DIT172 | Project 3.3 | itp22104 | 22/12/2023

1. **Πώς θα χειριζόσασταν τους επικαλυπτόμενους κανόνες ACL ή πολλαπλές καταχωρίσεις που έρχονται σε αντίθεση μεταξύ τους στο ίδιο ACL;**

> Για την αντιμετώπιση περιπτώσεων όπως οι παραπάνω, ορισμένες ενδεικτικές ενέργειες είναι οι ακόλουθες:

1. Rule Priority: Αναθέτουμε προτεραιότητες στους κανόνες σύμφωνα με τη σειρά εφαρμογής τους. Ο πρώτος κανόνας που ταιριάζει θα εφαρμοστεί, και οι υπόλοιποι θα αγνοηθούν.
2. Exception Rules: Καθορίζουμε εξαιρέσεις για συγκεκριμένους κανόνες που πρέπει να έχουν προτεραιότητα έναντι των υπολοίπων.
3. Specific Rules: Δίνουμε προτεραιότητα σε λεπτομερείς κανόνες που είναι πιο συγκεκριμένοι και ισχυροί από γενικούς.
4. Overlapping Approval: Αξιολογούμε την επικάλυψη ανάμεσα στους διαφορετικούς κανόνες και αποφασίζουμε ποιος θα έχει προτεραιότητα.
5. Review and Monitoring: Καθορίζουμε κανόνες για την αναθεώρηση και την παρακολούθηση των ACL, ώστε να διασφαλιστεί η συνέχεια και η αποτελεσματικότητά τους.

---

2. **Πώς αντιμετωπίζετε ζητήματα επεκτασιμότητας και απόδοσης κατά τη διαχείριση των ACL σε ένα μεγάλο περιβάλλον δικτύου με πολλές συσκευές και χρήστες;**

> Ζητήματα επεκτασιμότητας και απόδοσης σε τέτοιου τύπου περιβάλλοντα μπορούν να προσεγγιστούν με τις εξής ενδεικτικές μεθόδους:

1. Hierarchical Management: Οργανώνουμε τα ACL ιεραρχικά, καθορίζοντας κανόνες σε επίπεδα. Αυτό βοηθά στη διευκόλυνση της ενημέρωσης και της επισκόπησης κανόνων.
2. Automation: Χρησιμοποιούμε εργαλεία αυτοματοποίησης για τη διαχείριση ACL. Η αυτοματοποίηση μπορεί να μειώσει τον ανθρώπινο παράγοντα και να εξασφαλίσει συνέπεια.
3. Distributed Deployments: Διανέμουμε την εφαρμογή των ACL σε πολλαπλές συσκευές και διακριτικά σημεία παρακολούθησης για τη βελτίωση της απόδοσης.
4. Performance Assessment: Καθορίζουμε περιοδικά αξιολογήσεις απόδοσης για την αναγνώριση ενδεχόμενων προβληματικών σημείων και τη βελτιστοποίηση των ACL όταν απαιτείται.
5. Policy-based Management: Εφαρμόζουμε πολιτικές διαχείρισης που καθορίζουν τη συμπεριφορά των ACL ανάλογα με τις ανάγκες του περιβάλλοντος.

---

3. **Συγκρίνετε και αντιπαραβάλλετε standard και extended ACL, παρέχοντας πραγματικά παραδείγματα για το πότε θα χρησιμοποιούσατε κάθε τύπο**

- Συνοπτικά χαρακτηριστικά των *standard ACL*
    1. Βασίζονται κυρίως στη source IP address
    2. Εφαρμόζονται στο 3ο επίπεδο του μοντέλου OSI
    3. Προσφέρουν περιορισμένη δυνατότητα ορισμού κανόνων
- Χρήση των *standard ACL* (παράδειγμα)
  Μπορούν να χρησιμοποιηθούν για να επιτρέψουν ή να απαγορεύσουν την πρόσβαση από μια source IP address προς έναν υπολογιστή ή μια ομάδα υπολογιστών

```
access-list 1 permit 192.168.1.1
access-list 1 deny any
```

- Συνοπτικά χαρακτηριστικά των *extended ACL*
    1. Βασίζονται σε πολλά χαρακτηριστικά, όπως destination IP address, η source IP address, το port number, κ.ά.
    2. Εφαρμόζονται επίσης στο 3ο επίπεδο του μοντέλου OSI
    3. Προσφέρουν εκτεταμένες δυνατότητες καθορισμού κανόνων
- Χρήση των *extended ACL* (παράδειγμα)
  Μπορούν να χρησιμοποιηθούν για να επιτρέψουν ή να απαγορεύσουν την πρόσβαση από μια source IP address σε μια destination IP address σε συγκεκριμένο port

```
access-list 101 permit tcp host 192.168.2.2 host 10.0.0.5 eq 80
access-list 101 deny ip any any
```

---

4. **Πώς διαφέρουν τα ACL σε διάφορες συσκευές δικτύου, όπως δρομολογητές, μεταγωγείς και τείχη προστασίας, και πώς προσαρμόζετε τις στρατηγικές υλοποίησης για να ανταποκρίνονται σε αυτές τις διαφορές;**

> Ανάλογα με τις διάφορες συσκευές δικτύου, τα ACLs μπορεί να διαφέρουν ως εξής:

1. Σε δρομολογητές, οι ACLs χρησιμοποιούνται συνήθως για τον έλεγχο της κυκλοφορίας δεδομένων μεταξύ διαφορετικών δικτύων. Μπορεί να χρησιμοποιηθούν για να επιτραπεί ή να οριστεί απαγόρευση πρόσβασης σε συγκεκριμένες πηγές ή προορισμούς.
2. Σε μεταγωγείς, οι ACLs χρησιμοποιούνται γενικά στο 2ο επίπεδο του μοντέλου OSI για τον έλεγχο της κυκλοφορίας δεδομένων μεταξύ φυσικών θυρών. Μπορεί να χρησιμοποιηθούν για να επιτραπεί ή να οριστεί απαγόρευση της μετάδοσης δεδομένων με βάση τη διεύθυνση MAC.
3. Σε τείχη προστασίας, οι ACLs χρησιμοποιούνται για τον έλεγχο της κυκλοφορίας δεδομένων μεταξύ του εσωτερικού και του εξωτερικού δικτύου. Μπορεί να περιλαμβάνουν κανόνες που περιορίζουν την πρόσβαση από το Διαδίκτυο στο εσωτερικό δίκτυο.

> Ως προς την προσαρμογή των στρατηγικών υλοποίησης:

1. Στους δρομολογητές, πρέπει να λαμβάνεται υπόψη η λογική routing του δικτύου (τοπολογία δικτύου κλπ) και οι προορισμοί των δεδομένων
2. Στους μεταγωγείς, ο έλεγχος είναι συνήθως σε επίπεδο θύρας και MAC διευθύνσεων
3. Σε τείχη προστασίας, ο έλεγχος είναι πιο ποιοτικός, με κανόνες που προσδιορίζουν τις πηγές και τους προορισμούς που επιτρέπονται ή αποκλείονται.

---

5. **Ποιες είναι οι κυρώσεις για παραβιάσεις του GDPR;**

> Οι κύριες κατηγορίες κυρώσεων περιλαμβάνουν:

1. Υψηλά πρόστιμα. Το ποσό των προστίμων εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του βαθμού της παραβίασης και του είδους των προσωπικών δεδομένων που επηρεάζονται.
2. Επιτακτικά μέτρα στους υπεύθυνους επεξεργασίας, όπως απαγόρευση ή περιορισμός συγκεκριμένων επεξεργασιών δεδομένων
3. Δημοσίευση παραβίασης. Σε ορισμένες περιπτώσεις, εάν υπάρχει σοβαρός κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, οι υπεύθυνοι επεξεργασίας μπορεί να υποχρεωθούν να ενημερώσουν τους ενδιαφερόμενους για παραβιάσεις δεδομένων

---

6. **Τι είναι μια λειτουργία επεξεργασίας δεδομένων κατά GDPR;**

> Μια λειτουργία επεξεργασίας δεδομένων αναφέρεται σε οποιαδήποτε δραστηριότητα ή σειρά δραστηριοτήτων πραγματοποιούνται σε προσωπικά δεδομένα, είτε αυτές πραγματοποιούνται αυτοματοποιημένα είτε όχι.
> Παραδείγματα μπορεί να περιλαμβάνουν τη συλλογή, αποθήκευση και αντιγραφή, επεξεργασία και ανάλυση, μεταφορά ή και διαγραφή δεδομένων.

---

7. **Διαφέρει η συμμόρφωση με τον GDPR με βάση τον αριθμό των εργαζομένων που έχει μια εταιρεία; Είναι υποχρεωτικός ο διορισμός DPO;**

> Η συμμόρφωση με το GDPR δεν εξαρτάται από τον αριθμό των εργαζομένων μιας εταιρείας. Οι υποχρεώσεις σύμφωνα με το GDPR εφαρμόζονται σε όλους τους φορείς επεξεργασίας προσωπικών δεδομένων, ανεξάρτητα από το μέγεθός τους.
> Όσον αφορά τον διορισμό DPO, αυτός είναι υποχρεωτικός σε συγκεκριμένες περιπτώσεις, όπως:

1. Όταν η επεξεργασία δεδομένων πραγματοποιείται από δημόσιες αρχές ή φορείς
2. Εάν η κύρια δραστηριότητα μιας εταιρείας είναι το συστηματικό και εκτενές data monitoring
3. Όταν η επεξεργασία προσωπικών δεδομένων αφορά μεγάλη κλίμακα και συμπεριλαμβάνει ευαίσθητες κατηγορίες δεδομένων

---

8. **Τι είναι οι CSIRT και το EU-CyCLONe κατά την Οδηγία NIS2;**

> Το CSIRT (Computer Security Incident Response Teams) αντιπροσωπεύει τα "Κέντρα Αντιμετώπισης Συμβάντων της Ασφάλειας Υπολογιστών".
> Είναι οργανισμοί που αναλαμβάνουν τον συντονισμό και την αντιμετώπιση περιστατικών ασφαλείας στον τομέα της πληροφορικής προς οποιονδήποτε χρήστη, εταιρεία, κυβερνητικό φορέα ή οργανισμό. Το CSIRT αποτελεί ένα αξιόπιστο σημείο επικοινωνίας για την καταγγελία περιστατικών ασφαλείας των υπολογιστών παγκοσμίως. Παρέχει τα μέσα για την καταγραφή περιστατικών και για τη διάδοση σημαντικών πληροφοριών που σχετίζονται με αυτά.
> Το EU-CyCLONe (European cyber crisis liaison organisation network) είναι ένα δίκτυο συνεργασίας για τις εθνικές αρχές των κρατών μελών που είναι υπεύθυνες για τη διαχείριση κυβερνοκρίσεων.

---

9. **Η οδηγία NIS2 καλύπτει ποιους τομείς καλύπτει;**

> Η Οδηγία NIS2 καλύπτει τους εξής τομείς:

1. Παροχή Σημαντικών Υπηρεσιών: Οι παρόχοι σημαντικών υπηρεσιών πρέπει να λαμβάνουν μέτρα για την προστασία των δικτύων και των πληροφοριακών συστημάτων τους.
2. Παρόχοι Ψηφιακών Υπηρεσιών: Ορισμένοι παρόχοι ψηφιακών υπηρεσιών, όπως αγορές, κοινωνικά δίκτυα, και πλατφόρμες ανταλλαγής αρχείων, υπόκεινται επίσης στις απαιτήσεις της οδηγίας.
3. Διαχειριστές Ουσιαστικών Υποδομών: Οι διαχειριστές ουσιαστικών υποδομών, όπως ενέργεια, μεταφορές, τράπεζες και υγεία, υπόκεινται σε ειδικές διατάξεις για την προστασία των κρίσιμων υποδομών.
4. Δημόσιος Τομέας: Τα κράτη μέλη πρέπει να λαμβάνουν μέτρα για την προστασία των πληροφοριακών τους συστημάτων και να αναφέρουν σημαντικά περιστατικά ασφαλείας.

---

10. **Συμφωνα με την NIS2 τι αποφασίστηκε για EU vulnerability database;**

> Σύμφωνα με την Οδηγία NIS2, προβλέπεται η δημιουργία μιας κοινής ευρωπαϊκής βάσης δεδομένων ευπαθειών (EU vulnerability database) η οποία αποσκοπεί στη συγκέντρωση και ανταλλαγή πληροφοριών σχετικά με ευπάθειες (vulnerabilities) και περιστατικά ασφάλειας μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης.

> Συγκεκριμένα, η EU vulnerability database θα παρέχει ενημερωμένες πληροφορίες σχετικά με ευπάθειες λογισμικού, υλικού ή/και δικτύων που μπορεί να επηρεάσουν την κυβερνοασφάλεια. Η ίδρυση αυτής της βάσης συνεισφέρει στην αντιμετώπιση προβλημάτων κυβερνοασφάλειας, προωθώντας την κοινή κατανόηση και τη συνεργασία μεταξύ των κρατών μελών.