Όνομα Οργανισμού

Πολιτική Διαχείρισης Ευπαθειών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διαχείρισης Ευπαθειών |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχομένων

[1. Σκοπός 4](#_Toc153537693)

[2. Παρακολούθηση Ασφάλειας 4](#_Toc153537694)

[2.1. Ελεγχόμενα συστήματα 4](#_Toc153537695)

[2.2. Τρόπους Ανίχνευσης, εντοπισμού των ευπαθειών και καταγραφή 5](#_Toc153537696)

[2.3. Ανίχνευση και Καταγραφή Ευπαθειών 7](#_Toc153537697)

[2.4. Συσσώρευση Συμβάντων 7](#_Toc153537698)

[2.4.1 Συγκέντρωση Ημερολογίων 7](#_Toc153537705)

[2.4.2 Ανάλυση Ημερολογίων 8](#_Toc153537706)

[2.4.3 Συσχετισμός 8](#_Toc153537707)

[2.4.4 Αποθήκευση και προστασία των ημερολογίων 8](#_Toc153537708)

[3. Διαχείριση Ευπαθειών και Τρωτότητας 9](#_Toc153537709)

[3.1. Αξιολόγηση και Αποκατάσταση Ευπαθειών 9](#_Toc153537710)

[3.2. Αποκατάσταση Ευπαθειών 10](#_Toc153537711)

[3.3. Σχέδιο και προσέγγιση βάσει κινδύνου 10](#_Toc153537712)

[3.4. Πολιτική αποκατάστασης ευπαθειών 10](#_Toc153537713)

[3.5. Αποκατάσταση Ευπαθειών με Έγκριση της Διοίκησης 10](#_Toc153537714)

[3.6. Διαδικασίες ασφάλειας ευπαθειών 11](#_Toc153537715)

[3.7. Εφαρμογή ενεργειών 11](#_Toc153537716)

[3.8. Ταξινόμηση και επισήμανση πληροφοριών 11](#_Toc153537717)

[3.9. Διαχείριση αλλαγών 11](#_Toc153537718)

[3.9.1 Αποκατάσταση Ευπαθειών με Βάση τη Διαδικασία Διαχείρισης Αλλαγών 12](#_Toc153537729)

[3.10. Δοκιμές Διείσδυσης 13](#_Toc153537730)

[4. Διορθωτικές Ενέργειες και Διαχείριση Ευπαθειών Ασφάλειας 14](#_Toc153537731)

[5. Κρίσιμα Συστήματα 15](#_Toc153537732)

[5.1. Σχέδιο Προσέγγισης για Έλεγχο Ευπαθειών 15](#_Toc153537733)

[5.2. Ανταπόκριση σε Ευπάθειες Κρίσιμης Σημασίας 16](#_Toc153537734)

# Σκοπός

Η Διαχείριση Ευπαθειών και Τρωτότητας είναι η στρατηγική που συνδυάζει τις τεχνικές Αξιολόγησης και Αποκατάστασης Ευπαθειών (Vulnerability Assessment and Patch Management) και Δοκιμές Διείσδυσης (Penetration Tests) για να επιβεβαιώσει ότι οι πρακτικές ασφάλειας και οι έλεγχοι, τηρούνται και είναι αποτελεσματικοί. Σκοπός των τεχνικών αυτών είναι ο εντοπισμός και η αποκατάσταση των υφιστάμενων, αλλά και καινούργιων ευπαθειών στα πληροφοριακά συστήματα του [Όνομα Οργανισμού].

Σκοπός του Προτύπου Διαχείρισης Ευπαθειών και Τρωτότητας είναι να προστατεύσει τα πληροφοριακά συστήματα, προβλέποντας τυχόν ευπάθειες ή τυχόν κενά στην ασφάλεια των πληροφοριακών συστημάτων. Απώτερος σκοπός είναι να διασφαλίσει τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών του [Όνομα Οργανισμού].

Το Πρότυπο Διαχείρισης Ευπαθειών και Τρωτότητας απευθύνεται στο προσωπικό του [Όνομα Οργανισμού], στους προμηθευτές, και σε τρίτους που δραστηριοποιούνται εκ μέρους του [Όνομα Οργανισμού].

# Παρακολούθηση Ασφάλειας

# Ελεγχόμενα συστήματα

Τα ημερολόγια των συστημάτων(log books) του [Όνομα Οργανισμού] πρέπει να συσσωρεύονται προκειμένου να επιτυγχάνεται η αποφυγή καθώς και η άμεση ανταπόκριση των ευπαθειών ή της κακόβουλης εισβολής στα πληροφοριακά συστήματα και πληροφορίες. Πιο συγκεκριμένα τα ημερολόγια πρέπει να συγκεντρώνονται, να αναλύονται και να συσχετίζονται σε κεντρικό σύστημα διαχείρισης ημερολόγιών (Security Information and Events Management - SIEM).

Σε περιπτώσεις όπου απαιτείται από το κανονιστικό πλαίσιο, τα ημερολόγια θα πρέπει να αποθηκεύονται για μια χρονική περίοδο. Η εν λόγω χρονική περίοδος, καθορίζεται από την Γενική Διεύθυνση σε συνεργασία με το [Αρμόδιο Τμήμα Νομικής]. Η χρονική περίοδος διατήρησης των ημερολόγιων για το κάθε σύστημα μπορεί να είναι διαφορετική.

Απαιτείται η συσσώρευση και η καταγραφή, των ημερολογίων (logs) τουλάχιστον για τα πιο κάτω συστήματα:

* Συστήματα προστασίας από επιθέσεις άρνησης υπηρεσιών (Flood Guards)
* Firewalls, including Network, Application, Database firewalls
* Συστήματα Ανίχνευσης και Πρόληψης Εισβολής (IDS/IPS).
* Σύστημα πρόληψης απώλειας δεδομένων (DLP)
* Σύστημα τύπου Sandbox
* Συστήματα ηλεκτρονικού ταχυδρομείου
* Συστήματα προστασίας από ιούς (antivirus).
* Συστήματα Web Proxy
* Κεντρικά συστήματα πληροφοριακών συστημάτων.
* Συστήματα Πιστοποίησης (Authentication Servers) και Ελεγκτές Τομέων (Domain Controllers). Έμφαση θα πρέπει να δίνεται στην παρακολούθηση ημερολογίων λογαριασμών χρηστών (user account logs).
* Συστήματα ελέγχου πρόσβασης τόσο για την λογική όσο και για την φυσική πρόσβαση στα πληροφοριακά συστήματα, πληροφορίες και εγκαταστάσεις του [Όνομα Οργανισμού]
* Ημερολόγια βάσεων Δεδομένων
* Συστήματα ελέγχου πρόσβασης για τοποθεσίες και εγκαταστάσεις, που φιλοξενούν κρίσιμα συστήματα ή/ και πληροφορίες (π.χ. δωμάτια κεντρικών συστημάτων, αρχειοφυλάκιο) Συστήματα κλειστού κυκλώματος βιντεοπαρακολούθησης
* Ημερολόγια δικτυακών συσκευών (routers, switch).
* Ημερολόγια υποδομή ιδεατού περιβάλλοντος (Virtualization).
* Ημερολόγια ανίχνευσης (scan) δικτύων.
* Ημερολόγια υγείας και σφαλμάτων των συστημάτων.
* Ημερολόγια εφαρμογών.
* Ημερολόγια βάσεων Δεδομένων
* Ημερολόγια εφεδρείας και ανάκτησης δεδομένων.
* Κλήσεις προβλημάτων γραφείου υποστήριξης (Helpdesk).
* Συστήματα τηλεφωνίας (τηλεφωνικό σύστημα).
* Συστήματα στιγμιαίων μηνυμάτων (instant messaging)
* Ημερολόγια πολυλειτουργικών εκτυπωτών.
* Οποιαδήποτε άλλα ημερολόγια που θεωρούνται κρίσιμα.

Όλα τα πληροφοριακά συστήματα πρέπει να έχουν συγχρονισμένα τα ρολόγια τους με τον Ntp server.

# Τρόπους Ανίχνευσης, εντοπισμού των ευπαθειών και καταγραφή

Τα εργαλεία ελέγχου ευπάθειας είναι εφαρμογές λογισμικού ή υπηρεσίες που έχουν σχεδιαστεί για να βοηθούν τους οργανισμούς να εντοπίζουν και να αξιολογούν τις αδυναμίες ασφάλειας στα συστήματα, τα δίκτυα ή τις εφαρμογές τους. Αυτά τα εργαλεία αυτοματοποιούν τη διαδικασία ελέγχου ευπάθειας, καθιστώντας την πιο αποτελεσματική, ακριβή και συνεπή.

Υπάρχουν διάφοροι τύποι εργαλείων δοκιμής ευπάθειας, όπως:

* Σαρωτές ευπάθειας δικτύου: Αυτά τα εργαλεία σαρώνουν δίκτυα για ανοιχτές θύρες, εσφαλμένες ρυθμίσεις παραμέτρων και άλλες αδυναμίες ασφαλείας.
* Σαρωτές ευπάθειας εφαρμογών Ιστού: Αυτά τα εργαλεία είναι ειδικά σχεδιασμένα για να εντοπίζουν τρωτά σημεία σε εφαρμογές Ιστού, όπως η έγχυση SQL, η δέσμη ενεργειών μεταξύ τοποθεσιών (XSS) και ο κατεστραμμένος έλεγχος ταυτότητας.
* Εργαλεία στατικής δοκιμής ασφάλειας εφαρμογών (SAST): Σχεδιασμένα για να αναλύουν τον πηγαίο κώδικα ή τον μεταγλωττισμένο κώδικα για τον εντοπισμό πιθανών τρωτών σημείων ασφαλείας χωρίς την εκτέλεση της εφαρμογής.
* Εργαλεία δοκιμής δυναμικής ασφάλειας εφαρμογών (DAST): Σχεδιασμένα για να αλληλεπιδρούν με εφαρμογές που εκτελούνται για να εντοπίζουν αδυναμίες ασφαλείας κατά τη διάρκεια του χρόνου εκτέλεσης.
* Εργαλεία δοκιμών Fuzz: Δημιουργήστε και στείλτε εσφαλμένες ή απροσδόκητες εισόδους σε εφαρμογές για τον εντοπισμό τρωτών σημείων που σχετίζονται με την επικύρωση εισόδου και τον χειρισμό σφαλμάτων.
* Εργαλεία διαχείρισης διαμόρφωσης και συμμόρφωσης: Αυτά τα εργαλεία αξιολογούν τις διαμορφώσεις συστήματος και εφαρμογών σε σχέση με καθιερωμένες βέλτιστες πρακτικές ασφάλειας ή πρότυπα συμμόρφωσης, όπως σημεία αναφοράς CIS ή PCI DSS.
* Εργαλεία ασφάλειας κοντέινερ και cloud: Αυτά τα εργαλεία επικεντρώνονται στον εντοπισμό τρωτών σημείων και εσφαλμένων διαμορφώσεων σε περιβάλλοντα που βασίζονται σε σύννεφο και σε εφαρμογές με κοντέινερ.

Μετά την εντόπιση της ευπάθειας υψηλού κινδύνου, θα πρέπει να υπάρχει συμπερίληψη στοιχείων όπου θα παρουσιαστή στην διοίκηση, με σκοπό να εξασφαλίζεται η εκ των άνω προς τα κάτω επίγνωση των ευπαθειών με δυνητικές επιπτώσεις και να προσδιορίζονται τα κατάλληλα μέτρα για την αποκατάσταση και την εφαρμογή διορθωτικών συστημάτων και διαδικασιών[VM3]. Επίσης να εντοπίζονται οι απειλές, ευπάθειες και κινδύνους στους οποίους εκτίθενται τα στοιχεία ενεργητικού, τα συστήματα και οι διαδικασίες του οργανισμού[RM3]. Ο [Όνομα Οργανισμού] θα πρέπει να καταγράφει τις σχετικές ευπάθειες στον κατάλογο απειλών, ευπαθειών και κινδύνων. Η καταγραφή αυτή αποτελεί τον βασικό πυλώνα για την ανάλυση και τη διαχείριση των πιθανών απειλών που ενδέχεται να επηρεάσουν την ασφάλεια των πληροφοριών μας. Οι ευπάθειες που μπορεί να εκτεθούν σε πιθανούς κινδύνους ταξινομούνται και καταγράφονται λεπτομερώς. Ο κατάλογος απειλών και ευπαθειών αποτελεί μια βάση δεδομένων για τις ευπάθειες σε συστήματα, εφαρμογές και διαδικασίες. Η τακτική ενημέρωση και αξιολόγηση του καταλόγου συμβάλει στην πρόληψη και αντιμετώπιση ενδεχόμενων κινδύνων.

Ο [Όνομα Οργανισμού] πρέπει να έχει θεσπίσει, εφαρμόζει και διατηρεί διαδικασία για την καταγραφή και την αναφορά των ευπαθειών που έχουν εντοπιστεί, ώστε να είναι δυνατή η αποκατάσταση και η ενημέρωση συστημάτων και διαδικασιών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Να διασφαλιστεί ότι οι ευπάθειες καταγράφονται και υποβάλλονται σε σχετικές εκθέσεις, ώστε να είναι δυνατή η λήψη τεκμηριωμένων αποφάσεων από τη διοίκηση όσον αφορά τον χειρισμό τους[VM2]. Η διαδικασία αποκατάστασης ευπαθειών και η εφαρμογή ενημερώσεων ασφάλειας είναι ουσιαστικά συνδεδεμένες με την διοικητική λήψη αποφάσεων. Αυτή η προσέγγιση εξασφαλίζει ότι οι διαδικασίες αυτές ανταποκρίνονται στις στρατηγικές και τις προτεραιότητες του [Όνομα Οργανισμού]. Συγκεκριμένα:

Συγκεκριμένα:

1. Η διαδικασία ξεκινά με την καταγραφή ευπαθειών από την ασφάλεια πληροφοριών. Ειδικευμένες ομάδες πραγματοποιούν συστηματικές αξιολογήσεις και υποβάλλουν σχετικές εκθέσεις.
2. Οι εκθέσεις υποβάλλονται στη διοίκηση για ανάλυση και αξιολόγηση. Η διοίκηση αξιολογεί τη σοβαρότητα, τις επιπτώσεις και τις ανάγκες για αποκατάσταση.
3. Η διοίκηση λαμβάνει αποφάσεις σχετικά με την προτεραιότητα και τον τρόπο αντιμετώπισης των ευπαθειών. Αυτές οι αποφάσεις καθορίζουν την κατεύθυνση για την αποκατάσταση και τις απαραίτητες ενημερώσεις ασφάλειας.
4. Οι αποφάσεις μεταφράζονται σε δράσεις μέσω ελεγχόμενων διαδικασιών. Η υλοποίηση περιλαμβάνει τόσο αυτόματες ενημερώσεις όσο και δράσεις που απαιτούν την επέμβαση εξειδικευμένου προσωπικού.

# Ανίχνευση και Καταγραφή Ευπαθειών

Παρακάτω περιγράφεται μια ολοκληρωμένη διαδικασία ανίχνευσης και καταγραφής ευπαθειών:

1. Εντοπισμός Ευπαθειών:

Συστηματικοί έλεγχοι και δοκιμές για τον εντοπισμό πιθανών ευπαθειών σε εφαρμογές, συστήματα και δίκτυα.

1. Καταγραφή Ευπαθειών:

Οι ευπάθειες και οι ευαίσθητες περιοχές καταγράφονται σε ένα κεντρικό σύστημα διαχείρισης ευπαθειών, παρέχοντας ολοκληρωμένη εικόνα των ευπαθειών σε όλο τον οργανισμό.

1. Ανάλυση Ευπαθειών:

Αναλυτική αξιολόγηση και κατηγοριοποίηση των ευπαθειών, εκτιμώντας τον βαθμό κινδύνου και τις επιπτώσεις.

1. Αναφορά Ευπαθειών:

Οι ευπάθειες και οι αναλύσεις τους αναφέρονται σε εκθέσεις που προωθούνται σε αρμόδιους φορείς, συμπεριλαμβανομένων των ανωτάτων στελεχών, για λήψη αποφάσεων και ενεργειών.

1. Αποκατάσταση και Ενημέρωση:

Αφού ολοκληρωθούν οι αναλύσεις, ακολουθεί άμεση αποκατάσταση των ευπαθειών και ενημέρωση των συστημάτων και των διαδικασιών του οργανισμού.

1. Συνεχής Βελτίωση:

Η διαδικασία επανεκτιμάται και βελτιώνεται διαρκώς, λαμβάνοντας υπόψη νέες απειλές και εξελίξεις στον τομέα της κυβερνοασφάλειας.

Με αυτήν τη διαδικασία, διασφαλίζουμε ότι η ανίχνευση, η καταγραφή και η αντιμετώπιση των ευπαθειών είναι ολοκληρωμένες, γρήγορες και αποτελεσματικές, διατηρώντας την υψηλή ασφάλεια των πληροφοριών μας.

# Συσσώρευση Συμβάντων

1.
2. 1.
	2.
	3.
	4.

### Συγκέντρωση Ημερολογίων

* Η συγκέντρωση των ημερολογίων πρέπει να είναι αυτοματοποιημένη στο μέγιστο.
* Η συγκέντρωση ημερολογίων πρέπει να γίνεται με τη βοήθεια εργαλείου συγκέντρωσης ημερολογίων και συσχέτισης αδυναμιών των συστημάτων (SIEM, event log manager ).
* Τα ημερολόγια και τα συμβάντα πρέπει να φιλτράρονται κατά τη συλλογή τους. Συνιστάται να φιλτράρονται τα αποδεκτά συμβάντα.
* Τα κρίσιμα συμβάντα των κρίσιμων συστημάτων, εφαρμογών, δικτυακών συσκευών του [Όνομα Οργανισμού] ή αυτών που εξυπηρετούν τον [Όνομα Οργανισμού] πρέπει να αποθηκεύονται και να ελέγχονται.

### Ανάλυση Ημερολογίων

* Η ανάλυση των ημερολογίων πρέπει να είναι αυτοματοποιημένη στο μέγιστο.
* Τα ημερολόγια για το κάθε πληροφοριακό σύστημα πρέπει να ελέγχονται σε καθημερινή βάση από τους διαχειριστές του συστήματος.
* Οι βασικοί έλεγχοι στα ημερολόγια πρέπει να συμπεριλαμβάνουν τα εξής:
	+ Λογαριασμούς χρηστών.
	+ Ημερομηνίες και ώρα σύνδεσης (σύνδεση και αποσύνδεση από το σύστημα).
	+ Όνομα και IP διεύθυνση των συστημάτων αφετηρίας και προορισμού.
	+ Επιτυχή, ανεπιτυχή σύνδεση.
	+ Επιτυχή, ανεπιτυχή προσπάθεια αλλαγής κωδικού και δικαιωμάτων.
	+ Ημερολόγια προσπαθειών πρόσβασης στα δεδομένα (επιτυχείς, ανεπιτυχείς).
	+ Ημερολόγια προσπαθειών πρόσβασης ή αλλαγής σε βάσεις δεδομένων (επιτυχείς, ανεπιτυχείς).
	+ Ημερολόγια πρόσβασης πόρων (επιτυχής, ανεπιτυχής).
	+ Log of the action(s) performed/executed.
* Σε περίπτωση ανίχνευσης συμβάντων που απειλούν την ασφάλεια των πληροφοριακών συστημάτων ή/και πληροφοριών πρέπει να εφαρμόζονται διαδικασίες Άμεσης Ανταπόκρισης Περιστατικών Ασφαλείας.

### Συσχετισμός

* Ο συσχετισμός πρέπει να είναι αυτοματοποιημένος στο μέγιστο.
* Το λογισμικό πρέπει να συσχετίζει τις συγκεντρωμένες πληροφορίες από τα Ελεγχόμενα Συστήματα ούτως ώστε να υπάρχει διαφάνεια τυχόν ευπαθειών.
* Γραφικές παραστάσεις/απεικονίσεις, σε πραγματικό χρόνο, της απόδοσης των συστημάτων και των δικτύων, πρέπει να μπορούν να δημιουργηθούν με τη βοήθεια των εργαλείων ή άλλων επιπρόσθετων εργαλείων. Συνιστάται η απεικόνιση των πληροφοριακών συστημάτων ολόκληρης της υποδομής και των συστημάτων του [Όνομα Οργανισμού] σε διάφορα επίπεδα λεπτομέρειας.
* Αναφορές σχετικά με το συσχετισμό πρέπει να ελέγχονται σε καθημερινή βάση σε συνεργασία με το διαχειριστή του συστήματος για τυχόν ευπάθειες.
* Σε περίπτωση κρίσιμου περιστατικού πρέπει να εφαρμόζονται διαδικασίες Άμεσης Ανταπόκρισης Περιστατικών Ασφαλείας.

### Αποθήκευση και προστασία των ημερολογίων

Τα ημερολόγια θα πρέπει να αποθηκεύονται και να διατηρούνται για τουλάχιστο **[Ορίστε χρονικό διάστημα σε μήνες]**. Σε περίπτωση περιστατικού/συμβάν τα ημερολόγια πρέπει να διατηρούνται για **[Ορίστε χρονικό διάστημα σε χρόνια]** ή μέχρι τη λήξη του περιστατικού. Σημειώνεται ότι η πιο πάνω περίοδος διατήρησης, ενδέχεται να διαφοροποιείται σε περίπτωση όπου καθορίζεται διαφορετικά με βάση το Κανονιστικό Πλαίσιο και το Retention Policy του [Όνομα Οργανισμού].

Επιπρόσθετα η ακεραιότητα των ημερολόγιών θα πρέπει να διασφαλίζεται. Τα ημερολόγια πρέπει να πιστοποιούνται όταν αποθηκεύονται. Κανένας δεν πρέπει να είναι σε θέση να τροποποιήσει τα ημερολόγια. Νοείται ότι τα ημερολόγια δεν πρέπει να είναι προσβάσιμα από μη εξουσιοδοτημένους χρήστες.

# Διαχείριση Ευπαθειών και Τρωτότητας

# Αξιολόγηση και Αποκατάσταση Ευπαθειών

Αξιολόγηση και αποκατάσταση ευπαθειών είναι μια μέθοδος αξιολόγησης της ασφάλειας σε πληροφοριακά συστήματα που εξετάζει τις παρεχόμενες υπηρεσίες, θύρες δικτύων, λογαριασμούς, εφαρμογές και λειτουργικά συστήματα. Στη συνέχεια συγκρίνει τα αποτελέσματα με μια βάση δεδομένων που περιλαμβάνει γνωστές ευπάθειες (known vulnerabilities).

* Η αξιολόγηση και αποκατάσταση ευπαθειών πρέπει να πραγματοποιείται με δοκιμασμένες μεθοδολογίες.
* Η αξιολόγηση και αποκατάσταση ευπαθειών πρέπει να εκτελείται με τη βοήθεια εργαλείου/ων σάρωσης και αποκατάστασης ευπαθειών (vulnerability scanner and patch management)
* Τα εργαλεία συνιστάται να συμμορφώνονται με τις διεθνείς νομοθεσίες, κανονισμούς και πρότυπα.
* Η αξιολόγηση και αποκατάσταση ευπαθειών πρέπει να πραγματοποιείται από αξιόπιστα και καταρτισμένα άτομα με reactive και ad-hoc τρόποΑξιολόγηση Ευπαθειών
* Η αξιολόγηση ευπαθειών πρέπει να εκτελείται **σε μηνιαία βάση**, κατά την αλλαγή μιας υπηρεσίας/συστήματος και κατά την υλοποίηση μιας καινούριας υπηρεσίας/συστήματος.
* Η αξιολόγηση ευπαθειών πρέπει να περιλαμβάνει μεταξύ άλλων την ανίχνευση:
	+ Ανοικτών δικτυακών θυρών (open ports)
	+ Περιττών υπηρεσιών
	+ Περιττών λογισμικών
	+ Περιττών κοινών φακέλων στο δίκτυο
	+ Περιττών λογαριασμών χρηστών
	+ Ανενεργών λογαριασμών
	+ Αδύνατων ή κενών κωδικών πρόσβασης
	+ Missing service packs, patches and fixes
	+ Κακόβουλων λογισμικών
	+ Λανθασμένων ρυθμίσεων και διαμορφώσεων των πληροφοριακών συστημάτων
* End of life συστημάτων και εφαρμογών
* Τα ευρήματα πρέπει να κατηγοριοποιούνται με βάση επίπεδο κινδύνου
* Τα αποτελέσματα της αξιολόγησης ευπαθειών πρέπει να αποστέλλονται στους Επιχειρησιακούς Ιδιοκτήτες των συστημάτων με κοινοποίηση στο [αρμόδιο τμήμα εσωτερικού ελέγχου] Τα αποτελέσματα πρέπει να αποστέλλονται σε μορφή έκθεσης, [ορίστε συχνότητα] ή κατά την ανάπτυξη/αλλαγή μιας καινούριας υπηρεσίας ή/και συστήματος. Η έκθεση πρέπει να χρησιμοποιείται για την αξιολόγηση επικινδυνότητας.
* Η Αξιολόγηση ευπαθειών πρέπει να συμμορφώνεται με τις πολιτικές και διαδικασίες του [Όνομα Οργανισμού].

# Αποκατάσταση Ευπαθειών

Το χρονικό διάστημα αποκατάστασης των ευπαθειών ορίζεται ανάλογα με το επίπεδο κινδύνου της ευπάθειας.

* + Ευπάθειες πολύ υψηλού κινδύνου τουλάχιστον σε διάστημα **[χ ημέρες]**
	+ Ευπάθειες υψηλού κινδύνου τουλάχιστον σε διάστημα **[χ ημέρες]**
	+ Ευπάθειες μεσαίου κινδύνου τουλάχιστον σε διάστημα **[χ ημέρες]**
	+ Ευπάθειες χαμηλού κινδύνου τουλάχιστον σε διάστημα **[χ ημέρες]**
* Τα αποτελέσματα της αποκατάστασης ευπαθειών πρέπει να παραδίδονται σε μορφή έκθεσης Η έκθεση πρέπει να χρησιμοποιείται για την αξιολόγηση επικινδυνότητας.

# Σχέδιο και προσέγγιση βάσει κινδύνου

Ο [Όνομα Οργανισμού] θα πρέπει να έχει καταρτήσει, εφαρμόσει και διατηρεί σχέδιο και προσέγγιση βάσει του κινδύνου για τη δοκιμή εφαρμογών, συστημάτων και δικτύων για ευπάθειες και αδυναμίες, οι οποίες θα μπορούσαν να τύχουν εκμετάλλευσης από απειλές.

# Πολιτική αποκατάστασης ευπαθειών

Ο [Όνομα Οργανισμού] θα πρέπει να έχει ενεργοποιήσει ή εφαρμόζει πολιτική για την αποκατάσταση ευπαθειών μέσω αυτόματης εγκατάστασης ενημερώσεων ή μέσω εξουσιοδοτημένο προσωπικό που ελέγχει πρώτα τις ενημερώσεις και στην συνέχεια διενεργεί τις σχετικές εγκαταστάσεις.

1. Αυτόματη Εγκατάσταση Ενημερώσεων:

Η πολιτική προβλέπει την αυτόματη εγκατάσταση ενημερώσεων για λογισμικά, λειτουργικά συστήματα και εφαρμογές. Αυτή η διαδικασία εξασφαλίζει όχι μόνο την ταχύτητα αλλά και τη συνέχεια στην εφαρμογή των κρίσιμων ενημερώσεων για την ασφάλεια των συστημάτων.

1. Έλεγχος από Εξουσιοδοτημένο Προσωπικό:

Ομάδα εξειδικευμένου προσωπικού που είναι υπεύθυνο για τον έλεγχο των ενημερώσεων πριν από την εγκατάστασή τους. Αυτό εξασφαλίζει τη συμβατότητα και αξιοπιστία των ενημερώσεων που εισέρχονται στο σύστημά του οργανισμού.

Με αυτήν τη συνδυασμένη προσέγγιση, εξασφαλίζεται όχι μόνο η άμεση αντιμετώπιση ευπαθειών μέσω αυτόματων ενημερώσεων αλλά και ο προσεκτικός έλεγχος από εξειδικευμένο προσωπικό, διασφαλίζοντας τη συνολική ασφάλεια των συστημάτων του [Όνομα Οργανισμού].

# Αποκατάσταση Ευπαθειών με Έγκριση της Διοίκησης

Η στρατηγική αποκατάστασης των ευπαθειών ακολουθεί μια συνεκτική προσέγγιση, ενσωματώνοντας διαδικασίες που έχουν εγκριθεί από τη διοίκηση. Αναγνωρίζονται δύο βασικές κατηγορίες ενεργειών:

1. Αυτόματες Ενέργειες:

Ορισμένες ευπάθειες αντιμετωπίζονται αυτόματα, χωρίς προηγούμενη δοκιμή. Παραδείγματα περιλαμβάνουν την εφαρμογή αυτόματων ασφαλειακών ενημερώσεων και την ενεργοποίηση εκ των προτέρων καθορισμένων πολιτικών ασφαλείας.

1. Ενέργειες Μετά τον Έλεγχο:

Κάποιες ευπάθειες απαιτούν προσεκτικό έλεγχο πριν από την αποκατάσταση. Μετά την αυτόματη αναγνώριση, επιτελείται προσεκτικός έλεγχος και δοκιμή για να διασφαλιστεί η αποτελεσματική αποκατάσταση.

# Διαδικασίες ασφάλειας ευπαθειών

Ο [Όνομα Οργανισμού] θα πρέπει να έχει θεσπίσει, εφαρμόζει και διατηρεί διαδικασίες για την αποκατάσταση ευπαθειών και την εισαγωγή ενημερώσεων ασφάλειας για ευπάθειες που εντοπίζονται σε συστήματα, εφαρμογές και στοιχεία δικτύου, και τα οποία απαιτούν μετριασμό ως αποτέλεσμα της αξιολόγησης της διοίκησης. Αυτές οι διαδικασίες μπορούν να περιλαμβάνουν:

1. Συστηματικές αξιολογήσεις για τον εντοπισμό ευπαθειών σε συστήματα, εφαρμογές και δίκτυα.
2. Καθορισμός προτεραιοτήτων για την άμεση αντιμετώπιση των ευπαθειών που ανακαλύπτονται, αναλαμβάνοντας γρήγορες και αποτελεσματικές δράσεις.
3. Ανάπτυξη ενημερώσεων ασφάλειας που καλύπτουν τις ευπάθειες που εντοπίζονται, προκειμένου να προληφθούν περαιτέρω προβλήματα.
4. Ελεγχόμενη διαδικασία για την εισαγωγή ενημερώσεων, ελέγχοντας πρώτα τη συμβατότητα και την αξιοπιστία τους.

Συνεχής αξιολόγηση των ευπαθειών και ενημερώνουμε των διαδικασιών του οργανισμού, προσαρμόζοντας τις στις συνεχώς εξελισσόμενες κυβερνοαπειλές.

# Εφαρμογή ενεργειών

Να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών.

# Ταξινόμηση και επισήμανση πληροφοριών

Να εξασφαλιστεί ότι τα δεδομένα ταξινομούνται και επισημαίνονται κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους.

# Διαχείριση αλλαγών

Να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα ή η αυθεντικότητα των πληροφοριών [CM1]. Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης αλλαγών για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας.

1. Αναγνώριση Ανάγκης:

Καθορισμός των αναγκών για αλλαγή, είτε λόγω εσωτερικών παραγόντων όπως βελτιστοποίηση των διαδικασιών, είτε λόγω εξωτερικών παραγόντων όπως νομοθετικές αλλαγές.

1. Σχεδιασμός Αλλαγών:

Καθορισμός λεπτομερών σχεδίων για την υλοποίηση των αλλαγών, συμπεριλαμβανομένων των αναγκαίων πόρων, των χρονοδιαγραμμάτων και των υπεύθυνων.

1. Ενημέρωση Εμπλεκόμενων Μερών:

Ενημέρωση του προσωπικού και των εμπλεκόμενων μερών σχετικά με τις αλλαγές που πρόκειται να εφαρμοστούν, παρέχοντας σαφείς επεξηγήσεις και εκπαιδεύοντας όπου κρίνεται απαραίτητο.

1. Υλοποίηση Αλλαγών:

Εφαρμογή των σχεδιασμένων αλλαγών στο περιβάλλον του οργανισμού.

1. Επισκόπηση και Επικοινωνία:

Παρακολούθηση της αποτελεσματικότητας των αλλαγών, αξιολόγηση της αντίκτυπους, και επικοινωνία των αποτελεσμάτων στα ενδιαφερόμενα μέρη.

1. Προσαρμογή και Εκτίμηση:

Συνεχής εκτίμηση των αλλαγών και προσαρμογή των σχεδίων ανάλογα με τις επιδόσεις και τις ανάγκες του οργανισμού.

1. 1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.

### Αποκατάσταση Ευπαθειών με Βάση τη Διαδικασία Διαχείρισης Αλλαγών

Η αποκατάσταση ευπαθειών ενσωματώνεται στην ευρύτερη διαδικασία διαχείρισης αλλαγών, διασφαλίζοντας όχι μόνο την ασφάλεια αλλά και τη συνοχή των συστημάτων και των διαδικασιών του οργανισμού. Η διαδικασία αυτή περιλαμβάνει τα εξής βήματα:

1. Καταγραφή Ευπαθειών:

Οι ευπαθείς περιοχές αναγνωρίζονται κατά την αξιολόγηση ασφαλείας. Οι ευπαθείς περιοχές αυτές καταγράφονται ως αλλαγές που απαιτούν προσοχή.

1. Αξιολόγηση Σοβαρότητας:

Ορίζεται η σοβαρότητα κάθε ευπάθειας και η επιρροή της στο περιβάλλον μας. Κρίνεται εάν απαιτείται άμεση αντιμετώπιση.

1. Καταγραφή στο Σύστημα Διαχείρισης Αλλαγών:

Οι ευπαθείς περιοχές καταγράφονται επίσημα στο σύστημα διαχείρισης αλλαγών, καθορίζοντας περαιτέρω δράσεις.

1. Αξιολόγηση Κινδύνου και Σχεδιασμός:

Εκτιμάται ο κίνδυνος που συνδέεται με κάθε ευπάθεια και σχεδιάζονται οι αντίστοιχες δράσεις αποκατάστασης.

1. Επικοινωνία και Ενημέρωση:

Οι εμπλεκόμενοι ενημερώνονται για τις αλλαγές που πρόκειται να υλοποιηθούν και οι δράσεις αποκατάστασης.

1. Υλοποίηση και Παρακολούθηση:

Οι απαραίτητες δράσεις αποκατάστασης υλοποιούνται με τη συμμετοχή των επιχειρησιακών ομάδων. Ολοκληρώνονται με προσεκτική παρακολούθηση για την επιτυχή έκβαση.

# Δοκιμές Διείσδυσης

Δοκιμή διείσδυσης είναι μια μέθοδος αξιολόγησης της ασφάλειας σε πληροφοριακά συστήματα με προσομοίωση μιας επίθεσης από εισβολέα. Η διαδικασία περιλαμβάνει την ενεργό ανάλυση του συστήματος για τυχόν αδυναμίες, τεχνικές ατέλειες ή τρωτά σημεία.

* Οι δοκιμές διείσδυσης πρέπει να υλοποιούνται με δοκιμασμένες μεθοδολογίες και αξιόπιστα εργαλεία.
* Οι δοκιμές διείσδυσης πρέπει να υλοποιούνται από εξουσιοδοτημένα, αξιόπιστα και καταρτισμένα άτομα από το **[αρμόδιο Τμήμα]**
	+ Οι δοκιμές διείσδυσης δύναται να εκτελεστούν σε ανύποπτο χρονικό διάστημα από τις αρμόδιες Υπηρεσίες/Μονάδες ή εξωτερικούς συμβούλους για σκοπούς αξιολόγησης του ευρύτερου πλαισίου ασφάλειας του [Όνομα Οργανισμού] και του βαθμού ανταπόκρισης σε ενδεχόμενα πραγματικά περιστατικά.
	+ Πριν την οποιαδήποτε δοκιμή διείσδυσης πρέπει να ενημερώνεται τουλάχιστον ο Ιδιοκτήτης του συστήματος και ο [Υπεύθυνος Ασφάλειας Πληροφοριών].
* Παρόλο που οι δοκιμές διείσδυσης πρέπει να εκτελούνται σε ετήσια βάση, συνιστάται οι δοκιμές διείσδυσης να εκτελούνται **κάθε 6 (έξι) μήνες** τουλάχιστον για τα κρίσιμα συστήματα. Επίσης πρέπει να εκτελούνται δοκιμές διείσδυσης κατά την ανάπτυξη μιας καινούργιας υπηρεσίας ή κατά την αλλαγή μιας υφιστάμενης υπηρεσίας.
* Στις περιπτώσεις που οι δοκιμές διείσδυσης εκτελούνται από εξωτερικούς συνεργάτες θα πρέπει να λαμβάνεται υπόψη η ανάθεση σε διαφορετικούς συνεργάτες **κάθε 2 (δυο) χρόνια**.
* Οι δοκιμές διείσδυσης πρέπει να περιλαμβάνουν τις πιο κάτω φάσεις.
	+ Footprinting and Reconnaissance
	+ Scanning and Enumeration
	+ Gaining Access
	+ Maintain Access
	+ Clearing Track
* Οι δοκιμές διείσδυσης πρέπει να περιλαμβάνουν σενάρια εισβολής τόσο από το εσωτερικό όσο και από το εξωτερικό δίκτυο του [Όνομα Οργανισμού]. Επίσης, οι δοκιμές πρέπει να εκτελούνται με τις ακόλουθες προσεγγίσεις Blind, Double Blind, Gray Box, Double Gray Box, Tandem, and Reversal. Οι δοκιμές αυτές, μεταξύ άλλων πρέπει να περιλαμβάνουν τα εξής:
	+ Δοκιμές εντοπισμού ή/και σπασίματος κωδικού πρόσβασης (password cracking)
	+ Σάρωση για περιμετρικές ευπάθειες (Perimeter Vulnerability Scan)
	+ Δοκιμές διείσδυσης περιμέτρου (Perimeter Penetration Test)
	+ Δοκιμές διείσδυσης ασύρματων δικτύων (Wireless Penetration Test)
	+ Δοκιμές διείσδυσης από το εσωτερικό (Internal Penetration Test)
	+ Social Engineering Test
	+ Web Application Test
	+ Database Test
	+ Software Development Life Cycle (SDLC) integrated testing.
	+ Διαδικασίες
* Τα αποτελέσματα των δοκιμών διείσδυσης πρέπει να παραδίδονται σε μορφή έκθεσης. Η έκθεση πρέπει να χρησιμοποιείται για την αξιολόγηση επικινδυνότητας και πρέπει να περιλαμβάνει τουλάχιστο τα ακόλουθα:
	+ λεπτομερή έκθεση όλων των περιστατικών που συνέβησαν,
	+ δραστηριότητες που πραγματοποιήθηκαν, κατά τη διάρκεια της δοκιμής,
	+ οποιεσδήποτε άλλες παρατηρήσεις κατά τις δοκιμές
	+ ευρήματα (ευπάθειες και κενά ασφαλείας). Τα ευρήματα πρέπει να προσδιορίζονται με επίπεδο κινδύνου (critical, major, high, medium, low)
	+ προτεινόμενες λύσεις και το κόστος τους.

# Διορθωτικές Ενέργειες και Διαχείριση Ευπαθειών Ασφάλειας

Ο [Όνομα Οργανισμού] αναγνωρίζει την ολοένα και αυξανόμενη σημασία της διαχείρισης ευπαθειών και της υλοποίησης αποτελεσματικών διορθωτικών ενεργειών για τη διασφάλιση της ασφάλειας. Παρατηρείται η προσέγγισή της προς τις διορθωτικές ενέργειες να είναι πολύ συχνά "reactive" και "ad-hoc," δηλαδή αντιδραστική και συχνά χωρίς προηγούμενο σχέδιο ή προσδιορισμένη προσέγγιση.

Για να αντιμετωπιστεί αυτή η πραγματικότητα, ο [Όνομα Οργανισμού] εφαρμόζει βελτιωμένες πρακτικές στον τομέα της ασφάλειας. Ακολουθούν ορισμένες αρχές για τη διαχείριση ευπαθειών και την υλοποίηση διορθωτικών ενεργειών:

1. Ανίχνευση Ευπαθειών (Vulnerability Detection):

Συστηματική αξιολόγηση και παρακολούθηση πολιτικών, διαδικασιών και τεχνολογιών για την ανίχνευση πιθανών ευπαθειών.

1. Άμεση Αντίδραση (Immediate Response):

Ανάληψη άμεσων δράσεων κατά τον εντοπισμό ευπαθειών για την αποτροπή πιθανών απειλών.

Παροχή αναφορών άμεσα σε κατάλληλα πρόσωπα και αρμόδιες αρχές.

1. Ανάπτυξη Κατάλληλων Διορθωτικών Μέτρων (Corrective Measures):

Σχεδιασμός και υλοποίηση διορθωτικών μέτρων που εξαλείφουν τις ευπαθείς σημεία και ενισχύουν το σύστημα ασφαλείας.

1. Συνεχής Αναθεώρηση (Continuous Review):

Εκ νέου αξιολόγηση των μέτρων ασφαλείας και πολιτικών κατά τακτικά χρονικά διαστήματα για την προσαρμογή σε νέες εξελίξεις και απειλές.

1. Ευελιξία και Προσαρμογή (Flexibility and Adaptation):

Χρήση Ad-hoc μέτρων όταν απαιτείται άμεση και ευέλικτη αντίδραση σε νέες απειλές ή ανακαλύπτονται αναπάντητες ευπαθείς πτυχές.

1. Συνεργασία και Κοινοποίηση Πληροφοριών (Collaboration and Information Sharing):

Ενθάρρυνση της συνεργασίας με εξωτερικούς εμπειρογνώμονες, οργανισμούς ασφαλείας, και άλλα ενδιαφερόμενα μέρη για την ανταλλαγή πληροφοριών και καλύτερη κατανόηση των απειλών.

# Κρίσιμα Συστήματα

Ο [Όνομα Οργανισμού] αναγνωρίζει την κρίσιμη σημασία της έγκαιρης ανίχνευσης και εντοπισμού ευπαθειών στα κρίσιμα συστήματα της. Θεσπίζει συγκεκριμένους μηχανισμούς προκειμένου να διασφαλίσει τη δημιουργία επαφών για την άμεση λήψη πληροφοριών και την αντιμετώπιση ευπαθειών. Οι παρακάτω μηχανισμοί ενισχύουν την ανταλλαγή πληροφοριών και τη συνεργασία εντός του οργανισμού:

1. Συστηματική συλλογή πληροφοριών σχετικά με τις απειλές και τις ευπαθείς πτυχές των κρίσιμων συστημάτων.
2. Δημιουργία στενών επαφών με ειδικούς ασφαλείας, εξωτερικούς οργανισμούς και κοινότητες για την ανταλλαγή εμπειριών και πληροφοριών.
3. Ενθάρρυνση της ανοιχτής επικοινωνίας και συνεργασίας με προμηθευτές και εταίρους προκειμένου να ανιχνεύονται και να διορθώνονται ευπαθείς σημεία.
4. Παροχή εκπαίδευσης στους εργαζομένους για τον ανίχνευση και την αντιμετώπιση ευπαθειών, καθώς και ενίσχυση της ευαισθητοποίησης για τη σημασία της ασφάλειας.
5. Επανεξέταση των μηχανισμών ανίχνευσης και εντοπισμού ευπαθειών κατά τακτικά χρονικά διαστήματα με σκοπό την βελτίωσή τους.
6. Διασφάλιση της εμπιστευτικότητας των πληροφοριών που σχετίζονται με ευπαθείς πτυχές, καθώς και της αποτελεσματικής προστασίας των διαδικτυακών και φυσικών πόρων.

# Σχέδιο Προσέγγισης για Έλεγχο Ευπαθειών

Σύμφωνα με τον Κανονισμό Κ.Δ.Π. 389/2020, Ο [Όνομα Οργανισμού] εξετάζει τον εντοπισμό ευπαθειών που προκύπτουν από νέες ή τροποποιημένες διαδικασίες ή συστήματα στα πλαίσια επεξεργασίας πληροφοριών. Οι ευπάθειες πρέπει να ανιχνεύονται και να εντοπίζονται στο πλαίσιο των απειλών κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Για τον σκοπό αυτό, εφαρμόζεται ένα σχέδιο προσέγγισης βάσει του κινδύνου για τη δοκιμή εφαρμογών, συστημάτων και δικτύων για ευπάθειες και αδυναμίες, οι οποίες θα μπορούσαν να τύχουν εκμετάλλευσης από απειλές [VM1].

Κυριότερα Σημεία:

1. Κατάρτιση Σχεδίου Κινδύνου:

 Έχουμε αναπτύξει ένα εκτενές σχέδιο κινδύνου που περιλαμβάνει ανάλυση κινδύνου για εφαρμογές, συστήματα και δίκτυα. Αυτή η ανάλυση βασίζεται σε κατηγορίες κινδύνου και προσδιορίζει τις πλέον ευπαθείς περιοχές.

1. Συστηματική Δοκιμή Ευπαθειών:

 Εφαρμόζουμε συστηματικές διαδικασίες δοκιμής ευπαθειών σε εφαρμογές, συστήματα και δίκτυα μας. Αυτές οι δοκιμές περιλαμβάνουν σενάρια που εκτιμούν την ανθεκτικότητα των πληροφοριακών μας πόρων.

1. Αξιολόγηση Κρίσιμων Σημείων:

 Καθορίζουμε και αξιολογούμε τα κρίσιμα σημεία ευπαθειών, δηλαδή τις περιοχές που, εάν παραβιαστούν, θα επηρεάσουν σοβαρά τη λειτουργικότητα και την ασφάλεια του οργανισμού.

1. Διαδικασίες Διαχείρισης Ευπαθειών:

 Διαθέτουμε συστηματικές διαδικασίες διαχείρισης ευπαθειών που περιλαμβάνουν την ταχεία επιδιόρθωση και τον ενημερωμένο έλεγχο.

1. Εφαρμογή Κατάλληλων Τεχνολογιών:

Χρησιμοποιούμε σύγχρονες τεχνολογίες για την ανίχνευση και τον έλεγχο ευπαθειών, συμπεριλαμβανομένων αυτόματων συστημάτων εντοπισμού κινδύνων.

# Ανταπόκριση σε Ευπάθειες Κρίσιμης Σημασίας

Θέσπιση, εφαρμογή και διατήρηση μιας πολιτικής ταξινόμησης και επισήμανσης που διασφαλίζει την ταξινόμηση και επισήμανση των πληροφοριών, σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους. Εξέταση ενδεχομένου εφαρμογής συστημάτων ταξινόμησης και επισήμανσης με βάση τις διεθνείς και βιομηχανικές βέλτιστες πρακτικές, όπως το πρωτόκολλο «Traffic Light Protocol» [DS2].

Αντιμετώπιση των ευπαθειών κρίσιμης σημασίας, καθορίζοντας σαφείς διαδικασίες ανταπόκρισης για κάθε κατηγορία στοιχείων του ενεργητικού μας. Η ανταπόκρισή του [Όνομα Οργανισμού] εστιάζεται σε πολλά επίπεδα, αναλύοντας τον ενιαίο κατάλογο στοιχείων ενεργητικού:

1. Κρίσιμα Δεδομένα:

• Τα κρίσιμα δεδομένα αναγνωρίζονται και κατηγοριοποιούνται. Δημιουργούνται σχέδια άμεσης ανακάλυψης και αναστολής λειτουργίας για την αντιμετώπιση πιθανών περιστατικών παραβίασης.

1. Κρίσιμα Συστήματα:

• Ενημερωμένος κατάλογος των κρίσιμων συστημάτων, και ανάπτυξη σχεδίων ανάκαμψης και επαναφοράς για τη διασφάλιση της συνεχούς λειτουργίας.

1. Κρίσιμα Δίκτυα:

• Τακτικοί έλεγχοι ευπαθειών και εφαρμογή προληπτικών μέτρων για την εξάλειψή τους.

1. Κρίσιμες Εφαρμογές:

• Καταγραφή ευπαθειών στις κρίσιμες εφαρμογές και δημιουργία σχεδίων αντιμετώπισης για τη διασφάλιση της σταθερής λειτουργία τους.