ΕΠΛ362: Τεχνολογία Λογισμικού ΙΙ

(μετάφραση στα ελληνικά των διαφανειών του βιβλίου Software Engineering, 9/E, Ian Sommerville, 2011)

Ενότητα 2 (κεφάλαιο 14) – Τεχνολογία Προστασίας από Εξωτερικούς Κινδύνους

Οι διαφάνειες αυτές έχουν συμπληρωματικό και επεξηγηματικό χαρακτήρα και σε καμία περίπτωση δεν υποκαθιστούν το βιβλίο

Γιώργος Α. Παπαδόπουλος
Τμήμα Πληροφορικής
Πανεπιστήμιο Κύπρου

Περιεχόμενα

- Τεχνολογία προστασίας και διαχείριση κινδύνων.
  - Η τεχνολογία προστασίας ασχολείται με εφαρμογές ενώ η διαχείριση κινδύνων ασχολείται με την υποδομή.
- Εκτίμηση των κινδύνων σε σχέση με την προστασία.
  - Ο σχεδιασμός ενός συστήματος με βάση την εκτίμηση των κινδύνων σε σχέση με την προστασία του συστήματος.
- Σχεδιασμός με στόχο την προστασία από εξωτερικούς κινδύνους.
  - Πως πρέπει να σχεδιασθούν οι αρχιτεκτονικές ενός συστήματος για να υπάρχει ασφάλεια.
- Οδηγίες σχεδιασμού για ασφάλεια.
  - Οδηγίες που βοηθούν στο σχεδιασμό ενός ασφαλούς συστήματος.
- Σχεδιασμός για διανομή.
  - Ο σχεδιασμός πρέπει να ελαχιστοποιεί τα προβλήματα ύπαρξης αδύνατων σημείων ασφάλειας σε ένα σύστημα κατά τη διανομή του.
- Επιβιωσιμότητα του συστήματος.
  - Επιτρέπει στο σύστημα να παρέχει απαραίτητες υπηρεσίες όταν γίνεται επίθεση σε αυτό.

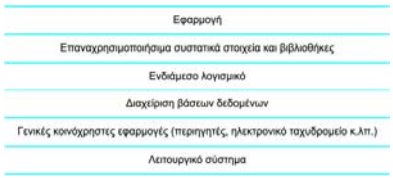
Τεχνολογία προστασίας από εξωτερικούς κινδύνους

- Εργαλεία, τεχνικές και μέθοδοι υποστήριξης της ανάπτυξης και συντήρησης συστημάτων τα οποία μπορούν να αντισταθούν σε κακόβουλες επιθέσεις που έχουν στόχο να προκαλέσουν ζημιές σε αυτά ή στα δεδομένα τους.
- Αποτελεί μέρος του γενικότερου τομέα της προστασίας υπολογιστών από εξωτερικούς κινδύνους.

Προστασία εφαρμογών και προστασία υποδομών

- Η προστασία εφαρμογών αποτελεί πρόβλημα της τεχνολογίας λογισμικού, δηλαδή το σύστημα πρέπει να είναι σχεδιασμένο ώστε να ανθίσταται σε επιθέσεις.
- Η προστασία υποδομών συνιστά πρόβλημα διαχείρισης συστημάτων, δηλαδή η υποδομή ενός συστήματος πρέπει να έχει διευθετηθεί έτσι ώστε να ανθίσταται σε επιθέσεις.
- Το επίκεντρο του κεφαλαίου αυτού είναι η προστασία εφαρμογών.

Επίπεδα του συστήματος όπου μπορεί να υπονομευθεί η ασφάλεια



Έννοιες προστασίας από εξωτερικούς κινδύνους

Όρος	Περιγραφή
Πόρος.	Πόρος συστήματος που έχει κάποια αξία και πρέπει να προστατευτεί.
Έκθεση.	Η πιθανή απώλεια ή βλάβη που θα μπορούσε να προκύψει από μία επιτυχημένη επίθεση. Μπορεί να είναι απώλεια ή ζημιά στα δεδομένα, ή απώλεια χρόνου και προσπάθειας αν είναι αναγκαία η ανάκαμψη μετά από κάποια παραβίαση των μέτρων προστασίας.
Ευπάθεια.	Μία αδυναμία σε ένα σύστημα που βασίζεται σε υπολογιστές, η εκμετάλλευση της οποίας μπορεί να προκαλέσει απώλειες ή βλάβη.
Επίθεση.	Η εκμετάλλευση μίας ευπάθειας του συστήματος. Γενικά, προέρχεται έξω από το σύστημα και αποτελεί σκόπιμη προσπάθεια να προκληθεί κάποια ζημιά.
Απειλές.	Περιστάσεις που ενδεχομένως προκαλούν απώλειες ή βλάβες. Μπορείτε να τις θεωρήσετε ως ευπάθειες του συστήματος οι οποίες μπορεί να δεχτούν επιθέσεις.
Μέτρο.	Προστατευτικό μέτρο που μειώνει την ευπάθεια ενός συστήματος. Ένα παράδειγμα μέτρου για τη μείωση της ευπάθειας ενός συστήματος χαλαρής πρόσβασης θα μπορούσε να είναι η κρυπτογράφηση.

Παραδείγματα εννοιών προστασίας από εξωτερικούς κινδύνους

Όρος	Περιγραφή
Πόρος.	Τα αρχεία κάθε ασθενούς που υποβάλλεται ή έχει υποβληθεί σε θεραπεία.
Έκθεση.	Ενδεχόμενα διαφυγόντα κέρδη από μελλοντικούς ασθενείς οι οποίοι αποφεύγουν τη νοσηλεία διότι δεν εμπιστεύονται την κλινική στην προστασία των δεδομένων τους. Οικονομικές απώλειες από πιθανή αγωγή εκ μέρους του αθλητικού αστέρα. Απώλεια υπόληψης.
Ευπάθεια.	Ένα χαλαρό σύστημα κωδικών πρόσβασης που διευκολύνει τους χρήστες να ορίζουν κωδικούς πρόσβασης οι οποίοι μπορούν να προβλεφθούν εύκολα. Αναγνωριστικά χρηστών που είναι ίδια με τα ονόματά τους.
Επίθεση.	Πλαστοπροσωπία σε βάρος ενός εξουσιοδοτημένου χρήστη.
Απειλές.	Ένας μη εξουσιοδοτημένος χρήστης θα αποκτήσει πρόσβαση στο σύστημα μαντεύοντας τα διαπιστευτήρια ενός εξουσιοδοτημένου χρήστη (όνομα σύνδεσης και κωδικό πρόσβασης).
Μέτρο.	Ένα σύστημα ελέγχου κωδικών πρόσβασης το οποίο δεν θα επιτρέπει στους χρήστες να ορίζουν κωδικούς πρόσβασης που είναι ονόματα ή λέξεις οι οποίες περιλαμβάνονται σε κάποιο λεξικό.

Απειλές κατά της προστασίας από εξωτερικούς κινδύνους

- Απειλές για την εμπιστευτικότητα του συστήματος και των δεδομένων του.
- Απειλές για την ακεραιότητα του συστήματος και των δεδομένων του.
- Απειλές για τη διαθεσιμότητα του συστήματος και των δεδομένων του.

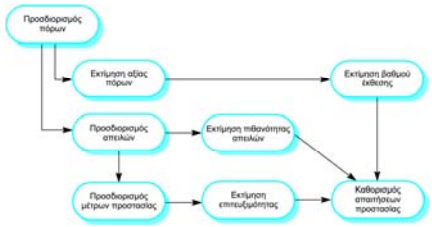
Μέτρα προστασίας από εξωτερικούς κινδύνους

- Μέτρα που έχουν σκοπό να διασφαλίσουν ότι οι επιθέσεις δεν θα επιτύχουν. Είναι παρεμφερή με τις μεθόδους αποφυγής σφαλμάτων.
- Μέτρα που στοχεύουν στην ανίχνευση και απώθηση επιθέσεων. Είναι παρεμφερή με τις μεθόδους ανίχνευσης και ανοχής σε σφάλματα.
- Μέτρα που υποστηρίζουν την ανάκαμψη από προβλήματα. Είναι παρεμφερή με τις μεθόδους ανάκαμψης από σφάλματα.

Διαχείριση κινδύνων σχετικών με την προστασία

- Η διαχείριση κινδύνων σχετικών με την προστασία αφορά την εκτίμηση των πιθανών απωλειών που μπορεί να προκύψουν από επιθέσεις στο σύστημα, καθώς και την επίτευξη μίας ισορροπίας μεταξύ αυτών των απωλειών και του κόστους των διαδικασιών προστασίας οι οποίες είναι σε θέση να τις περιορίσουν.
- Η διαχείριση κινδύνων σχετικών με την προστασία πρέπει να καθοδηγείται από μία γενική εταιρική πολιτική.
- Η διαχείριση κινδύνων σε σχέση με την προστασία περιλαμβάνει:
  - Προκαταρκτική αξιολόγηση κινδύνων.
  - Αξιολόγηση κινδύνων κύκλου ζωής.
  - Αξιολόγηση κινδύνων λειτουργίας.

Προκαταρκτική αξιολόγηση κινδύνων



Περιπτώσεις κακής χρήσης

- Οι περιπτώσεις κακής χρήσης είναι ένα είδος απειλών προς το σύστημα.
- Απειλές αναχαίτισης.
  - Ο επιτιθέμενος αποκτά πρόσβαση σε πόρους του συστήματος.
- Απειλές διακοπής.
  - Ο επιτιθέμενος καθιστά μέρος του συστήματος μη διαθέσιμο.
- Απειλές τροποποίησης.
  - Ο επιτιθέμενος αλλοιώνει πόρους του συστήματος.
- Απειλές πλαστογράφησης.
  - Ο επιτιθέμενος προσθέτει ψευδείς πληροφορίες στο σύστημα.

Ανάλυση πόρων (σε ένα πληροφοριακό σύστημα νοσοκομείου)

Πόρος	Αξία	Βαθμός έκθεσης
Το πληροφοριακό σύστημα.	Υψηλή. Είναι απαραίτητο για την υποστήριξη όλων των κλινικών διαγνώσεων. Ενδεχομένως κρίσιμο από άποψη ασφάλειας.	Υψηλός. Οικονομικές απώλειες, καθώς μπορεί να απαιτηθεί η διακοπή της λειτουργίας κάποιων κλινικών. Κόστος για την αποκατάσταση του συστήματος. Πιθανή βλάβη για τους ασθενείς, αν κάποια θεραπεία δεν μπορεί να συνταγογραφηθεί.
Η βάση δεδομένων των ασθενών.	Υψηλή. Είναι απαραίτητη για την υποστήριξη όλων των κλινικών διαγνώσεων. Ενδεχομένως κρίσιμη από άποψη ασφάλειας.	Υψηλός. Οικονομικές απώλειες, καθώς μπορεί να απαιτηθεί η διακοπή της λειτουργίας κάποιων κλινικών. Κόστος για την αποκατάσταση του συστήματος. Πιθανή βλάβη για τους ασθενείς, αν κάποια θεραπεία δεν μπορεί να συνταγογραφηθεί.
Τα ατομικά ιστορικά των ασθενών.	Συνήθως χαμηλή, αν και μπορεί να είναι υψηλή για συγκεκριμένους ασθενείς υψηλού προφίλ.	Μικρές άμεσες απώλειες, αλλά πιθανή απώλεια υπόληψης.

Ανάλυση απειλών και μέτρων προστασίας

Απειλή	Πιθανότητα	Μέτρο προστασίας	Επιτευξιμότητα
Μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση ως διαχειριστής συστήματος και καθιστά το σύστημα μη διαθέσιμο.	Χαμηλή.	Η χρήση του συστήματος με διαχειριστικά προνόμια να επιτρέπεται μόνο από συγκεκριμένους χώρους οι οποίοι διαθέτουν φυσική προστασία.	Χαμηλό κόστος υλοποίησης, αλλά πρέπει να ληφθεί μέριμνα σχετικά με τη διανομή των κλειδιών και να διασφαλιστεί ότι τα κλειδιά θα είναι διαθέσιμα σε περίπτωση επείγουσας ανάγκης.
Μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση ως χρήστης συστήματος και προσπελάζει εμπιστευτικές πληροφορίες.	Υψηλή.	Πιστοποίηση ταυτότητας όλων των χρηστών με τη χρήση βιομετρικών μηχανισμών. Καταγραφή κάθε αλλαγής που πραγματοποιείται σε πληροφορίες ασθενούς, για την παρακολούθηση της χρήσης του συστήματος.	Λύση τεχνικά εφικτή αλλά με υψηλό κόστος. Πιθανή αντίδραση των χρηστών. Απλή και διαφανής στην υλοποίηση, και υποστηρίζει επίσης τη δυνατότητα ανάκτησης.

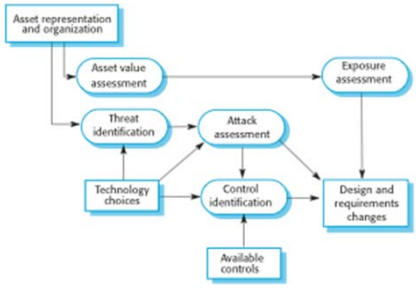
Απαιτήσεις προστασίας από εξωτερικούς κινδύνους

- Κατά το ξεκίνημα μίας περιόδου εργασίας από κάποια κλινική, οι πληροφορίες των ασθενών πρέπει να λαμβάνονται από τη βάση δεδομένων και να τοποθετούνται σε μία προστατευμένη περιοχή της εφαρμογής-πελάτη που χρησιμοποιείται από το προσωπικό της κλινικής.
- Οι πληροφορίες των ασθενών δεν πρέπει να διατηρούνται στις εφαρμογές-πελάτες του συστήματος μετά το πέρας κάποιας περιόδου εργασίας μίας κλινικής.
- Κάθε μεταβολή που πραγματοποιείται στη βάση δεδομένων πρέπει να διατηρείται σε ένα ημερολόγιο το οποίο θα είναι αποθηκευμένο σε υπολογιστή διαφορετικό από το διακομιστή της βάσης δεδομένων.

Αξιολόγηση κινδύνων κύκλου ζωής

- Αξιολόγηση κατά την ανάπτυξη του συστήματος και αφού τεθεί σε λειτουργία.
- Υπάρχουν περισσότερες διαθέσιμες πληροφορίες – η πλατφόρμα, το ενδιάμεσο λογισμικό, και η αρχιτεκτονική και οργάνωση των δεδομένων του συστήματος.
- Επομένως μπορούν να προσδιοριστούν ευπάθειες που ανακύπτουν από σχεδιαστικές επιλογές.

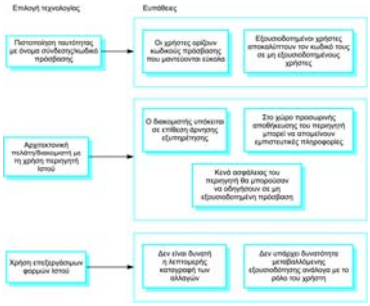
Ανάλυση κινδύνων κύκλου ζωής



Παραδείγματα σχεδιαστικών αποφάσεων

- Πιστοποίηση της ταυτότητας των χρηστών του συστήματος με χρήση συνδυασμού ονόματος σύνδεσης/κωδικού πρόσβασης.
- Η αρχιτεκτονική του συστήματος είναι τύπου πελάτη-διακομιστή και οι πελάτες προσπελάζουν το σύστημα μέσω ενός συνηθισμένου προγράμματος περιήγησης του ιστού.
- Οι πληροφορίες παρουσιάζονται στους χρήστες ως επεξεργάσιμη φόρμα ιστού.

Ευπάθειες που σχετίζονται με τεχνολογικές επιλογές



Απαιτήσεις ασφάλειας

- ✧ Ένα πρόγραμμα ελέγχου κωδικών πρόσβασης θα πρέπει να είναι διαθέσιμο και να εκτελείται καθημερινά. Αν διαπιστώσει ότι κάποιος κωδικός είναι επισφαλής (π.χ. κοινά ονόματα, ακολουθία συνεχόμενων χαρακτήρων, κλπ.) το αναφέρει στο διαχειριστή του συστήματος.
- ✧ Πρόσβαση στο κεντρικό σύστημα επιτρέπεται μόνο από πελάτες-υπολογιστές που έχουν εγκριθεί.
- ✧ Όλοι οι πελάτες-υπολογιστές θα πρέπει να έχουν εγκατεστημένο ένα μόνο περιηγητή ιστού ο οποίος και θα είναι εγκεκριμένος από τους διαχειριστές.

Αξιολόγηση κινδύνων λειτουργίας

- ✧ Συνέχεια της αξιολόγησης κινδύνων κύκλου ζωής αλλά με επιπρόσθετες πληροφορίες αναφορικά με το περιβάλλον στο οποίο το σύστημα χρησιμοποιείται.
- ✧ Τα χαρακτηριστικά του περιβάλλοντος μπορεί να οδηγήσουν σε καινούργια είδη κινδύνων για το σύστημα.
  - Π.χ. σε ένα περιβάλλον όπου οι χρήστες διακόπτονται συνεχώς, υπάρχει πιθανότητα ένας χρήστης να αφήνει τον υπολογιστή του ανεπιτήρητο με αποτέλεσμα κάποιος να καταφέρει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.

Σχεδιασμός με στόχο την προστασία από εξωτερικούς κινδύνους

- Αρχιτεκτονικός σχεδιασμός.
  - Πώς επηρεάζουν το βαθμό προστασίας ενός συστήματος οι αποφάσεις αρχιτεκτονικού σχεδιασμού;
- Καλές πρακτικές.
  - Ποιες είναι οι αποδεκτές καλές πρακτικές κατά το σχεδιασμό προστατευμένων συστημάτων;
- Σχεδιασμός με στόχο τη διανομή.
  - Τι είδους υποστήριξη πρέπει να ενσωματώνεται κατά το στάδιο του σχεδιασμού στα συστήματα ώστε να αποφεύγεται η εισαγωγή ευπαθειών όταν το σύστημα διανέμεται προς χρήση;

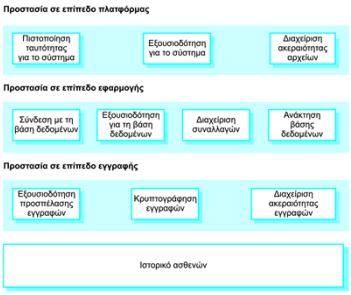
Αρχιτεκτονικός σχεδιασμός

- Κατά το σχεδιασμό μίας αρχιτεκτονικής συστήματος η οποία διατηρεί τον απαραίτητο βαθμό προστασίας, πρέπει να εξετάζονται δύο θεμελιώδη ζητήματα:
  - Προστασία.
    - Πώς πρέπει να οργανωθεί το σύστημα έτσι ώστε οι κρίσιμοι πόροι να είναι προστατευμένοι από εξωτερικές επιθέσεις;
  - Κατανομή.
    - Πώς πρέπει να κατανεμηθούν οι πόροι ενός συστήματος έτσι ώστε να ελαχιστοποιηθούν οι επιπτώσεις μίας επιτυχημένης επίθεσης;
- Υπάρχει το ενδεχόμενο διένεξης.
  - Αν οι πόροι είναι κατανεμημένοι, το κόστος για την προστασία τους θα είναι μεγαλύτερο, αλλά σε περίπτωση παραβίασης δεν θα υπάρχει ολοκληρωτική απώλεια.
  - Αν όλοι οι πόροι είναι σε μία θέση, τότε είναι πιο εύκολο να προστατευθούν αλλά τυχόν παραβίαση θα θέσει σε κίνδυνο όλους τους πόρους.

Προστασία

- Σε επίπεδο πλατφόρμας.
  - Το ανώτερο επίπεδο ελέγχει την πρόσβαση στην πλατφόρμα όπου εκτελείται ένα σύστημα. Συνήθως περιλαμβάνει τη σύνδεση του χρήστη (login) σε ένα συγκεκριμένο υπολογιστή. Επίσης, η πλατφόρμα συνήθως διαθέτει υποστήριξη για τη διατήρηση της ακεραιότητας των αρχείων στο σύστημα.
- Σε επίπεδο εφαρμογής.
  - Περιλαμβάνει την προσπέλαση της εφαρμογής από κάποιο χρήστη, ο οποίος πιστοποιείται και εξουσιοδοτείται να προβεί σε ενέργειες. Πιθανόν να υπάρχουν και επιπλέον μηχανισμοί ελέγχου ακεραιότητας.
- Σε επίπεδο εγγραφών.
  - Ενεργοποιείται όταν απαιτείται προσπέλαση σε συγκεκριμένες εγγραφές, και αφορά τον έλεγχο ότι ο χρήστης είναι εξουσιοδοτημένος να εκτελέσει τις λειτουργίες που ζητήθηκαν στη συγκεκριμένη εγγραφή.
- Τα ανωτέρω επίπεδα οδηγούν σε μία πολυεπίπεδη αρχιτεκτονική προστασίας.

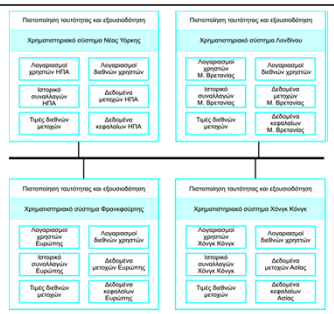
Μία πολυεπίπεδη αρχιτεκτονική προστασίας



Κατανομή πόρων

- Με την κατανομή των πόρων σε διαφορετικά μέρη, αν γίνει επίθεση σε ένα μέρος του συστήματος αυτό δεν θα οδηγήσει σε πλήρη απώλεια των υπηρεσιών του συστήματος.
- Κάθε πλατφόρμα έχει διαφορετικό μηχανισμό προστασίας, έτσι ώστε να μην έχουν κοινές αδυναμίες.
- Η κατανομή πόρων είναι ιδιαίτερα σημαντική αν το ρίσκο επιθέσεων άρνησης εξυπηρέτησης είναι υψηλό.

Κατανεμημένα περιουσιακά στοιχεία σε ένα σύστημα χρηματαγορών



Κατευθύνσεις σχεδιασμού για τεχνολογία προστασίας από εξωτερικούς κινδύνους

- Οι οδηγίες σχεδιασμού εμπεριέχουν τις καλές πρακτικές σχεδιασμού προστατευμένων συστημάτων.
- Οι οδηγίες σχεδιασμού εξυπηρετούν δύο σκοπούς:
  - Αποτελούν μέσο εγρήγορσης για τα μέλη μίας ομάδας τεχνολογίας λογισμικού πάνω σε θέματα προστασίας. Τα θέματα της ασφάλειας εξετάζονται στη φάση σχεδιασμού του συστήματος.
  - Συνιστούν τη βάση για μία λίστα ελέγχου επισκόπησης η οποία θα μπορούσε να χρησιμοποιηθεί κατά τη διαδικασία επικύρωσης του συστήματος.
- Οι οδηγίες σχεδιασμού είναι εφαρμόσιμες κατά τις διαδικασίες εξαγωγής προδιαγραφών και σχεδιασμού του λογισμικού.

Σχεδιαστικές οδηγίες για την τεχνολογία προστατευμένων συστημάτων

Σχεδιαστικές οδηγίες
Λήψη αποφάσεων για την προστασία βάσει ρητής πολιτικής
Αποφυγή μοναδικών σημείων αστοχίας
Αστοχία με διατήρηση του επιπέδου προστασίας
Εξισορρόπηση βαθμού προστασίας και χρηστικότητας
Εγρήγορση για την πιθανότητα κοινωνικής μηχανικής
Χρήση υπερεπάρκειας και ποικιλίας για τη μείωση των κινδύνων
Επικύρωση όλων των εισόδων
Διαμερισματοποίηση των πόρων
Σχεδιασμός με στόχο τη διανομή
Σχεδιασμός με στόχο τη δυνατότητα ανάκαμψης

Σχεδιαστικές οδηγίες (α)

- Λαμβάνουμε αποφάσεις που αφορούν την προστασία βάσει ρητής πολιτικής.
  - Ορίζουμε για τον οργανισμό μία πολιτική που καθορίζει τις θεμελιώδεις προδιαγραφές ασφάλειας που πρέπει να ισχύουν για όλα τα συστήματα του οργανισμού.
- Αποφεύγουμε μοναδικά σημεία αστοχίας.
  - Δεν πρέπει να βασιζόμαστε σε ένα μόνο μηχανισμό διασφάλισης της ασφάλειας (π.χ. να υπάρχει και κωδικός πρόσβασης και μηχανισμός «ερώτηση/απάντηση»).
- Φροντίζουμε για τη διατήρηση του επιπέδου προστασίας κατά την αστοχία.
  - Για οποιονδήποτε λόγο και να έχει δημιουργηθεί αστοχία, οι ευαίσθητες πληροφορίες πρέπει να παραμένουν προστατευμένες από μη εξουσιοδοτημένη πρόσβαση.

Σχεδιαστικές οδηγίες (β)

- Βρίσκουμε την ισορροπία μεταξύ βαθμού προστασίας και χρηστικότητας.
  - Πρέπει να αποφεύγουμε την επιβολή απαιτήσεων ασφάλειας οι οποίες καθιστούν το σύστημα δύσκολο να χρησιμοποιηθεί. Μερικές φορές είναι καλύτερο να υιοθετούνται λιγότερο ισχυροί μηχανισμοί προστασίας για να είναι το σύστημα πιο εύχρηστο.
- Είμαστε ενήμεροι για την πιθανότητα επιθέσεων κοινωνικής μηχανικής.
  - Καταγραφή των ενεργειών των χρηστών ώστε να είναι δυνατή η κατοπινή ανάλυσή τους για να ανακαλυφθεί ποιος έκανε τι. Αν οι χρήστες γνωρίζουν για αυτή την καταγραφή, μειώνεται η πιθανότητα να συμπεριφερθούν με μη αξιόπιστο τρόπο.
- Μειώνουμε τους κινδύνους με τη βοήθεια της υπερεπάρκειας και της ποικιλίας.
  - Διατήρηση περισσότερων από μία εκδόσεων του λογισμικού ή των δεδομένων σε ένα σύστημα όπου διαφορετικές εκδόσεις βασίζονται σε διαφορετικές πλατφόρμες και τεχνολογίες. Έτσι, μία ευπάθεια στην πλατφόρμα ή την τεχνολογία δεν θα επηρεάσει όλες τις εκδόσεις οδηγώντας σε γενική αστοχία.

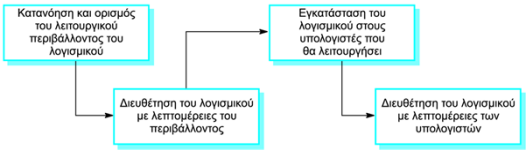
Σχεδιαστικές οδηγίες (γ)

- Επικυρώνουμε όλες τις εισόδους.
  - Ελέγχουμε ότι όλα τα δεδομένα εισόδου βρίσκονται μέσα στα επιτρεπτά όρια ώστε το σύστημα να μη τροφοδοτηθεί με μη αναμενόμενα δεδομένα.
- Διαμερισματοποιούμε τους πόρους.
  - Οι πληροφορίες σε ένα σύστημα πρέπει να οργανώνονται έτσι ώστε οι χρήστες να έχουν πρόσβαση μόνο σε αυτές που τους είναι απαραίτητες και όχι σε κάθε διαθέσιμη πληροφορία.
- Σχεδιάζουμε με στόχο τη διανομή.
  - Το σύστημα πρέπει να σχεδιάζεται με τρόπο που να περιλαμβάνει μέσα τα οποία να απλοποιούν τη διανομή του και να ελέγχουν για ενδεχόμενα λάθη διευθέτησης και παραλήψεις.
- Σχεδιάζουμε με στόχο τη δυνατότητα ανάκαμψης.
  - Να επινοηθούν τρόποι εύκολης ανάκαμψης και αποκατάστασης του συστήματος σε λειτουργική κατάσταση κάτω από τον επιθυμητό βαθμό προστασίας.

Σχεδιασμός με στόχο τη διανομή

- Στη διανομή περιλαμβάνεται η διευθέτηση του λογισμικού ώστε να λειτουργεί στο περιβάλλον εργασίας, η εγκατάστασή του και η ρύθμισή του για την εκάστοτε πλατφόρμα λειτουργίας.
- Σε αυτό το στάδιο συχνά παρεισφρέουν στο λογισμικό ευπάθειες λόγω λαθών διευθέτησης.
- Αν στο σχεδιασμό του συστήματος ενταχθεί υποστήριξη διανομής, η πιθανότητα ευπαθειών θα μειωθεί.

Διανομή λογισμικού



Ευπάθειες στη διευθέτηση του λογισμικού

- ✧ Ευπαθείς προεπιλεγόμενες ρυθμίσεις.
  - Αν κάποιες προεπιλεγόμενες ρυθμίσεις είναι αδύνατες (συχνά για να αυξηθεί η χρηστικότητα του συστήματος), τότε οι επιτιθέμενοι σε ένα σύστημα μπορούν να ανακαλύψουν τις τιμές τους και να το εκμεταλλευτούν αυτό αναλόγως.
- ✧ Ανάπτυξη παρά διευθέτηση.
  - Μερικές παράμετροι για διευθέτηση ενός συστήματος είναι σχεδιασμένες με τρόπο που να επιτρέπει ανάπτυξη και αποσφαλμάτωση του λογισμικού. Αν αυτές παραμείνουν ενεργές μετά τη διανομή του συστήματος θα μπορούσαν να αποτελέσουν σημεία ευπάθειας και να υποστούν εκμετάλλευση από επιτιθέμενους.

Υποστήριξη διανομής (α)

- ✧ Συμπερίληψη υποστήριξης για την προβολή και ανάλυση των παραμέτρων διευθέτησης.
  - Το σύστημα πρέπει να περιλαμβάνει μέσα τα οποία να επιτρέπουν στους διαχειριστές του να έχουν πλήρη εικόνα της διευθέτησης του συστήματος. Με αυτό τον τρόπο είναι πιο εύκολο να εντοπισθούν σφάλματα και παραλείψεις.
- ✧ Ελαχιστοποίηση των προεπιλεγμένων προνομίων και, επομένως, περιορισμός της ζημιάς που μπορεί να προκληθεί.
  - Η προεπιλεγμένη διευθέτηση ενός συστήματος πρέπει να παρέχει ελάχιστα βασικά προνόμια. Έτσι, η ζημιά που μπορούσε να προκαλέσει κάποιος επιτιθέμενος είναι περιορισμένη.

Υποστήριξη διανομής (β)

- Συγκεντρωτική διευθέτηση ρυθμίσεων.
  - Όλα τα στοιχεία μίας διευθέτησης που αφορούν το ίδιο τμήμα ενός συστήματος πρέπει να βρίσκονται στο ίδιο σημείο. Διαφορετικά ο χρήστης θα μπορούσε να παραλείψει τη ρύθμισή τους ή ακόμα και να μη γνωρίζει την ύπαρξη ορισμένων δυνατοτήτων προστασίας του συστήματος.
- Παροχή εύκολων τρόπων για τη διόρθωση ευπαθειών προστασίας.
  - Το σύστημα πρέπει να διαθέτει απλούς μηχανισμούς ενημέρωσής του με σκοπό τη διόρθωση ευπαθειών προστασίας που έχουν διαπιστωθεί, όπως ο αυτόματος έλεγχος για ενημερώσεις προστασίας και λήψη των ενημερώσεων αυτών μόλις είναι διαθέσιμες.

Επιβιωσιμότητα συστημάτων

- Η επιβιωσιμότητα είναι μία ανακύπτουσα ιδιότητα του συστήματος η οποία αντανακλά την ικανότητά του να συνεχίσει να παρέχει απαραίτητες υπηρεσίες ενώ δέχεται επίθεση ή μετά τη βλάβη κάποιου τμήματός του.
- Η ανάλυση επιβιωσιμότητας και ο αντίστοιχος σχεδιασμός πρέπει να εντάσσονται στα πλαίσια της τεχνολογία προστασίας από εξωτερικούς κινδύνους.

Σημασία της επιβιωσιμότητας

- Η οικονομική και κοινωνική ζωή μας εξαρτάται από πληροφοριακά συστήματα.
  - Κρίσιμες υποδομές – ηλεκτρισμός, φυσικό αέριο, τηλεπικοινωνίες.
  - Υγεία.
  - Κυβέρνηση.
- Απώλεια ενός πληροφοριακού συστήματος, έστω και για μικρό χρονικό διάστημα, μπορεί να έχει σοβαρές αρνητικές οικονομικές επιπτώσεις.
  - Συστήματα κρατήσεων αεροπορικών θέσεων.
  - Συστήματα ηλεκτρονικών επιχειρήσεων (e-business).
  - Συστήματα πληρωμών.

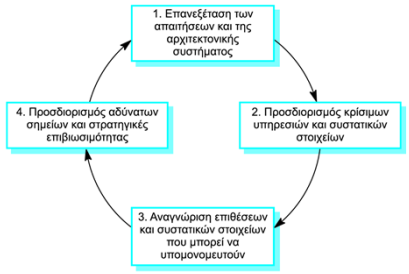
Διαθεσιμότητα υπηρεσιών

- Ποιες υπηρεσίες συστήματος είναι οι πλέον κρίσιμες για μία επιχείρηση;
- Πώς θα μπορούσαν να υπονομευτούν αυτές οι υπηρεσίες;
- Ποια είναι η ελάχιστη ποιότητα υπηρεσιών που πρέπει να διατηρηθεί;
- Πώς θα μπορούσαν να προστατευτούν οι υπηρεσίες αυτές;
- Πόσο γρήγορα μπορεί να γίνει ανάκαμψη σε περίπτωση μη διαθεσιμότητας μίας υπηρεσίας;

Στρατηγικές επιβιωσιμότητας

- Αντίσταση.
  - Αποφυγή προβλημάτων με την ενσωμάτωση στο σύστημα δυνατοτήτων για την απόκρουση επιθέσεων.
- Αναγνώριση.
  - Ανίχνευση προβλημάτων μέσω της ενσωμάτωσης στο σύστημα δυνατοτήτων ανίχνευσης επιθέσεων και αστοχιών, καθώς και δυνατοτήτων αξιολόγησης των βλαβών που προκύπτουν.
- Ανάκαμψη.
  - Ανοχή σε προβλήματα μέσω δυνατοτήτων οι οποίες επιτρέπουν στο σύστημα να παρέχει τις απαραίτητες υπηρεσίες ενώ δέχεται επίθεση.

Στάδια στην ανάλυση επιβιωσιμότητας



Κύριες δραστηριότητες

- ✧ Κατανόηση του συστήματος.
  - Ανασκόπηση των στόχων, των απαιτήσεων και της αρχιτεκτονικής του.
- ✧ Προσδιορισμός κρίσιμων υπηρεσιών.
  - Προσδιορισμός υπηρεσιών που πρέπει να διατηρηθούν.
- ✧ Προσομοίωση επιθέσεων.
  - Επινόηση σεναρίων επίθεσης και προσδιορισμός των συστατικών στοιχείων που επηρεάζονται.
- ✧ Ανάλυση επιβιωσιμότητας.
  - Προσδιορισμός στρατηγικών επιβιωσιμότητας που πρέπει να εφαρμοστούν.

Επιβιωσιμότητα συστήματος συναλλαγών

- ✧ Τηρούνται αντίγραφα των λογαριασμών χρηστών και των τιμών μετοχών, έτσι υπάρχει πρόβλεψη επιβιωσιμότητας σε κάποιο βαθμό.
- ✧ Η βασική δυνατότητα που πρέπει να διατηρείται είναι η δυνατότητα υποβολής ενταλμάτων αγοραπωλησίας μετοχών.
- ✧ Τα εντάλματα πρέπει να είναι ακριβή και να αντιπροσωπεύουν τις πραγματικές αγορές/πωλήσεις στις οποίες προχώρησε ο επενδυτής.

Διατήρηση της υπηρεσίας ενταλμάτων

- ✧ Η βασική υπηρεσία που πρέπει να διατηρηθεί είναι η δυνατότητα ενταλμάτων συναλλαγών από εξουσιοδοτημένους χρήστες.
- ✧ Αυτό προϋποθέτει ότι τρία συστατικά στοιχεία του συστήματος είναι διαθέσιμα και λειτουργούν αξιόπιστα:
  - Πιστοποίηση ταυτότητας χρήστη, που επιτρέπει τη σύνδεση εξουσιοδοτημένων χρηστών στο σύστημα.
  - Εμφάνιση τιμής μετοχής, για να είναι δυνατή η εξέταση της πιθανότητας αγοράς ή πώλησης της μετοχής.
  - Υποβολή εντάλματος αγοράς ή πώλησης μίας μετοχής.

Πιθανές επιθέσεις

- Ένας κακόβουλος χρήστης αποκτά πρόσβαση στο σύστημα χρησιμοποιώντας τα δικά του διαπιστευτήρια και υποβάλει ψεύτικα εντάλματα αγοράζοντας και πουλώντας μετοχές, έτσι ώστε να δημιουργήσει προβλήματα στον εξουσιοδοτημένο χρήστη.
- Ένας μη εξουσιοδοτημένος χρήστης αλλοιώνει τη βάση δεδομένων συναλλαγών, αποκτώντας άδεια να υποβάλει εντολές οι οποίες καθιστούν αδύνατη την εναρμόνιση των πωλήσεων με τις αγορές.

Ανάλυση επιβιωσιμότητας του συστήματος συναλλαγών

Επίθεση	Αντίσταση	Αναγνώριση	Ανάκαμψη
Μη εξουσιοδοτημένος χρήστης υποβάλει κακόβουλες εντολές.	Η υποβολή ενταλμάτων πρέπει να πραγματοποιείται με την παροχή ενός ειδικού κωδικού πρόσβασης, ο οποίος διαφέρει από τον κωδικό πρόσβασης για τη σύνδεση.	Αποστολή αντιγράφου του εντάλματος μέσω e-mail στον εξουσιοδοτημένο χρήστη, το οποίο θα περιέχει τηλέφωνο επαφής (έτσι ώστε να μπορούν να ανιχνευθούν κακόβουλες εντολές). Διατήρηση του ιστορικού εντολών του χρήστη και έλεγχος για ασυνήθιστα μοτίβα συναλλαγών.	Παροχή μηχανισμών για την αυτόματη «αναίρεση» συναλλαγών και την αποκατάσταση λογαριασμών χρηστών. Αποζημίωση χρηστών για απώλειες που οφείλονται σε κακόβουλες ενέργειες. Εξασφάλιση για επακόλουθες απώλειες.
Αλλοίωση της βάσης δεδομένων συναλλαγών.	Οι προνομιακοί χρήστες πρέπει να εξουσιοδοτούνται μέσω ενός ισχυρότερου μηχανισμού πιστοποίησης ταυτότητας, όπως τα ψηφιακά πιστοποιητικά.	Διατήρηση αντιγράφων «μόνο για ανάγνωση» των συναλλαγών ενός γραφείου σε διεθνή διακομιστή. Περιοδική σύγκριση των συναλλαγών για τον έλεγχο περιπτώσεων αλλοίωσης. Διατήρηση κρυπτογραφικών αθροισμάτων ελέγχου για όλα τα αρχεία συναλλαγών με σκοπό την ανίχνευση αλλοιώσεων.	Ανάκαμψη βάσης δεδομένων από εφεδρικά αντίγραφα. Παροχή μηχανισμού αναπαραγωγής των συναλλαγών από μία καθορισμένη ημερομηνία για την αναδημιουργία της βάσης δεδομένων.

Κύρια σημεία (α)

- Η τεχνολογία προστασίας από εξωτερικούς κινδύνους εστιάζεται στο πώς αναπτύσσονται και συντηρούνται συστήματα λογισμικού τα οποία είναι σε θέση να αντιστέκονται σε κακόβουλες επιθέσεις.
- Οι απειλές κατά της προστασίας μπορεί να είναι απειλές κατά της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας ενός συστήματος και των δεδομένων του.
- Η διαχείριση κινδύνων προστασίας περιλαμβάνει την εκτίμηση των πιθανών απωλειών από επιθέσεις, καθώς και την παραγωγή απαιτήσεων προστασίας με στόχο την ελαχιστοποίηση αυτών των απωλειών.
- Στο σχεδιασμό με στόχο την προστασία προβλέπονται τα στοιχεία της αρχιτεκτονικής του συστήματος, η τήρηση καλών πρακτικών σχεδιασμού και η ελαχιστοποίηση της πιθανότητας εισαγωγής ευπαθειών στο σύστημα.

Κύρια σημεία (β)

- Βασικά ζητήματα κατά το σχεδιασμό αρχιτεκτονικών με στόχο την προστασία είναι η οργάνωση της δομής του συστήματος για την προστασία των πόρων και η κατανομή αυτών των πόρων με στόχο την ελαχιστοποίηση των απωλειών.
- Οι γενικές κατευθυντήριες οδηγίες ευαισθητοποιούν τους σχεδιαστές συστημάτων στα θέματα που αφορούν την προστασία και αποτελούν βάση για τη δημιουργία λίστας ελέγχου σε επισκοπήσεις.
- Η οπτικοποίηση της διευθέτησης του συστήματος, η συγκεντρωτική διαρρύθμιση των ρυθμίσεων και η ελαχιστοποίηση των προκαθορισμένων προνομίων συμβάλλουν στη μείωση των σφαλμάτων διανομής.
- Η επιβιωσιμότητα ενός συστήματος αντικατοπτρίζει την ικανότητά του να συνεχίσει την παροχή απαραίτητων υπηρεσιών ενώ δέχεται κάποια επίθεση ή αφού έχει υποστεί ζημιά ένα μέρος του συστήματος.