑΙΟΥ πληροφοριακού συστήματος με προβλέψεις τόσο για την ασφάλειά του όσο και την ασφάλεια των δεδομένων του. Η συρραφή διαφορετικών κανονισμών και λειτουργιών των πρώην ταμείων με συνέπεια την «μπαλωματική επικόλληση» των πληροφοριακών τους συστημάτων και την διασταλτική χρήση του όρου «διαλειτουργικότητα», δεν διευκολύνει σε καμία περίπτωση τον ορισμό εκείνων των διαδικασιών που θα εξασφαλίσουν την προστασία της ακεραιότητας των δεδομένων και των συστημάτων του Φορέα. Οποιαδήποτε άλλη προσέγγιση θα καταστήσει ολέθρια την λειτουργία των συστημάτων» (ΕΥΘ-1),

«….Θα μπορούσα να γράφω σελίδες σε ατή την απάντηση αλλά θα αρκεστώ σε μία μόνο παρατήρηση: Αναθέστε σε ειδικούς το θέμα» (ΥΠΑΛ-1),

«…Θα πρέπει να εφαρμοστεί ένα ενιαίο πληροφοριακό σύστημα στον e ΕΦΚΑ το οποίο να χειρίζεται όλες τις διαδικασίες του φορέα και να υπάρχει σωστός καθορισμός πολιτικής ασφαλείας» (ΥΠΑΛ-2).

ΚΕΦΑΛΑΙΟ 5ο

5.1 ΣΥΜΠΕΡΑΣΜΑΤΑ

Μετά από την σχολαστική μελέτη των απαντήσεων της έρευνας των συναδέρφων-υπαλλήλων του e-ΕΦΚΑ αλλά και από την προσωπική μου άποψη και καθημερινή εκτίμηση και αξιολόγηση τα συμπεράσματα μου ως ερευνήτρια είναι τα εξής:

Ο e-ΕΦΚΑ είναι ένας φορέας που προήλθε από συγχώνευση πολλών ταμείων κοινωνικής ασφάλισης οπότε αυτό σαν γεγονός καθιστά πολύ δύσκολο το εγχείρημα του μετασχηματισμού του σε ένα φορέα που θα μπορεί να ανταποκριθεί στις ανάγκες των πολιτών και της σύγχρονης εποχής, της εποχής της τεχνολογίας και της εξέλιξης.

Θα χρειαστεί χρόνος για την δύσκολη αυτή μετάβαση αλλά η πιο σημαντική συνιστώσα σε αυτή την προσπάθεια είναι η συνεργασία με το ανθρώπινο δυναμικό του φορέα.

Από την έρευνα όμως διαπιστώσαμε ότι δεν υπάρχει καμία συνεργασία και ενημέρωση στους υπαλλήλους για την ασφάλεια των πληροφοριακών συστημάτων, καμία ιδιαίτερη εκπαίδευση για τους τρόπους προστασίας από τις κυβερνοαπειλές, καμία ουσιαστική διεπαφή της διοίκησης του φορέα με έναν από τους πόρους των πληροφοριακών συστημάτων δηλαδή το έμψυχο υλικό του φορέα.

Οι ίδιοι οι υπάλληλοι όμως είναι πρόθυμοι να εκπαιδευτούν, να προσαρμοστούν και να υποστηρίξουν κάθε προσπάθεια μετασχηματισμού και εξέλιξης, αν και όπως πιστεύουν και οι ίδιοι, είναι αναγκαίο να υπάρξει ένα ενιαίο θεσμικό πλαίσιο για ένα ενιαίο πληροφοριακό σύστημα και μία ενιαία πολιτική ασφαλείας τα οποία θα συμβάλλουν στην διαλειτουργικότητα των πληροφοριακών συστημάτων και την διασύνδεση με τους υπολοίπους φορείς του δημοσίου.

5.2 ΕΝΔΕΙΚΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ ΚΑΙ ΤΗΝ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ e-ΕΦΚΑ

Για τους υπαλλήλους του e ΕΦΚΑ που χρησιμοποιούν τα ΠΣ

- Γνώση και συμμόρφωση: Να έχουν διαβάσει, κατανοήσει και αποδεχτεί τις πολιτικές του Πλαισίου Ασφάλειας που τον αφορούν. Ειδικότερα, κατά την απόδοση σε αυτόν λογαριασμών χρήστη, πρέπει να του γνωστοποιείται η παρούσα Πολιτική Ορθής Χρήσης Πληροφοριακών Πόρων από τον άμεσα διοικητικό του προϊστάμενο και να δεσμεύεται για την κατανόηση και την αποδοχή της, αν είναι δυνατόν εγγράφως.
- Ρόλος: να γνωρίζουν επακριβώς ποιες είναι οι αρμοδιότητές του σε σχέση με την Ασφάλεια Πληροφοριών και Πληροφοριακών Συστημάτων, ιδίως ως προς το Πλαίσιο Ασφάλειας.
- Χρήση Λογαριασμών Πρόσβασης: να γνωρίζουν ότι οι λογαριασμοί πρόσβασης σε πληροφοριακά συστήματα είναι αυστηρά προσωπικοί και ότι κάθε ενέργεια των λογαριασμών συνδέεται με τους ίδιους και μόνο. Να γνωρίζουν ότι ως νόμιμοι κάτοχοι ενός λογαριασμού είναι υπόλογοι σε περίπτωση εντοπισμού ανάρμοστης ή και παράνομης χρήσης των Πληροφοριακών Πόρων μέσω του λογαριασμού που τους έχει παραχωρηθεί.

Να αποκτά πρόσβαση στους Πληροφοριακούς Πόρους κάνοντας χρήση μόνο του λογαριασμού που του έχει παραχωρηθεί.

- Απαγορεύεται να εκτελεί οποιαδήποτε δραστηριότητα με λογαριασμούς που ανήκουν σ' άλλους χρήστες καθώς και να γνωστοποιεί το λογαριασμό του σε τρίτους.
- Χρήση εξοπλισμού/υλικού: ο εξοπλισμός που τους έχει διατεθεί για τα υπηρεσιακά τους καθήκοντα δεν πρέπει να χρησιμοποιείται για προσωπικούς λόγους και ούτε να παραχωρείται σε τρίτους. Επιπλέον, δεν επιτρέπεται να συνδέει ιδιόκτητες συσκευές όπως υπολογιστές, ταμπλέτες, έξυπνα κινητά τηλέφωνα, κάμερες κ.λπ. στην υποδομή των πληροφοριακών συστημάτων. Σε περίπτωση που υπηρεσιακές ανάγκες το επιβάλλουν, θα πρέπει να ζητήσει πρώτα έγγραφη εξουσιοδότηση από τον άμεσο διοικητικό του προϊστάμενο παρέχοντας επαρκής αιτιολόγηση.
- Κλείδωμα οθόνης υπολογιστή: όταν απουσιάζει/απομακρύνεται από το γραφείο του, η οθόνη του προσωπικού υπολογιστή πρέπει να κλειδώνει με μυστικό προσωπικό κωδικό την επιφάνεια εργασίας.
- Χρήση φορητών υπολογιστών: απαιτείται ιδιαίτερη προσοχή κατά την μετακίνηση φορητών υπολογιστών και συσκευών που περιέχουν δεδομένα εκτός των εγκαταστάσεων του φορέα (π.χ. οι φορητοί υπολογιστές να μην μένουν αφύλακτοι σε δημόσιους χώρους ή σε αυτοκίνητα). Σε περίπτωση κλοπής ή απώλειας, το περιστατικό πρέπει να αναφέρεται άμεσα
- Εχεμύθεια: να τηρεί εχεμύθεια για θέματα που χαρακτηρίζονται απόρρητα ή προστατεύονται από την κείμενη νομοθεσία, ή όταν αυτό επιβάλλεται από την κοινή πείρα και λογική για γεγονότα ή πληροφορίες των οποίων λαμβάνει γνώση ή επεξεργάζεται κατά την εκτέλεση των καθηκόντων του. Πρέπει να δίδεται ιδιαίτερη προσοχή ώστε κατά τις προφορικές συζητήσεις επιχειρησιακών θεμάτων να μην αποκαλύπτονται διαβαθμισμένες πληροφορίες σε τρίτους.
- Ανάγκη χρήσης/ανάγκη γνώσης: να περιορίζεται μόνο στην πρόσβαση/επεξεργασία που είναι απαραίτητη για την εκτέλεση των καθηκόντων του.
- Διακίνηση διαβαθμισμένης πληροφορίας (με συμβατική ή ηλεκτρονική αλληλογραφία): να φροντίζει ώστε τα δεδομένα που χαρακτηρίζονται ως

διαβαθμισμένα να προστατεύονται επαρκώς σύμφωνα με την Πολιτική Διαχείρισης Πληροφοριακών Πόρων. Σε περίπτωση ηλεκτρονικής διακίνησής τους να χρησιμοποιούνται εγκεκριμένες μέθοδοι, όπως κρυπτογράφηση, σύμφωνα με το Πλαίσιο Ασφάλειας.

- Χρήση φορητών αποθηκευτικών μέσων: να μην αντιγράφει υπηρεσιακά στοιχεία ή δεδομένα των Πληροφοριακών Συστημάτων σε εξωτερικά και αποσπώμενα μέσα όπως CD-ROM, DVD-ROM, flash drives, εξωτερικούς σκληρούς δίσκους κ.λπ. Σε περίπτωση που υπηρεσιακές ανάγκες επιβάλουν τη χρήση τέτοιων μέσων, πρέπει να δοθεί έγγραφη εξουσιοδότηση από τον άμεσο διοικητικό του προϊστάμενο μετά από τεκμηριωμένο αίτημα. Η αντιγραφή πρέπει να γίνεται με χρήση εγκεκριμένων μεθόδων του Πλαισίου Ασφάλειας, όπως κρυπτογράφηση, ώστε σε περίπτωση απώλειας του φορητού αποθηκευτικού μέσου να μην υπάρχει δυνατότητα διαρροής.
- Καθαρή επιφάνεια εργασίας: να λαμβάνει μέριμνα για την διατήρηση καθαρής επιφάνειας

Συμπερασματικά από τις πληροφορίες που συλλέξαμε, από τις απόψεις των υπαλλήλων αλλά και από την γενικότερη έρευνά μας καταλήγουμε στα εξής:

1.Μετά τη λειτουργική ενοποίηση όλων των ασφαλιστικών ταμείων οι ανάγκες του φορέα είναι τεράστιες και απαιτούν καθοριστικές λύσεις και καταλυτικές αποφάσεις οι οποίες θα προέρχονται από μία διαρκή συνεργασία της Διοίκησης, της επιστήμης της πληροφορικής και του ανθρώπινου δυναμικού. Είναι επιτακτική ανάγκη να υπάρξει ενιαίο πληροφοριακό σύστημα το οποίο θα εξασφαλίσει ποιοτική απόδοση, ταχύτητα και ασφάλεια. Συγχρόνως όμως επιβάλλεται σύμπραξη και συμμετοχή του ανθρώπινου δυναμικού σε μία συνεχή ενημέρωση, εκπαίδευση και υποστήριξη από την Διοίκηση για μία ενιαία προσπάθεια.

2.Στην υφιστάμενη μεταβατική φάση η ελλιπής πολιτική ασφαλείας είναι ένας από τους παράγοντες που εμποδίζει την ομαλή λειτουργία της υπηρεσίας και δημιουργεί σημαντικά εμπόδια στην ευελιξία, απόδοση και αποτελεσματικότητα.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΠΗΓΕΣ

Α. ΒΙΒΛΙΟΓΡΑΦΙΑ ΕΛΛΗΝΙΚΗ

- Ανοικτά Δεδομένα από e ΕΦΚΑ. Νέες Τεχνικές Προδιαγραφές
- Ανοικτά Δεδομένα από e ΕΦΚΑ. Σχέδιο Διακήρυξη Ανοικτού Διαγωνισμού
- Ανοικτά Δεδομένα από e ΕΦΚΑ. Το υπ'αριθμ.πρωτ.369371/23-09-2021 Παροχή Υπηρεσιών Συμφωνημένου Επιπέδου (SLA) για υπηρεσίες Υποστήριξης Παραγωγικής Λειτουργίας, Διαχείρισης Έργου-Διασφάλισης Ποιότητας, Ασφάλειας σε Συστήματα του e-ΕΦΚΑ και Υπεύθυνου Ασφάλειας, Συντήρησης Λογισμικού Εφαρμογών, On-demand Συμβουλευτικές/Υποστηρικτικές Υπηρεσίες των Πληροφοριακών Συστημάτων
- Ανοικτά Δεδομένα από ΕΦΚΑ. Τεχνικές και Λειτουργικές προδιαγραφές. Διασύνδεση του ΕΦΚΑ με το Ευρωπαϊκό Σύστημα Ηλεκτρονικής Ανταλλαγής Πληροφοριών για την Κοινωνική Ασφάλιση (EESSI)
- Αποστολάκης Ι., Λουκής Ε., Χάλαρης Ι. (2008) Ηλεκτρονική Δημόσια Διοίκηση Εκδόσεις Παπαζήση, Αθήνα
- Δουκίδης Γ. (2011) Καινοτομία Στρατηγική Ανάπτυξη και Πληροφοριακά Συστήματα Εκδόσεις Σιδέρη, Αθήνα
- Ένταξη φορέων, κλάδων, τομέων και λογαριασμών στον Ε.Φ.Κ.Α. Ν.4387/2016, άρθρο 53, (ΦΕΚ Α΄85/12-5-2016)
- Ισαρη Φ.- Μπουρκός Μ. Ποιοτική (2015) Μεθοδολογία Ερευνας Εκδόσεις Ελληνικά Συγράμματα
- Κάτσικας Σ. Γκρίτζαλης Σ. Λαμπρινουδάκης Κ. (2021) Ασφάλεια Πληροφοριών και Συστημάτων στο Κυβερνοχώρο Εκδόσεις Νέων Τεχνολογιών Αθήνα
- Λαζακίδου Α. (2019) Ηλεκτρονική Διακυβέρνηση και Ηλεκτρονικές Υπηρεσίες προς Πολίτες και Επιχειρήσεις Εκδόσεις Δίσιγμα

Β. ΒΙΒΛΙΟΓΡΑΦΙΑ ΑΓΓΛΙΚΗ

- Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law
- Wilson, Duance C. "Cybersecurity"(2021). The MIT Press Essential Knowledge Series, MIT Press

Γ.ΙΣΤΟΣΕΛΙΔΕΣ

- https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ (προσπέλαση 19-03-2022)
- https://ec.europa.eu/commission/presscorner/detail/el/ip_21_3088 (προσπέλαση 25-03-2022)
- https://ec.europa.eu/commission/presscorner/detail/el/QANDA_21_5483 (προσπέλαση 23-03-2022)
- https://ejournals.epublishing.ekt.gr/index.php/eekp/article/view/14604 (προσπέλαση 23-03-2022)
- https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle (προσπέλαση 20-03-2022)
- https://en.wikipedia.org/wiki/Computer_security (προσπέλαση 19-03-2022)
- https://en.wikipedia.org/wiki/Kill_chain (προσπέλαση 20-03-2022)
- https://en.wikipedia.org/wiki/Malware (προσπέλαση 19-03-2022)
- https://en.wikipedia.org/wiki/Spyware (προσπέλαση 20-03-2022)
- https://en.wikipedia.org/wiki/Trojan_horse_(computing) (προσπέλαση 19-03-2022)
- https://eurozoi.gr/2022/01/%ce%b7-%ce%ba%cf%85%ce%b2%ce%b5%cf%81%ce%bd%ce%bf%ce%b1%cf%83%cf%86%ce%ac%ce%bb%ce%b5%ce%b9%ce%b1-%cf%83%cf%84%ce%b7%ce%bd-%ce%b5%ce%b5-%cf%84%ce%b7%ce%bd-%cf%80%ce%b5%cf%81%ce%af%ce%bf%ce%b4%ce%bf/ (προσπέλαση 22-03-2022)
- https://gr.rua.gr/2022/01/21/%CF%87%CE%AC%CE%BA%CE%B5%CF%81-%CE%B5%CF%80%CE%B9%CF%84%CE%AD%CE%B8%CE%B7%CE%BA%CE%B1%CE%BD-%CF%83%CE%B5-%CF%84%CF%81%CE%AF%CE%B1-%CE%BD%CE%BF%CF%83%CE%BF%CE%BA%CE%BF%CE%BC%CE%B5%CE%AF%CE%B1-%CF%84/ (προσπέλαση 25-03-2022)
- https://ictplus.gr/sti-bouli-fernei-o-syriza-p-s-ypothesi-kenon-asfaleias-sta-pliroforiaka-systimata-e-efka-kai-ypourgeiou-psifiakis-diakybernisis/?fbclid=IwAR3F5gPd0RQKoCDE1dbYBVgPpV939Hlgpd8yxBNRC28-hTvGYx3akLoYUSo (προσπέλαση 24-03-2022)

- https://iguru.gr/elta-dothike-anakoinosi-gia-ton-tropo-tis-kyvernoepithesis/?feed_id=2119&_unique_id=6239719e4a483&fbclid=IwAR3GOBZSnFBYI74pBk7AJ-y8L_TayOeAsDOWBGBHmBqKwHa4K4PDkiJeZaM (προσπέλαση 24-03-2022)
- https://mindigital.gr/kyvernoasfaleia (προσπέλαση 23-03-2022)
- https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf?fbclid=IwAR0JDJGj5D5H6-DfmMqsc_Sw2x4bVGXrhaaHdlhzYfldW8FqQUiQaN1EUDA (προσπέλαση 22-03-2022)
- https://ticketing.1555.gov.gr/odigosUI/ (προσπέλαση 23-03-2022)
- https://www.aade.gr/menoy/aade/asfaleia-ilektronikon-ypiresion (προσπέλαση 24-03-2022)
- https://www.antinews.gr/action.read/ellada/i-aristi-metatropi-tou-efka-se-upiresia-koinonikis-anaisthisias/4.157063 (24-03-2022)
- https://www.asfalisinet.gr/%CE%BC%CE%B5-%CF%84%CE%BF-%CF%85%CF%88%CE%B7%CE%BB%CF%8C%CF%84%CE%B5%CF%81%CE%BF-%CE%BA%CF%8C%CF%83%CF%84%CE%BF%CF%82-%CF%80%CE%B1%CF%81%CE%B1%CE%B2%CE%AF%CE%B1%CF%83%CE%B7%CF%82-%CE%B4%CE%B5%CE%B4/ (προσπέλαση 25-03-2022)
- https://www.asfalisinet.gr/%CE%BF%CE%B9-%CF%87%CE%AC%CE%BA%CE%B5%CF%81%CF%82-%CE%B1%CE%BD%CE%B5%CE%B2%CE%AC%CE%B6%CE%BF%CF%85%CE%BD-%CF%84%CE%B9%CF%82-%CE%B1%CF%80%CE%B1%CE%B9%CF%84%CE%AE%CF%83%CE%B5%CE%B9%CF%82-%CF%84%CE%BF/ (προσπέλαση 25-03-2022)
- https://www.asfalisinet.gr/%CF%80-%CF%84%CF%83%CE%B1%CE%BA%CE%BB%CF%8C%CE%B3%CE%BB%CE%BF%CF%85-%CE%BF-%CE%B5%CE%BA%CF%83%CF%85%CE%B3%CF%87%CF%81%CE%BF%CE%BD%CE%B

9%CF%83%CE%BC%CF%8C%CF%82-%CF%84%CE%BF%CF%85-%CE%B5%CF%86%CE%BA/ (προσπέλαση 25-03-2022)

- https://www.asfalisinet.gr/%CF%83%CE%B5-%CE%B5%CF%86%CE%B9%CE%AC%CE%BB%CF%84%CE%B7%CF%82-%CE%B3%CE%B9%CE%B1-%CF%80%CE%BF%CE%BB%CE%AF%CF%84%CE%B5%CF%82-%CE%BA%CE%B1%CE%B9-%CE%B5%CF%80%CE%B9%CF%87%CE%B5%CE%B9%CF%81%CE%AE%CF%83/(προσπέλαση 25-03-2022)
- https://www.asfalisinet.gr/%CF%85%CF%80%CE%BF%CF%85%CF%81%CE%B3%CE%B5%CE%AF%CE%BF-%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1%CF%82-%CE%B4%CF%81%CE%B1%CF%83%CF%84%CE%B9%CE%BA%CE%AD%CF%82-%CF%80%CE%B1%CF%81%CE%B5%CE%BC%CE%B2/ (προσπέλαση 25-03-2022)
- https://www.csc.com.gr/cloud-computing/ (προσπέλαση 23-03-2022)
- https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks (προσπέλαση 19-03-2022)
- https://www.dianeosis.org/wp-content/uploads/2021/09/e-gov_policy-paper.pdf (προσπέλαση 22-03-2022)
- https://www.dikastiko.gr/eidhsh/sfodri-antidrasi-tis-olomeleias-ston-efka-me-apeili-lipsis-metron-quot-dekades-dikigoroi-vrethikan-paranomos-anasfalistoi-quot/ (24/03/2022)
- https://www.enisa.europa.eu/about-enisa/about/el (προσπέλαση 22-03-2022)
- https://www.enisa.europa.eu/news/ecsm-2021-pr/cnect-2021-00359-02-00-el-tra-00.pdf?fbclid=IwAR2_-QUwGISf0foyQnvkl4_3fzVziQYTtuG6oMzE_I0S7UCzPNm5u7y9U68 (προσπέλαση 22-03-2022)
- https://www.e-nomothesia.gr/kat-ergasia-koinonike-asphalise/nomos-4387-2016-phek-85a-12-5-2016.html (προσπέλαση 23-03-2022)

- https://www.ertnews.gr/eidiseis/oikonomia/ey-i-tacheia-prosarmogi-stin-tilergasia/?fbclid=IwAR0z7sW4ziCCw7V9aVN7LmXRXcgryqYhIyKJLgFwTyY6RCBwQOzA-Jejhh4 (προσπέλαση 22-03-2022)
- https://www.ethnos.gr/technology/article/166472/enisahkardiathskybernoasfaleiasthseyrophsxtypasthnellada (προσπέλαση 23-03-2022)
- https://www.europarl.europa.eu/factsheets/el/sheet/55/%CE%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%B7-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B9%CF%83%CE%B7-%CF%83%CE%B5-%CE%B1%CE%BB%CE%BB%CE%B1-%CE%BA%CF%81%CE%B1%CF%84%CE%B7-%CE%BC%CE%B5%CE%BB%CE%B7-%CF%84%CE%B7%CF%82-%CE%B5%CE%B5 (προσπέλαση 25-03-2022)
- https://www.europarl.europa.eu/news/el/headlines/society/20220120STO21428/kuvernoasfaleia-oi-megaluteres-apeiles-gia-to-2021-grafima#missinglink (προσπέλαση 22-03-2022)
- https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (προσπέλαση 22-03-2022)
- https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks (προσπέλαση 19-03-2022)
- https://www.fortunegreece.com/article/i-evropaikes-chores-me-ti-megaliteri-kivernoasfalia-i-thesi-tis-elladas/ (προσπέλαση 22-03-2022)
- https://www.fpress.gr/ellada/story/86189/egkainiasthike-i-edra-toy-enisa-stin-athina (προσπέλαση 22-03-2022)
- https://www.ieidiseis.gr/oikonomia/134998/efka-9-asyndetes-psifiakes-platformes-talaiporoyn-tous-asfalismenous?fbclid=IwAR3ixzQex3ZnOen4__mpGGFL1C4RG-vASATv_gFSc8_twdfWx8XHh0gp_Ao (προσπέλαση 23-03-2022)
- https://www.kathimerini.gr/economy/561723097/pempti-pagkosmios-i-ellada-stis-psifiakes-epitheseis-phishing/ (προσπέλαση 25-03-2022)
- https://www.kathimerini.gr/politics/561680272/epithesi-chakers-sti-voyli/ (προσπέλαση 24-03-2022)
- https://www.kathimerini.gr/world/561733171/oykrania-maziki-kyvernoepithesi-se-kyvernitikoys-istotopoys-kai-trapezes/ (προσπέλαση 24-03-2022)

- https://www.lifo.gr/stiles/optiki-gonia/problima-sto-systima-agapi-kai-efka (προσπέλαση 25-03-2022)
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.nextdeal.gr/epikairotita/oikonomia/116585/i-accenture-apokalyptei-tis-megalyteres-apeiles-poy-kyriarhoyn-ston (προσπέλαση 25-03-2022)
- https://www.pagenews.gr/2022/01/30/oikonomia/efka-pente-aksones-pou-allazoun-to-epipedo-ton-parexomenon-ypiresion-tou-infographic/ (προσπέλαση 23-03-2022)
- https://www.reporter.gr/Eidhseis/technologia/462967-H-kyberno-asfaleia-allazei-to-dhmosio (προσπέλαση 25-03-2022)
- https://www.researchgate.net/profile/Ioannis-Rossidis/publication/319623074_To_asphalistiko_systema_se_krise/links/59b630690f7e9b374355475b/To-asphalistiko-systema-se-krise.pdf?origin=publication_detail (προσπέλαση 25-03-2022)
- https://www.skai.gr/news/greece/kseperasan-to-1-ekatommyrio-oi-apantimenes-kliseis-sto-1555(προσπέλαση 25-03-2022)
- https://www.taxheaven.gr/news/58477/oee-diabebaiwseis-apo-e-efka-gia-amesh-epilysh-twn-problhmatwn-stis-synallages (προσπέλαση 25-03-2022)
- https://www.updatetimes.gr/prosochi-afti-einai-i-nea-apati-me-apostoli-email-oi-treis-protaseis-kai-sto-telos-o-ekviasmos/ (προσπέλαση 25-03-2022)