Όνομα Οργανισμού

Πολιτική Διαχείρισης Ευπαθειών και Τρωτότητας

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διαχείρισης Ευπαθειών και Τρωτότητας |
| **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

[Πίνακας Περιεχομένων 3](#_Toc184816663)

[1. Εισαγωγή 4](#_Toc184816664)

[1.1 Σκοπός 4](#_Toc184816665)

[1.2 Πεδίο Εφαρμογής 4](#_Toc184816666)

[2. Πολιτική Διαχείρισης Ευπαθειών και Τρωτότητας 4](#_Toc184816667)

[2.1. Ελεγχόμενα συστήματα 4](#_Toc184816668)

[2.2. Ανίχνευση και εντοπισμός ευπαθειών και τρωτότητας 5](#_Toc184816669)

[2.3. Καταγραφή και αναφορά ευπαθειών 6](#_Toc184816670)

[2.4. Αποκατάσταση ευπαθειών και ενημερώσεις ασφάλειας 7](#_Toc184816671)

[3. Διαδικασία Διαχείρισης Ευπαθειών και Τρωτότητας 9](#_Toc184816672)

[3.1. Αξιολόγηση και Αποκατάσταση Ευπαθειών 9](#_Toc184816673)

[3.2. Αποκατάσταση Ευπαθειών 10](#_Toc184816674)

[3.3. Σχέδιο και προσέγγιση βάσει κινδύνου 10](#_Toc184816675)

[3.4. Πολιτικές αποκατάστασης ευπαθειών 10](#_Toc184816676)

[3.5. Εφαρμογή ενεργειών 11](#_Toc184816677)

[4. Δοκιμές Διείσδυσης (Penetration Testing) 11](#_Toc184816678)

[5. Μηχανισμοί ευαισθητοποίησης και κανάλια επικοινωνίας 12](#_Toc184816679)

[6. Αναθεώρηση 14](#_Toc184816680)

[7. Αναφορές 14](#_Toc184816681)

# Εισαγωγή

## Σκοπός

Σκοπός της παρούσας Πολιτικής Διαχείρισης Ευπαθειών και Τρωτότητας είναι ο καθορισμός κατευθυντήριων γραμμών για τη διαχείριση ευπαθειών των πληροφοριακών πόρων του [Όνομα Οργανισμού]. Σκοπός των κατευθυντήριων γραμμών είναι ο έγκαιρος εντοπισμός και η αποκατάσταση των υφιστάμενων, αλλά και καινούργιων ευπαθειών στα πληροφοριακά συστήματα του [Όνομα Οργανισμού]. Αυτό επιτυγχάνεται μέσω μίας στρατηγικής 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.

## Πεδίο Εφαρμογής

Η παρούσα πολιτική διαχείρισης ευπαθειών εφαρμόζεται σε όλα τα πληροφοριακά συστήματα, τις εφαρμογές και τις δικτυακές υποδομές του [Όνομα Οργανισμού]. Περιλαμβάνει όλες τις διαδικασίες και τα εργαλεία που χρησιμοποιούνται για τον εντοπισμό και την αξιολόγηση των ευπαθειών και τρωτότητας, καθώς και τις ενέργειες που απαιτούνται για την αποκατάστασή τους. Η πολιτική αυτή ισχύει για όλα τα τμήματα και τους υπαλλήλους του [Όνομα Οργανισμού], καθώς και για τους εξωτερικούς συνεργάτες και προμηθευτές που δραστηριοποιούνται εκ μέρους του [Όνομα Οργανισμού] και έχουν πρόσβαση στα συστήματα και τις υποδομές του Οργανισμού.

# Πολιτική Διαχείρισης Ευπαθειών και Τρωτότητας

# Ελεγχόμενα συστήματα

Τα ημερολόγια καταγραφής ενεργειών συστημάτων(log books) του [Όνομα Οργανισμού] συγκεντρώνονται, αναλύονται να συσχετίζονται σε κεντρικό σύστημα διαχείρισης ενεργειών τύπου SIEM (Security Information and Events Management System). Στόχος είναι να αποφεύγονται εξ ολοκλήρου ή/και να επιτυγχάνεται η άμεση ανταπόκριση των ευπαθειών ή της κακόβουλης εισβολής στα πληροφοριακά συστήματα και πληροφορίες

Σε περιπτώσεις όπου απαιτείται από κάποιο κανονιστικό πλαίσιο, τα ημερολόγια καταγραφής ενεργειών συστημάτων θα πρέπει να αποθηκεύονται και διατηρούνται για μια συγκεκριμένη χρονική περίοδο ανάλγοα με την εκάστοτε απαίτηση. Η χρονική περίοδος διατήρησης των ημερολόγιων για το κάθε σύστημα δύναται να είναι διαφορετική.

Απαιτείται η συγκέντρωση ενεργειών 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.

Όλος ο πιο πάνω εξοπλισμός πρέπει να είναι συγχρονισμένος με κεντρικό σύστημα πρωτοκόλλου ώρας δικτύου (ntp) για τον ομοιόμορφο καθορισμό της ώρας / ημερομηνίας. H ακριβής ώρα είναι ζωτικής σημασίας για την ορθή λειτουργία των διαφόρων λειτουργιών του δικτύου, των πρωτοκόλλων ασφαλείας και των αρχείων καταγραφής ενεργειών εξασφαλίζοντας ορθότερη ανάλυση κατά τη διάρκεια ελέγχων ή ερευνών περιστατικών.

# Ανίχνευση και εντοπισμός ευπαθειών και τρωτότητας

Η γρηγορότερη ανίχνευση και ο εντοπισμός ευπαθειών είναι μια κρίσιμη διαδικασία στην ασφάλεια στον κυβερνοχώρο. Η διαδικασία αυτή περιλαμβάνει τις πιο κάτω προσεγγίσεις:

* + - Για την ανίχνευση ευπαθειών στα κρίσιμα συστήματα του [Όνομα Οργανισμού], έχουν εγκατασταθεί μηχανισμοί και έχουν δημιουργηθεί επαφές που εξασφαλίζουν την έγκαιρη λήψη πληροφοριών σχετικά με πιθανές απειλές και ευπάθειες.
    - Η διαδικασία ανίχνευσης και εντοπισμού ευπαθειών εφαρμόζεται όταν προκύπτουν νέες τροποποιημένες διαδικασίες ή συστήματα στα πλαίσια επεξεργασίας πληροφοριών και να λαμβάνει υπόψιν απειλές κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών του [Όνομα Οργανισμού].
    - Η ανίχνευση ευπαθειών πρέπει να γίνεται τουλάχιστον ανά τρίμηνο για εσωτερικά συστήματα, και τουλάχιστον κάθε μήνα για εξωτερικά εκτεθειμένα συστήματα.
    - Ο [Όνομα Οργανισμός] χρησιμοποιεί αυτοματοποιημένα μέσα και εργαλεία για την ανίχνευση και τον εντοπισμό ευπαθειών, τα οποία ακολουθούν και συμμορφώνονται με τις διεθνείς βέλτιστες πρακτικές.
    - Τα δεδομένα σχετικά με τις ευπάθειες πρέπει να ενσωματώνονται στη διαδικασία διαχείρισης κινδύνων και να χρησιμοποιούνται στα πλαίσια επιλογής των κατάλληλων μέτρων αντιμετώπισης και της αποκατάστασης ως μέρος του Σχεδίου Αντιμετώπισης Κινδύνων σύμφωνα με την απαίτηση VM3 της Απόφασης Κ.Δ.Π 389/2020.
    - Τα αποτελέσματα των ανιχνεύσεων πρέπει να καταγράφονται και να υποβάλλονται σε σχετικές εκθέσεις. Βλέπε παράγραφο 2.3 πιο κάτω.
    - Όπου είναι δυνατό ο [Όνομα Οργανισμός] συμμετέχει και λαμβάνει έγκυρες πληροφορίες Cyber threat intelligence οι οποίες μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο [Όνομα Οργανισμός].
    - Τα δεδομένα από τις αξιολογήσεις ευπαθειών (vulnerability assessments) πρέπει να αξιοποιούνται ως βάση για την αποτελεσματικότερη στόχευση των δοκιμών παρείσδυσης (penetration tests). Αυτές οι δοκιμές, οι οποίες περιλαμβάνουν μεθοδολογίες όπως white box και grey box, πρέπει να ενσωματώνονται σε ένα καλά καθορισμένο σχέδιο δοκιμών και να πραγματοποιούνται ετησίως.
    - Το σχέδιο δοκιμών παρείσδυσης (penetration test) θα πρέπει να περιλαμβάνει:
  + το πεδίο εφαρμογής τους (π.χ. δικτύου, web applications, APIs, hosted υπηρεσίες, μέτρα φυσικής πρόσβασης κα.)
  + τους περιορισμούς (π.χ. τις ώρες που μπορεί να διενεργηθεί, το προσωπικό που πρέπει να ενημερωθεί κ.α)
  + τα είδη των δοκιμών που θα διενεργηθούν
  + τις σχετικές μεθοδολογίες και πρότυπα
  + την συχνότητα διενέργειας
  + τον στόχο
  + τους ρόλους και αρμοδιότητες
  + το είδος της τεκμηρίωσης που θα διατηρηθεί και θα παραδοθεί στον Οργανισμό,
  + τα σημεία επαφής
  + ένα πλάνο άμεσων ενεργειών σε περίπτωση ευρήματος.

# Καταγραφή και αναφορά ευπαθειών

Ο [Όνομα Οργανισμού] 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 διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών. Η καταγραφή αυτή αποτελεί τον βασικό πυλώνα για την ανάλυση και τη διαχείριση των πιθανών απειλών που ενδέχεται να επηρεάσουν την ασφάλεια των πληροφοριών.

Το σύνολο των ευπαθειών καταγράφεται σε σχετικό κατάλογο απειλών ή βάση δεδομένων, ευπαθειών και κινδύνων. Η τακτική ενημέρωση και αξιολόγηση του καταλόγου συμβάλει στην πρόληψη και αντιμετώπιση ενδεχόμενων κινδύνων.

Μέσω της καταγραφής θα πρέπει να αναφέρονται και να συμπεριλαμβάνονται στοιχεία για υψηλού κινδύνου ευπάθειες με σκοπό την ενημέρωση στελεχών της διοίκησης, ώστε να είναι δυνατή η λήψη τεκμηριωμένων αποφάσεων από αυτήν όσον αφορά τον χειρισμό τους σύμφωνα με την απαίτηση VM2 της Απόφασης Κ.Δ.Π 389/2020.

Πρέπει να αξιολογείται το επίπεδο της ευπάθειας λαμβάνοντας υπόψη την δυνατότητα εκμετάλλευσης (exploitability) και την πιθανή επίπτωση της ευπάθειας ανά περίπτωση και ανά κατηγορία στοιχείων ενεργητικού.

Στον κατάλογο ευπαθειών πρέπει να καταγράφονται κατ΄ ελάχιστο ο πόρος ενεργητικού, η ευπάθεια, η απειλή (ή απειλές) που μπορεί να εκμεταλλευτούν την συγκεκριμένη ευπάθεια, ο κίνδυνος που θα δημιουργηθεί, η δυνατότητα εκμετάλλευσης, καθώς και το μέγεθος της ευπάθειας.

# Αποκατάσταση ευπαθειών και ενημερώσεις ασφάλειας

Ο [Όνομα Οργανισμού] έχει θεσπίσει διαδικασία αποκατάστασης των ευπαθειών, η οποία ακολουθεί την διαδικασία διαχείρισης αλλαγών. Η διαδικασία αποκατάστασης ευπαθειών και η εφαρμογή ενημερώσεων ασφάλειας είναι ουσιαστικά συνδεδεμένες με την διοικητική λήψη αποφάσεων του [Όνομα Οργανισμού], και οι οποίες λαμβάνονται με βάση την καταγραφή ευπαθειών και την κρισιμότητα τους ανά κατηγορία στοιχείων ενεργητικού και την υποβολή σχετικών εκθέσεων.

Αυτή η προσέγγιση εξασφαλίζει ότι οι διαδικασίες αυτές ανταποκρίνονται στις στρατηγικές και τις προτεραιότητες του [Όνομα Οργανισμού].

Ο τρόπος αποκατάστασης πρέπει να διαχωρίζεται σε ενέργειες που γίνονται αυτόματα, χωρίς προηγούμενη δοκιμή, και σε ενέργειες που απαιτούν δοκιμή πριν την εφαρμογή τους, λαμβάνοντας υπόψη την κρισιμότητα των ευπαθειών ανά κατηγορία στοιχείων ενεργητικού

Μετά την εφαρμογή των μέτρων για την αντιμετώπιση μιας ευπάθειας, πρέπει να ελέγχεται η αποτελεσματικότητα τους. Σε περίπτωση που τα αποτελέσματα της αξιολόγησης της αποτελεσματικότητας είναι αρνητικά, πρέπει να λαμβάνονται κατάλληλες διορθωτικές ενέργειες(π.χ εκτέλεση ενεργειών rollback).

Συγκεκριμένα ακολουθείτε η πιο κάτω διαδικασία:

1. Η διαδικασία ξεκινά με την καταγραφή ευπαθειών σε σχετικές εκθέσεις που προκύπτουν μετά από αξιολογήσεις και ελέγχους.
2. Τα αποτελέσματα των εκθέσεων 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 ολοκληρωμένο και καταρτισμό σχεδίου δράσης. Η υλοποίηση περιλαμβάνει τόσο αυτόματες ενημερώσεις όσο και δράσεις που απαιτούν την επέμβαση εξειδικευμένου προσωπικού του [Όνομα Οργανισμού] ή/και συνεργατών του.

Σημείωση: το μέρος πιο κάτω αφορά τη Διαδικασία Διαχείρισης Ευπαθειών και Τρωτότητας που σκοπό έχει την υποστήριξη της Πολιτικής που καταγράφεται στις πιο πάνω παραγράφους. Η διαδικασία δύναται να είναι σε ξεχωριστό έγγραφο από τη Πολιτική.

# Διαδικασία Διαχείρισης Ευπαθειών και Τρωτότητας

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί διαδικασίες για την αξιολόγηση και 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.

# 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
* Συστήνεται όπως 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.

# Πολιτικές αποκατάστασης ευπαθειών

Ο [Όνομα Οργανισμού] θα πρέπει να έχει ενεργοποιήσει ή εφαρμόζει διάφορες πολιτικές 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 είναι υπεύθυνο για τον έλεγχο των ενημερώσεων πριν από την εγκατάσταση 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].

# Εφαρμογή ενεργειών

Κατά την εφαρμογή της αποκατάστασης των ευπαθειών διασφαλίζεται ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια μέσω της Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών.

# Δοκιμές Διείσδυσης (Penetration Testing)

Δοκιμή διείσδυσης είναι μια μέθοδος αξιολόγησης της ασφάλειας σε πληροφοριακά συστήματα με προσομοίωση μιας επίθεσης από εισβολέα και θα πρέπει να εκτελείτε σε όλα τα κρίσιμα συστήματα του [Όνομα Οργανισμού]. 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].Πιθανές προσεγγίσεις που δύναται να ακολουθούνται στις δοκιμές αυτές είναι: 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.
  + Έλεγχος Διαδικασιών
* Τα αποτελέσματα των δοκιμών διείσδυσης πρέπει να παραδίδονται σε μορφή έκθεσης προς την Ανώτατη Διοίκησης του [Όνομα Οργανισμού]. 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.

# Μηχανισμοί ευαισθητοποίησης και κανάλια επικοινωνίας

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, την ευαισθητοποίηση και την αντιμετώπιση ευπαθειών. Οι παρακάτω μηχανισμοί ενισχύουν την ανταλλαγή πληροφοριών και τη συνεργασία ενός 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.
7. Κανάλι επικοινωνίας με το Εθνικό CSIRT-CY για ανταλλαγή πληροφοριών και ανατροφοδότηση εξειδικευμένων πληροφοριών για απειλές (threat intelligence)

# Αναθεώρηση

Τα έγγραφα σχετικά με την Πολιτική και τη Διαχείριση Ευπαθειών θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] (π.χ. τις επιχειρηματικές δραστηριότητες και τις τάσεις της αγοράς, κανονιστικές απαιτήσεις και τις απαιτήσεις συμμόρφωσης, την εφαρμογή νέων συστημάτων, τους νέους κινδύνους, τις αναδυόμενες απειλές κλπ.).

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διαχείριση Ευπαθειών Και Ενημερώσεων Ασφάλειας | VM1 | Ανίχνευση και εντοπισμός ευπαθειών | Να διασφαλιστεί ότι οι ευπάθειες συστημάτων είναι γνωστές στον οργανισμό, προκειμένου να τύχουν κατάλληλου χειρισμού. |
| Διαχείριση Ευπαθειών Και Ενημερώσεων Ασφάλειας | VM2 | Καταγραφή και αναφορά ευπαθειών | 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. |
| Διαχείριση Ευπαθειών Και Ενημερώσεων Ασφάλειας | VM3 | Αποκατάσταση ευπαθειών και ενημερώσεις ασφάλειας | Να εξασφαλιστεί η αποκατάσταση των ευπαθειών συστημάτων και η εφαρμογή ενημερώσεων ασφαλείας, κατόπιν απόφασης της διοίκησης |