ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Π Μ Σ: «Διδακτική της Τεχνολογίας & Ψηφιακά Συστήματα»

Risk Managment

Security Metrics

Πολλάτου Καλλιόπη

Σεπτέμβριος 2012

ΠΕΡΙΛΗΨΗ

Όλο και περισσότεροι οργανισμοί σε όλο τον κόσμο υιοθετούν μεθόδους αξιολόγησης της ασφάλειας των συστημάτων και των δικτύων τους, προκειμένου να είναι σε θέση να γνωρίζουν από τι απειλούνται και να εφαρμόσουν κατάλληλους ελέγχους έτσι ώστε να ελαχιστοποιήσουν ή ακόμη σε πολλές περιπτώσεις, να εξαλείψουν τις επιπτώσεις που θα υποστούν από μια πιθανή παραβίαση της ασφάλειας.
Με την εντατικοποίηση των προσπαθειών να δημιουργηθούν πιο ασφαλή προϊόντα και υπηρεσίες , η βιομηχανία παραγωγής λογισμικού έχει επικεντρωθεί στην βελτίωση της ασφάλειας των λογισμικών.

Η μέτρηση της ασφάλειας, τόσο ποιοτικά όσο και ποσοτικά, σήμερα αποτελεί αναπόσπαστο μέρος αυτής της βιομηχανίας (βιομηχανία παραγωγής λογισμικού).
Ποιοτικές προσεγγίσεις αξιολόγησης, πάσχουν από σημαντικές ελλείψεις που κυρίως προέρχονται από το είδος των ποιοτικών τιμών που χρησιμοποιούν. Ωστόσο, πολλές από αυτές τις ελλείψεις μπορούν να αντιμετωπιστούν με ποσοτικές προσεγγίσεις.

Ο βασικός σκοπός της παρούσας διπλωματικής εργασίας είναι να καθοριστεί ο όρος 'Μετρικές ασφάλειας' και να αναφερθούν τεχνικές ανάλυσης μετρικών ασφάλειας.

Πανεπιστήμιο Πειραιώς

Περιεχόμενα

Πανεπιστήμιο Πειραιώς

Πανεπιστήμιο Πειραιώς

ΕΙΣΑΓΩΓΗ

Σε ένα περιβάλλον ολοένα και πιο «διασυνδεδεμένο», είμαστε πλέον υποχρεωμένοι να αναπτύξουμε καλύτερες και πιο αποδοτικές άμυνες για τα συστήματα πληροφοριών μας. Στο παρελθόν, όταν η ασφάλεια των πληροφοριών ήταν το επίκεντρο των κυβερνήσεων και των στρατιωτικών μονάδων και όταν η ασφάλεια είχε σαν στόχο μόνο την έμπιστη ανταλλαγή πληροφοριών, τότε η έννοια της "απόλυτης" ασφάλειας εγκρίθηκε και εκατομμύρια δολάρια δαπανήθηκαν στο να εκπληρώσουν αυτόν τον σκοπό. Τα τελευταία χρόνια, οι απαιτήσεις του εμπορικού τομέα, έχουν αλλάξει και είναι πλέον κανόνας να αναζητείται «το κόστος της αποτελεσματικής ασφάλειας».

Ιδιαίτερη έμφαση δίνεται στην υιοθέτηση της παραδοχής, πως ορισμένοι «κίνδυνοι» θα πρέπει να γίνουν αποδεκτοί και να διαχειριστούν. Εάν η αξιολόγηση του κινδύνου δεν πραγματοποιείται αποτελεσματικά, τότε ο οργανισμός θα πρέπει είτε να σπαταλήσει πολλά χρήματα για την ασφάλεια των συστημάτων του είτε να εκτίθεται σε απροσδιόριστους κινδύνους.

Τον όρο ‘Risk Management’ τον αποδίδουμε σε μια λογική και συστηματική μέθοδο που χρησιμοποιείται για τον προσδιορισμό, την ανάλυση, την επεξεργασία και την παρακολούθηση των κινδύνων που εμπλέκονται σε οποιαδήποτε δραστηριότητα ή διαδικασία.

Είναι μία μεθοδολογία που βοηθά τα στελέχη μιας επιχείρησης να προβούν σε καλύτερη χρήση των διαθέσιμων πόρων τους. Χρησιμοποιείται ευρέως στο δημόσιο και στον ιδιωτικό τομέα, και καλύπτει ένα ευρύ φάσμα δραστηριοτήτων και λειτουργιών. Η αποτελεσματική διαχείριση των κινδύνων είναι μια αναγνωρισμένη αξία και ικανότητα. Πλέον έχει γίνει αναπόσπαστο μέρος του επιχειρηματικού σχεδιασμού.

Πανεπιστήμιο Πειραιώς

Τα βήματα της διαδικασίας διαχείρισης των κινδύνων είναι ένας γενικός κανόνας – οδηγός που ακολουθεί οποιοσδήποτε οργανισμός, ασχέτως με το είδος της επιχείρησης ή την δραστηριότητα της και είναι τα παρακάτω:

- Δημιουργία του πλαισίου
- Προσδιορισμός των κινδύνων
- Ανάλυση των κινδύνων
- Αξιολόγηση των κινδύνων
- Αντιμετώπιση των κινδύνων

Πανεπιστήμιο Πειραιώς

1. Ασφάλεια Πληροφοριακών Συστημάτων

Η αποτελεσματική διαχείριση της ασφάλειας πληροφοριών σε έναν οργανισμό περικλείει όλες τις οργανωτικές μονάδες, τις εταιρικές διαδικασίες και τις εμπλεκόμενες οντότητες με την ασφάλεια πληροφοριών. Η ασφάλεια πληροφοριών αποτελεί και πρέπει να αντιμετωπίζεται ως μία συνεχής διαδικασία, η οποία καθιστά τον οργανισμό ικανό να αντιμετωπίσει τα φλέγοντα ζητήματα ασφάλειας με στόχο να ικανοποιήσει τους επιχειρηματικούς του στόχους.

Η έννοια της ασφάλειας των Δικτύων και Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Εκτός αυτού, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Η ασφάλεια των δικτύων υπολογιστών διασφαλίζεται με τρεις βασικές έννοιες.

- Εμπιστευτικότητα (confidentiality): Εξασφάλιση ότι η πληροφορία είναι προσβάσιμη μόνο από όσους είναι εξουσιοδοτημένοι.
- Ακεραιότητα (integrity): Η διασφάλιση της ακρίβειας και της πληρότητας των πληροφοριών καθώς και των μεθόδων επεξεργασίας της.

Πανεπιστήμιο Πειραιώς

- Διαθεσιμότητα (availability): Εξασφάλιση ότι οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στην πληροφορία όποτε απαιτείται.

Η ασφάλεια πληροφοριών επιτυγχάνεται με την υλοποίηση των κατάλληλων μηχανισμών ελέγχου, οι οποίοι μπορεί να είναι πολιτικές ή πρακτικές διαδικασίες, οργανωτικές δομές και λειτουργίες λογισμικού.

Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών είναι ιδιαίτερα σημαντικά για τη διατήρηση ανταγωνιστικού πλεονεκτήματος, τη συμμόρφωση με τους νόμους, την εταιρική εικόνα και τα κέρδη μιας επιχείρησης που δραστηριοποιείται στο χώρου του ηλεκτρονικού εμπορίου.

Τα πληροφοριακά συστήματα και τα δίκτυα των οργανισμών συνεχώς αντιμετωπίζουν απειλές στην ασφάλεια τους από ένα μεγάλο εύρος διαφορετικών πηγών, όπως η ηλεκτρονική απάτη, η βιομηχανική κατασκοπεία, ο βανδαλισμός, και τα φυσικά φαινόμενα. Επιπλέον επιθέσεις με ιούς (computer viruses), hacking, και επιθέσεις τύπου άρνησης παροχής υπηρεσιών έχουν γίνει πλέον συνήθεις και όλο πιο πολύπλοκες στην αντιμετώπιση τους. Καθώς οι επιχειρήσεις εξαρτώνται από τα πληροφοριακά τους συστήματα, οι απειλές προς αυτά επηρεάζουν σημαντικά τις λειτουργίες των ίδιων των επιχειρήσεων.

Στην αρχική σχεδίαση πολλών πληροφοριακών συστημάτων δεν έχουν συμπεριληφθεί χαρακτηριστικά ασφάλειας. Η ασφάλεια που προσφέρουν είναι περιορισμένη και πρέπει να συμπληρωθεί από κατάλληλη διαχείριση και υλοποίηση επιμέρους διαδικασιών. Η επιλογή των κατάλληλων μηχανισμών ελέγχου, προϋποθέτει προσεκτικό και λεπτομερή σχεδιασμό.

Πανεπιστήμιο Πειραιώς

Βασικές έννοιες οι οποίες χρησιμοποιούνται στην ασφάλεια υπολογιστικών συστημάτων είναι οι Απαιτήσεις Ασφάλειας, οι Κίνδυνοι Ασφάλειας και οι Μηχανισμοί Ασφάλειας.

Απαιτήσεις ασφάλειας:

Είναι σημαντικό ένας οργανισμός να προσδιορίσει τις πραγματικές απαιτήσεις του σε θέματα ασφάλειας. Υπάρχουν τρεις κύριες πηγές για το σκοπό αυτό:

- Η αποτίμηση των κινδύνων που αντιμετωπίζει ο οργανισμός. Έτσι αναγνωρίζονται οι πιθανές απειλές προς το σύστημα, εκτιμάται η ευπάθειά του στις συγκεκριμένες απειλές και η πιθανότητα υλοποίησης τους καθώς και υπολογίζεται το κόστος που θα έχουν για τον οργανισμό.

- Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.

- Το σύνολο των αρχών, των απαιτήσεων και των στόχων για την επεξεργασία των πληροφοριών, που ορίζει ο ίδιος ο οργανισμός.

Κίνδυνοι ασφάλειας:

Οι απαιτήσεις ασφάλειας του οργανισμού προκύπτουν ύστερα από μεθοδική καταγραφή των κινδύνων που αντιμετωπίζει ο οργανισμός. Το κόστος των μηχανισμών ασφάλειας θα πρέπει να δικαιολογείται από την πιθανή ζημιά στον οργανισμό σε περίπτωση που παραβιαστεί η ασφάλεια του.

Πανεπιστήμιο Πειραιώς

Η αποτίμηση των κινδύνων ασφάλειας είναι μια συστηματική εξέταση των ακόλουθων παραγόντων:

- Της πιθανής ζημιάς που θα υποστεί ο οργανισμός σε περίπτωση που προκύψει κάποιος κίνδυνος ασφάλειας, συμπεριλαμβανομένων των συνεπειών από την απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας των πληροφοριών.
- Εκτίμησης της πιθανότητας να εμφανιστεί ένας τέτοιος κίνδυνος ασφάλειας σε σχέση με τους υπάρχοντες μηχανισμούς ελέγχου.

Τα αποτελέσματα αυτής της αποτίμησης καθορίζουν τις κατάλληλες ενέργειες και προτεραιότητες του οργανισμού, καθώς και τους τρόπους υλοποίησης των μηχανισμών ελέγχου της ασφάλειας απέναντι σε αυτούς τους κινδύνους. Η διαδικασία αποτίμησης των κινδύνων και η επιλογή των κατάλληλων μηχανισμών ελέγχου μπορεί να επαναληφθεί πολλές φορές προκειμένου να καλύψει διαφορετικά τμήματα του οργανισμού.

Είναι σημαντικό να γίνεται περιοδικός έλεγχος των κινδύνων ασφάλειας όπως και των μηχανισμών προστασίας προκειμένου να επιτυγχάνεται προσαρμογή στις ανάγκες και τις προτεραιότητες του οργανισμού, επέκταση στην προστασία από νέους κινδύνους, καθώς και επιβεβαίωση της ορθής και αποτελεσματικής λειτουργίας των υπαρχόντων μηχανισμών προστασίας.

Πανεπιστήμιο Πειραιώς

Μηχανισμοί ασφάλειας:

Αφού καθοριστούν οι απαιτήσεις ασφάλειας, μπορεί να γίνει η επιλογή των κατάλληλων μηχανισμών ελέγχου και προστασίας, οι οποίοι θα μειώσουν τον κίνδυνο σε αποδεκτά επίπεδα.

Οι μηχανισμοί θα πρέπει να επιλεγούν με βάση το κόστος υλοποίησης τους σε σχέση με τους κινδύνους που θα αντιμετωπίζουν καθώς και το κόστος των πιθανών επιπτώσεων των κινδύνων αυτών στον οργανισμό. Ποιοτικοί παράγοντες, όπως απώλεια φήμης του οργανισμού θα πρέπει να λαμβάνονται υπόψη.

Οι μηχανισμοί ελέγχου αποτελούν τη βάση για την ασφάλεια των πληροφοριών. Οι μηχανισμοί αυτοί βασίζονται είτε σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική στην ασφάλεια.

Μηχανισμοί βασισμένοι στη νομοθεσία είναι:

- Προστασία προσωπικών δεδομένων.
- Προστασία δεδομένων του οργανισμού.
- Δικαιώματα πνευματικής ιδιοκτησίας.

Μηχανισμοί που έχουν καθιερωθεί ως κοινή πρακτική είναι:

- Πολιτική ασφάλειας πληροφοριών.
- Καταμερισμός καθηκόντων που σχετίζονται με την ασφάλεια.
- Εκπαίδευση και κατάρτιση σε θέματα ασφάλειας.
- Αναφορά συμβάντων ασφάλειας.

Πανεπιστήμιο Πειραιώς

Οι πιο πάνω μηχανισμοί αποτελούν βασικά βήματα στην ασφάλεια και μπορούν να χρησιμοποιηθούν σχεδόν σε κάθε οργανισμό.

1.1. Πολιτική Ασφαλείας

Η πολιτική ασφάλειας πληροφοριών παρέχει κατευθύνσεις και υποστήριξη για τα ζητήματα ασφάλειας πληροφοριών. Η διοίκηση του οργανισμού θα πρέπει να καθορίσει μια σαφή πολιτική, την οποία θα υποστηρίζει έμπρακτα.

Το κείμενο της πολιτικής ασφάλειας θα πρέπει να γίνει αποδεκτό από τη διοίκηση του οργανισμού και έπειτα θα πρέπει να δημοσιοποιηθεί σε όλους τους υπαλλήλους. Θα πρέπει τουλάχιστον να περιλαμβάνει τα ακόλουθα:

- Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητα της.
- Την υποστήριξη της διοίκησης αναφορικά με την ασφάλεια.
- Την επεξήγηση της πολιτικής ασφάλειας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει ο οργανισμός, όπως σχετική νομοθεσία, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, προστασία από ιούς κλπ.
- Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας πληροφοριών.

Θα πρέπει να υπάρχει ένας υπεύθυνος για την πολιτική ασφάλειας, καθήκον του οποίου θα είναι ο περιοδικός έλεγχος και αναπροσαρμογή της ασφάλειας. Ο περιοδικός έλεγχος πρέπει να γίνεται σύμφωνα με την αποτελεσματικότητα της ασφάλειας δηλαδή με βάση τα περιστατικά

Πανεπιστήμιο Πειραιώς

παραβίασης της ασφάλειας, το κόστος των μηχανισμών προστασίας καθώς και την εξέλιξη της τεχνολογίας.

1.2. Ασφάλεια ενός Οργανισμού

Η διαχείριση της ασφάλειας μέσα σε έναν οργανισμό υλοποιείται και ελέγχεται από την υποδομή ασφάλειας πληροφοριών. Θα πρέπει να υπάρχει υποστήριξη από τη διοίκηση του οργανισμού για τη δημιουργία και εφαρμογή της πολιτικής ασφάλειας καθώς και τον καταμερισμό καθηκόντων. Αν είναι αναγκαίο, θα πρέπει να ζητηθεί η βοήθεια εμπειρογνωμόνων εκτός του οργανισμού.

Συντονισμός ασφάλειας πληροφοριών

Σε ένα οργανισμό θα πρέπει να υπάρχει μια ομάδα εργασίας η οποία θα συντονίζει την υλοποίηση των μηχανισμών προστασίας. Μια τέτοια τυπική ομάδα αναλαμβάνει τα ακόλουθα:

- Καθορίζει συγκεκριμένους ρόλους και καθήκοντα για την ασφάλεια του οργανισμού.
- Καθορίζει συγκεκριμένες διαδικασίες για την υλοποίηση της ασφάλειας, όπως αποτίμηση κινδύνου, διαβαθμίσεις ασφάλειας κλπ.
- Διασφαλίζει ότι η ασφάλεια αποτελεί μέρος των δραστηριοτήτων του οργανισμού.
- Ελέγχει την υλοποίηση συγκεκριμένων μηχανισμών ασφάλειας για νέα συστήματα και υπηρεσίες.

Πανεπιστήμιο Πειραιώς

- Εξετάζει τα συμβάντα σχετικά με την ασφάλεια.
- Υποστηρίζει ενεργά την εφαρμογή της ασφάλειας σε όλα τα τμήματα του οργανισμού.

Καθορισμός καθηκόντων

Τα καθήκοντα για την προστασία συγκεκριμένων στοιχείων του οργανισμού και την εφαρμογή συγκεκριμένων διαδικασιών θα πρέπει να είναι σαφώς καθορισμένα. Η πολιτική ασφάλειας θα πρέπει να παρέχει γενικές κατευθύνσεις για τον καθορισμό των ρόλων και των αρμοδιοτήτων στον οργανισμό.

Σε πολλούς οργανισμούς ένας υπεύθυνος ασφάλειας θα πρέπει να αναλάβει τον καθορισμό και την υλοποίηση της ασφάλειας, όπως και την επιλογή των μηχανισμών προστασίας και ελέγχου. Την ευθύνη για την καθημερινή ασφάλεια συγκεκριμένων στοιχείων του οργανισμού θα την έχουν επιλεγμένα στελέχη, τα οποία θα είναι οι τυπικοί ιδιοκτήτες τους.

Συνδρομή ειδικών εμπειρογνωμόνων

Είναι πιθανό σε πολλούς οργανισμούς να απαιτείται η συνδρομή ειδικών εμπειρογνωμόνων σε θέματα ασφάλειας. Οι εμπειρογνώμονες αυτοί, θα πρέπει να μπορούν να βοηθήσουν τον οργανισμό σε κάθε ζήτημα ασφάλειας. Οι γνώσεις τους και η εμπειρία τους, επηρεάζουν άμεσα την αποτελεσματικότητα της ασφάλειας του οργανισμού.

Η συνδρομή του συμβούλου ασφάλειας πρέπει να ζητείται όταν υπάρχει υποψία παραβίασης της ασφάλειας του οργανισμού ή όταν έχει παρουσιαστεί κάποιος καινούργιος κίνδυνος.

Πανεπιστήμιο Πειραιώς

Ανεξάρτητος έλεγχος της ασφάλειας

Το κείμενο της πολιτικής ασφάλειας καθορίζει την πολιτική και τις ευθύνες για την ασφάλεια των πληροφοριών. Η εφαρμογή του θα πρέπει να ελέγχεται ανεξάρτητα και συστηματικά, ώστε να επιβεβαιωθεί ότι οι πρακτικές που ακολουθεί ο οργανισμός είναι σύμφωνες με την πολιτική ασφάλειας του.

2. Μετρικές ασφάλειας

Οι μετρικές ασφάλειας (security metrics) είναι ένας τομέας της ασφάλειας υπολογιστών που συγκεντρώνει μεγάλο ερευνητικό ενδιαφέρον τον τελευταίο καιρό. Δεν είναι ένα νέο θέμα, αλλά ένα θέμα το οποίο επικεντρώνει το ενδιαφέρον σποραδικά. Πολλά από αυτά που έχουν γραφτεί σχετικά με τις μετρικές έχουν στόχο την παροχή κατευθυντήριων γραμμών για τον καθορισμό μιας μετρικής ασφάλειας και τον καθορισμό κριτηρίων γύρω από αυτή. Ωστόσο, δεν είναι ξεκάθαρο ποιες μετρικές είναι ουσιαστικά χρήσιμες και ποιες έχουν αποδειχθεί χρήσιμες στην πορεία. [1] ,[2].

Οι πληροφορίες από τις μετρικές ασφάλειας θεωρούνται σημαντικός παράγοντας στη λήψη ορθών αποφάσεων σχετικά με διάφορες πτυχές της ασφάλειας, όπως ο σχεδιασμός των αρχιτεκτονικών ασφάλειας καθώς και οι έλεγχοι για την αποτελεσματικότητα και την αποδοτικότητα των λειτουργιών που σχετίζονται με την ασφάλεια δικτύων και υπολογιστών. Η χρήση μετρικών ασφάλειας έχει ως στόχο να προσφέρει μια ποσοτική και αντικειμενική βάση για τη διασφάλιση της ασφάλειας. Οι κύριες χρήσεις εμπίπτουν σε διάφορες μεγάλες κατηγορίες:

- Στρατηγική υποστήριξη - Εκτιμήσεις των ιδιοτήτων ασφαλείας μπορούν να χρησιμοποιηθούν για να βοηθήσουν στην λήψη

Πανεπιστήμιο Πειραιώς

αποφάσεων, που αφορούν στο χρονοπρογραμματισμό, στην κατανομή των πόρων, και στην επιλογή των προϊόντων και των υπηρεσιών.

- Διασφάλιση ποιότητας – Οι μετρικές ασφαλείας μπορούν να χρησιμοποιηθούν κατά τη διάρκεια του κύκλου ζωής ανάπτυξης λογισμικού για την εξάλειψη των τρωτών σημείων, ιδιαίτερα κατά την παραγωγή του κώδικα, εκτελώντας λειτουργίες, όπως είναι η μέτρηση που εξασφαλίζει την τήρηση των προτύπων κωδικοποίησης, ο εντοπισμός των πιθανών αδυναμιών που μπορεί να υπάρχουν, και η παρακολούθηση και ανάλυση ελαττωμάτων ασφαλείας που μπορεί τελικά να προκύψουν.

- Τακτική εποπτεία - παρακολούθηση και υποβολή εκθέσεων για την κατάσταση ασφάλειας ενός πληροφοριακού συστήματος μπορούν να εφαρμοστούν τόσο για να εξακριβωθεί η συμμόρφωση με τις απαιτήσεις ασφαλείας (π.χ την πολιτική, τις διαδικασίες και τους κανονισμούς), όσο και για τη μέτρηση της αποτελεσματικότητας των ελέγχων ασφάλειας και τη διαχείριση κινδύνου, καθώς και τον καθορισμό συγκεκριμένων τομέων για βελτίωση.

Οι μετρικές ασφάλειας μπορούν να ταξινομηθούν με διάφορους τρόπους. Μια απλή ταξινόμηση είναι με βάση τις μετρικές που δηλώνουν το επίπεδο ωριμότητας των διαδικασιών που θεωρούνται ότι συμβάλλουν στην ασφάλεια του συστήματος, σε αντίθεση με τις μετρικές εκείνες που δηλώνουν το βαθμό στον οποίο κάποιο χαρακτηριστικό ασφαλείας είναι παρόν σε ένα σύστημα [3]. Η πρώτη εφαρμόζεται σε διαδικασίες ασφαλείας και στην εκπαίδευση που γίνεται κατά τον σχεδιασμό, τη διαμόρφωση, τη συντήρηση και τη λειτουργία ενός συστήματος. Η δεύτερη περίπτωση ισχύει για την κατάσταση ασφάλειας του συστήματος και το επίπεδο του κινδύνου.

Πανεπιστήμιο Πειραιώς

Υπάρχουν φυσικά περισσότερες σύνθετες ταξινομήσεις μετρικών ασφάλειας [4], [5].

Σε άλλους επιστημονικούς κλάδους, όπως στον τομέα της οικονομίας, έχουν χρησιμοποιηθεί ποσοτικές μέθοδοι για τον καθορισμό του κινδύνου σε συνδυασμό με τη λήψη αποφάσεων-πλαισίων, που βασίζονται σε καθιερωμένες μετρήσεις και μετρικές. Στο χώρο της ασφάλειας υπολογιστών μόλις εμφανίζονται τυποποιημένες μετρικές για την ασφάλεια του συστήματος πληροφοριών. Όμως, όπως σε κάθε επιστημονικό κλάδο, απαιτούνται ρεαλιστικές παραδοχές και δεδομένα για την επίτευξη αξιόπιστων αποτελεσμάτων. [6]

2.1. Θεωρητικό υπόβαθρο

Ο όρος «μετρικές ασφάλειας» χρησιμοποιείται συχνά σήμερα, αλλά με μια γκάμα εννοιών και ερμηνειών. Παρακάτω αναφέρονται μερικά παραδείγματα από πρόσφατες δημοσιεύσεις:

Σε υψηλό επίπεδο, οι μετρικές αποτελούν ποσοτικές μετρήσεις κάποιας άποψης του συστήματος ή της επιχείρησης. Για μια οντότητα (σύστημα, προϊόν, ή άλλο) για την οποία η ασφάλεια είναι μια σημαντική έννοια, υπάρχουν κάποια αναγνωρίσιμα χαρακτηριστικά που χαρακτηρίζουν συλλογικά την ασφάλεια της εν λόγω οντότητας. Περαιτέρω, μια μετρική ασφάλειας (ή ο συνδυασμός μετρικών ασφάλειας) είναι ένα μέτρο της ποσότητας αυτού του χαρακτηριστικού που κατέχει η εν λόγω οντότητα. [7]

Οι Μετρικές είναι εργαλεία που έχουν σχεδιαστεί για να διευκολύνουν τη λήψη αποφάσεων και τη βελτίωση των επιδόσεων που αφορούν στην ακρίβεια, μέσω της συλλογής, της ανάλυσης και της αναφοράς δεδομένων. Σκοπός της μέτρησης των επιδόσεων είναι τόσο η παρακολούθηση της κατάστασης των μετρούμενων δραστηριοτήτων όσο και να διευκολυνθεί η

Πανεπιστήμιο Πειραιώς

βελτίωση σε αυτές τις δραστηριότητες από την εφαρμογή διορθωτικών ενεργειών, βάσει των παρατηρούμενων μετρήσεων.

Οι μετρήσεις παρέχουν μια μεμονωμένη στο χρόνο άποψη ειδικών, διακριτών παραγόντων, ενώ οι μετρικές προέρχονται από τη σύγκριση και το συνδυασμό δύο ή περισσότερων μετρήσεων που ελήφθησαν μέσα στο χρόνο. Οι μετρήσεις προκύπτουν από την καταμέτρηση, ενώ οι μετρικές προκύπτουν από την ανάλυση. Με άλλα λόγια, οι μετρήσεις είναι αντικειμενικά δεδομένα ενώ οι μετρικές είναι είτε αντικειμενικές είτε υποκειμενικές ανθρώπινες ερμηνείες των στοιχείων αυτών. [8]

Μια μετρική συνεπάγεται ένα σύστημα μέτρησης που βασίζεται σε μετρήσιμες μεταβλητές. Οι μετρίσιμες τιμές των ιδιοτήτων πρέπει να διαταχτούν γραμμικά και η μέθοδος μέτρησης να οριστεί πλήρως, καθώς και να οριστούν οι λεπτομέρειες για το πώς συγκεκριμένοι παράγοντες προορίζονται για μέτρηση ή για αξιολόγηση. Σημαντικό είναι να δίνονται επεξηγήσεις των πηγών αβεβαιότητας. [9]

Για την ασφάλεια ενός συστήματος πληροφοριών, τα μέτρα αφορούν πτυχές του συστήματος που συμβάλλουν στην ασφάλεια του. Δηλαδή, οι μετρικές ασφαλείας περιλαμβάνουν την εφαρμογή μιας μεθόδου μέτρησης σε μια ή περισσότερες οντότητες ενός συστήματος που υπόκεινται σε κάποια σημαντική ιδιότητα από άποψη ασφάλειας. Από οργανωτική άποψη, τα μέτρα ασφαλείας και οι μετρικές θα πρέπει να επιτρέπουν σε έναν οργανισμό να μπορεί να εκτιμήσει πόσο καλά έχει επιτύχει τους στόχους της ασφάλειας.

Για να έχει αξία, η μέθοδος που χρησιμοποιούν οι μετρικές θα πρέπει να μπορούν να αναπαραχθούν, δηλαδή, να επιτυγχάνεται το ίδιο αποτέλεσμα όταν εκτελείται από διαφορετικούς αρμόδιους αξιολογητές. Το αποτέλεσμα θα πρέπει επίσης να είναι επαναλαμβανόμενο, έτσι ώστε μια δεύτερη εκτίμηση από τους ίδιους αξιολογητές να παράγει το ίδιο

Πανεπιστήμιο Πειραιώς

αποτέλεσμα. Η συνάφεια και η επικαιρότητα είναι επίσης σημαντικά στοιχεία, δεδομένου ότι δεν είναι ιδιαίτερα χρήσιμο να υπάρχουν μετρικές οι οποίες δεν έχουν νόημα ή η εφαρμογή τους απαιτεί αυξημένους πόρους του δικτύου με αποτέλεσμα την υπερφόρτωσή του.

Ενώ υπάρχει κάποια κλίση προς τις ποσοτικές μετρικές για την ασφάλεια των πληροφοριακών συστημάτων, στην πράξη, κατά κανόνα χρησιμοποιούνται ποιοτικά μέτρα τα οποία απεικονίζουν αιτιολογημένες εκτιμήσεις της ασφάλειας από έναν αξιολογητή. Δηλαδή, οι μετρικές ασφαλείας των ιδιοτήτων ενός συστήματος πληροφοριών συχνά με βάση την εμπειρία ενός αξιολογητή, μπορούν να επιφέρουν μια διάταξη, η οποία στη συνέχεια προσδιορίζεται ποσοτικά (π.χ., 1 = χαμηλή, 2 = μέση, 3 = υψηλή). Λόγω της συγκεκριμένης υποκειμενικότητας, μερικά από τα χαρακτηριστικά αυτά δεν είναι εύκολο να χρησιμοποιηθούν πρακτικά. Για παράδειγμα, τα αποτελέσματα της ανίχνευσης εισβολέων (Intrusion detection) ή άλλων μεθόδων αξιολόγησης που χρειάζονται εξειδικευμένες δεξιότητες μερικές φορές δεν μπορούν να επαναληφθούν, καθώς βασίζονται στη γνώση, το ταλέντο και την εμπειρία ενός αξιολογητή, ο οποίος μπορεί να διαφοροποιείται από τους άλλους αξιολογητές.

2.2. Πτυχές των Μετρήσεων Ασφαλείας

Πολλοί οργανισμοί έχουν επιχειρήσει πολλές σημαντικές προσπάθειες για τη μέτρηση ή την αξιολόγηση της ασφάλειας. Σε αυτές περιλαμβάνονται τα παρακάτω:

- Trusted Computer System Evaluation Criteria (TCSEC) [24],
- Information Technology Security Evaluation Criteria (ITSEC) [10],

Πανεπιστήμιο Πειραιώς

- Systems Security Engineering Capability Maturity Model (SSE-CMM) [7]

- Common Criteria. [11]

Κάθε μια από αυτές τις προσπάθειες δεν είχε την αναμενόμενη επιτυχία. Είναι λογικό να συμπεραίνει κανείς από τη μέχρι σήμερα εμπειρία ότι η μέτρηση της ασφάλειας είναι ένα δύσκολο πρόβλημα, το οποίο δεν πρέπει να υποτιμηθεί. [12]

Το Ινστιτούτο για την προστασία υποδομών πληροφοριών (Institute for Information Infrastructure Protection - I3P) ανέφερε το 2009 πως οι μετρικές ασφάλειας αναγνωρίστηκαν ως μία από τις τέσσερις προτεραιότητες έρευνας και ανάπτυξης για τα επόμενα πέντε έως δέκα χρόνια. [13]

Παρακάτω παρουσιάζονται κάποιες παρατηρήσεις σχετικά με ορισμένες κρίσιμες πτυχές των μετρήσεων ασφάλειας που προέκυψαν από προηγούμενες προσπάθειες. Ο στόχος είναι να αναδειχθούν οι παράγοντες που θεωρούνται πως είναι σχετικοί με μια ερευνητική προσπάθεια στις μετρικές ασφάλειας.

2.3. Ορθότητα και αποτελεσματικότητα

Η ασφάλεια ενός πληροφοριακού συστήματος αποτελείται από δύο αλληλένδετες έννοιες: την ορθότητα και την αποτελεσματικότητα. Η ορθότητα παρέχει τη διαβεβαίωση ότι ο κάθε μηχανισμός έχει εφαρμοστεί σωστά (δηλαδή, πως λειτουργεί ακριβώς όπως έχει σχεδιαστεί για να λειτούργει, όπως για παράδειγμα για να εκτελεί άριστα κάποιο υπολογισμό). Η αποτελεσματικότητα παρέχει τη διαβεβαίωση ότι ο κάθε μηχανισμός του συστήματος ανταποκρίνεται στους επιδιωκόμενους στόχους ασφαλείας (δηλαδή, δεν κάνει τίποτα διαφορετικό από αυτό που προορίζεται να κάνει,

Πανεπιστήμιο Πειραιώς

ικανοποιώντας παράλληλα τις προσδοκίες για ανθεκτικότητα). Είναι συχνό το φαινόμενο να παράγεται ένα πρόγραμμα το οποίο ικανοποιεί τα κριτήρια της ορθότητας, αλλά δεν πληρεί τα κριτήρια της αποτελεσματικότητας, ιδιαίτερα κάτω από έκτακτες και απρόβλεπτες συνθήκες.

Η ορθότητα μπορεί να αξιολογηθεί σε σχέση με την αναπτυξιακή διαδικασία και το περιβάλλον ανάπτυξης κατά την κατασκευή του συστήματος, αλλά και από τον τρόπο λειτουργίας του. Έμφαση δίνεται συνήθως στην τεκμηρίωση του πόσο καλά το σύστημα παρουσιάζει την αναμενόμενη συμπεριφορά κατά την χρήση του.

Η αξιολόγηση της αποτελεσματικότητας προκύπτει από τη δυνατότητα του εν λόγω μηχανισμού ασφαλείας να αντέχει τις επιθέσεις κατά την εκτέλεση των λειτουργιών του. Για την αποτελεσματικότητα απαιτείται να διαπιστωθεί πόσο καλά οι διάφοροι μηχανισμοί ασφαλείας δένουν μεταξύ τους και δρουν συνεργατικά, οι επιπτώσεις όλων των γνωστών ή μη προβλημάτων ασφαλείας και πώς όλα τα παρακάνω επηρεάζουν την ευχρηστία του συστήματος. Έμφαση δίνεται συνήθως στον έλεγχο για το αν το σύστημα παρουσιάζει ευπάθειες ασφαλείας (security vulnerabilities).

Στην πράξη, οι αξιολογήσεις ασφάλειας της ορθότητας και της αποτελεσματικότητας σε μεγάλο βαθμό γίνονται μέσω της λογικής και όχι μέσω άμεσης μέτρησης πραγματικών στοιχείων του hardware και του software. Συχνά, γίνονται απλουστευμένες υποθέσεις. Για παράδειγμα, μπορεί να υποτεθεί ότι το σύστημα επικοινωνεί μόνο με άλλα συστήματα που λειτουργούν υπό τον έλεγχο του ίδιου διαχειριστή και συνεπώς έχουν κοινή πολιτική ασφάλειας. Δεν θα πρέπει όμως να αντιμετωπίζεται ξεχωριστά η ανάγκη να εμπιστεύονται και να επικοινωνούν με εξωτερικά συστήματα που λειτουργούν υπό τον έλεγχο διαφορετικού διαχειριστή. [9]

Πανεπιστήμιο Πειραιώς

2.4. Leading και Lagging Indicators

Σε αναλογία με τους οικονομικούς δείκτες, οι μετρικές ασφάλειας μπορεί δυνητικά να είναι δείκτες οι οποίοι σε σχέση με την πραγματική κατάσταση της ασφάλειας του συστήματος είτε υστερούν χρονικά (Lagging Indicators), είτε είναι σύγχρονοι και συμπίπτουν, είτε προτρέχουν (Leading indicators). Η διάκριση είναι σημαντική. Αν ένας δείκτης που υστερεί αντιμετωπίζεται ως δείκτης που συμπίπτει ή προτρέχει, οι συνέπειες της παρερμηνείας και της αντίστοιχης αντίδρασης μπορεί να είναι σοβαρές. Όσο μεγαλύτερη είναι η λανθάνουσα περίοδος (latency period) για ένα Lagging Indicator, τόσο μεγαλύτερη είναι η πιθανότητα εμφάνισης προβλημάτων. Προφανώς, ένας δείκτης που υστερεί και παρουσιάζει σύντομη λανθάνουσα περίοδο ή καθυστέρηση είναι προτιμότερος από έναν που παρουσιάζει μακρά περίοδο λανθάνουσας κατάστασης, δεδομένου ότι κάθε απαραίτητη αντίδραση σε μια παρατηρούμενη αλλαγή στην ασφάλεια, μπορεί να λάβει χώρα νωρίτερα. Είναι σημαντικό να αναγνωρίζει κανείς ποιοι δείκτες παρουσιάζουν αυτή τη συμπεριφορά και αν χρησιμοποιούνται, πρέπει να είναι κανείς έτοιμος να αντιμετωπίσει την εγγενή καθυστέρηση και διάφορους συναφείς περιορισμούς.

Απλές αθροίσεις, όταν χρησιμοποιούνται ως μέτρο ασφαλείας, μπορεί να είναι ιδιαίτερα δύσκολο να ταξινομηθούν και να ερμηνευτούν. Για παράδειγμα, μπορεί μια αύξηση στον αριθμό των ιών, που ανιχνεύθηκαν από το λογισμικό προστασίας από ιούς, να χρησιμοποιηθεί ως Leading indicator, επειδή η αυξημένη δραστηριότητα δείχνει ένα υψηλό επίπεδο απειλής. Η ίδια παρατήρηση μπορεί να χρησιμοποιηθεί ως Lagging Indicator, γιατί η αυξημένη δραστηριότητα επιδεικνύει ένα εξαιρετικά αποδοτικό μηχανισμό προστασίας από ιούς, ή να χρησιμεύσουν ως σύγχρονος δείκτης που συμπίπτει με την κατάσταση του συστήματος, γιατί η αυξημένη δραστηριότητα λειτουργεί ως κοινοποίηση ότι άλλοι μηχανισμοί επιβολής ασφάλειας αποτυγχάνουν. Ομοίως, μειωμένη δραστηριότητα μπορεί να

Πανεπιστήμιο Πειραιώς

συμβαίνει είτε επειδή ο μηχανισμός προστασίας από ιούς χάνει την αποτελεσματικότητά του, είτε άλλοι μηχανισμοί επιβολής ασφάλειας παρουσιάζουν ολοένα και μεγαλύτερη επιτυχία, ή το σύστημα απλά δεν υπόκειται σε τόσες επιθέσεις.

Πολλές μετρικές ασφάλειας μπορεί να θεωρηθούν ως δείκτες που υστερούν χρονικά. Η τάση των αρχικών εκτιμήσεων της ασφάλειας του συστήματος, εάν έχουν γίνει είτε από έναν άνθρωπο - αξιολογητή (για παράδειγμα μέσω ελέγχων ανίχνευσης εισβολής), είτε από αυτοματοποιημένες διαδικασίες (για παράδειγμα μέσω ελέγχων στα αρχεία καταγραφής του συστήματος), ή με κάποιο συνδυασμό των δύο παραπάνω, είναι πιθανό να αλλάξει τελικά σε ένα χαμηλότερο επίπεδο απειλής. Ο κύριος λόγος είναι ότι με την πάροδο του χρόνου, επέρχεται καλύτερη γνώση του συστήματος και ταχύτερη εύρεση των ευπαθειών του, ιδίως υπό το πρίσμα επιτυχημένων επιθέσεων στο σύστημα ή με τη σύγκριση με άλλα συστήματα που παρουσιάζουν ανάλογα χαρακτηριστικά. Η καλύτερη γνώση του συστήματος στη συνέχεια οδηγεί σε περαιτέρω αξιολόγηση της κατάστασης του (π.χ. μέσω πρόσθετων ελέγχων). Ενώ ορισμένα προγράμματα αξιολόγησης έχουν διαδικασίες ανανέωσης της αρχικής αξιολόγησης της κατάστασης ασφάλειας του συστήματος, δε μπορεί να αποφευχθεί κάποια σημαντική καθυστέρηση μέχρι να γίνει ακριβής αξιολόγηση της κατάστασης. Δεν υπάρχει μετρική που να μπορεί να υποδηλώσει την κατάσταση της ασφάλειας ενός συστήματος απόλυτα [9], [15], [16].

2.5.Ποιοτικές και ποσοτικές Ιδιότητες

Η μέτρηση των ιδιοτήτων ενός λογισμικού, σε γενικές γραμμές είναι δύσκολο να επιτευχθεί . Πολλές επιθυμητές ιδιότητες, όπως η πολυπλοκότητα, η χρηστικότητα και η επεκτασιμότητα, είναι ιδιότητες που μπορεί να

Πανεπιστήμιο Πειραιώς

εκφράζονται με γενικούς όρους, αλλά είναι δύσκολο να προσδιοριστούν με αντικειμενικούς όρους που να είναι χρήσιμοι στη πράξη.

Η διάκριση μεταξύ της ποσοτικής και ποιοτικής μέτρησης της ασφάλειας δεν είναι ευδιάκριτη.[17]

Ποιοτικές αναθέσεις μπορεί να χρησιμοποιηθούν για να αναπαραστήσουν ποσοτικές μετρήσεις ιδιοτήτων ασφαλείας (π.χ., Χαμηλή σημαίνει ότι δε βρέθηκαν ευπάθειες, Μέση: βρέθηκαν μεταξύ ενός και πέντε, Υψηλή: βρέθηκαν πάνω από πέντε προβλήματα ασφάλειας). Πιο συχνά, χρησιμοποιούνται αριθμητικές τιμές για να αντιπροσωπεύσουν ταξινομήσεις που είναι ποιοτικές (π.χ., 1, 2, και 3, έναντι χαμηλής, μέσης και υψηλής). Η αριθμητική διαφορά μεταξύ τιμών μπορεί να είναι σημαντική για ορισμένες μετρήσεις, ενώ μπορεί να μην είναι για άλλες, πράγμα που συμβαίνει συχνά με τις μετρικές ασφάλειας.

Ποσοτικές αποτιμήσεις πολλών ιδιοτήτων ασφάλειας μπορούν να συνδυαστούν για τη δημιουργία μιας σύνθετης αξίας (π.χ., βαθμολογία = 0,25 * rankingA + rankingB * 0,75). Τέτοιες συνθέσεις μπορούν, ωστόσο, να παράγουν ανεπιθύμητα αποτελέσματα. Για παράδειγμα, στο σύστημα βαθμολόγησης ευπαθειών Common Vulnerability Scoring System (CVSS), πολλές περιπτώσεις ευπαθειών με διαφορετικά χαρακτηριστικά λάμβαναν τα ίδια αποτελέσματα, παρότι ήταν σαφώς σε πολύ διαφορετικά επίπεδα σοβαρότητας, γεγονός που οδήγησε στην αναθεώρηση της φόρμουλας [18].

Μερικές ποιοτικές ιδιότητες δεν μπορούν να ληφθούν με απευθείας μέτρηση. Ένα χαρακτηριστικό, όπως η ομορφιά, το άρωμα, ή η γεύση μπορεί να είναι υποκειμενικό, και ποικίλει από άτομο σε άτομο. Υπάρχουν περιπτώσεις όπου καμία ποσότητα δεν μπορεί να προσδιοριστεί με σαφήνεια, όπως η γεύση του κρασιού, είτε μια ομάδα εμπειρογνωμόνων βαθμολογεί τη

Πανεπιστήμιο Πειραιώς

κατάσταση με χρήση ποσοστών, είτε χρησιμοποιούνται κάποια μετρήσιμα χαρακτηριστικά τα οποία πιστεύεται ότι συσχετίζονται άμεσα με την εν λόγω ιδιότητα. Οι αξιολογήσεις ασφάλειας λογισμικού φαίνεται να μοιράζονται πολλά από τα χαρακτηριστικά αυτών των τύπων αξιολόγησης και θα μπορούσαν ενδεχομένως να επωφεληθούν από την προσαρμογή ορισμένων από τις παρακάτω τεχνικές [9].

2.6. Αξιολόγηση

Οι μετρήσεις ασφαλείας έχουν αποδειχθεί πολύ πιο επιτυχείς όταν ο στόχος της αξιολόγησης είναι μικρός και απλός παρά όταν ο στόχος είναι μεγάλος και σύνθετος. Για παράδειγμα, μια αξιολόγηση η οποία επικεντρώνεται αποκλειστικά στο Module κρυπτογράφησης ενός συστήματος, απαιτεί κατά κανόνα μικρότερο κόστος και χρόνο από την αξιολόγηση ασφάλειας κρυπτογράφησης του συνολικού συστήματος. Κάτι τέτοιο είναι απόλυτα λογικό αφού μεγαλύτερα συστήματα έχουν γενικά μεγαλύτερη πολυπλοκότητα και λειτουργικότητα. Καθώς ο αριθμός των συνιστωσών σε ένα σύστημα αυξάνεται, αυξάνεται και ο αριθμός των πιθανών αλληλεπιδράσεων με βάση το τετράγωνο του αριθμού των συνιστωσών [9].

Το πρόβλημα σύνθεσης στον τομέα της ασφάλειας είναι ένα μακροχρόνιο πρόβλημα. Δύο συστήματα, τα οποία κρίνονται ασφαλή, μπορεί αν συνδεθούν μεταξύ τους, το σύνθετο σύστημα που προκύπτει να μην είναι ασφαλές. Μια τεχνολογική επανάσταση στη διαδικασία σύνθεσης και σύνδεσης υποσυστημάτων θα ήταν να μπορούσε να προσφέρει ένα τρόπο έτσι ώστε οι μετρήσεις ασφάλειας των μικρών συστημάτων να συμβάλλουν άμεσα στις μετρήσεις ασφάλειας των μεγαλύτερων συστημάτων των οποίων αποτελούν μέρη. Η απουσία αξιόλογων μετρικών ασφάλειας υποσυστημάτων που μπορούν να χρησιμοποιηθούν για την αξιολόγηση της ασφάλειας σύνθετων συστημάτων, η τρέχουσα δυσκολία (από άποψη χρόνου και

Πανεπιστήμιο Πειραιώς

κόστους) στην αξιολόγηση μεγάλων και πολύπλοκων συστημάτων αναμένεται να συνεχιστεί [9].

2.7.Κατασκευή ενός προγράμματος μετρικών ασφαλείας

Για να διευκολυνθεί η κατανόηση σε όλα τα επίπεδα ενός νέου προγράμματος που χρησιμοποιεί μετρικές ασφαλείας, είναι σκόπιμο να σχεδιαστεί το πρόγραμμα με γνώμονα τις διαδικασίες και τις υποδομές που υπάρχουν ήδη στον οργανισμό.

Ανεξάρτητα όμως από τα χαρακτηριστικά του κάθε οργανισμού, θα μπορούσαν να χρησιμοποιηθούν τα παρακάτω βασικά βήματα για τον σχεδιασμό και την ανάπτυξη ενός προγράμματος μετρικών ασφάλειας [8]:

- Καθορισμός του στόχου του προγράμματος
- Επιλογή των μετρικών που θα παραχθούν
- Ανάπτυξη στρατηγικής για τη δημιουργία των μετρικών
- Δημιουργία πειραμάτων-δοκιμών και στόχων (benchmarking)
- Καθορισμός του τρόπου αναφοράς των μετρήσεων (reporting)

Τα βήματα της παραπάνω μεθοδολογίας περιγράφονται στη συνέχεια:

Βήμα 1ο: Καθορισμός του στόχου του προγράμματος

Επειδή η ανάπτυξη και η συντήρηση ενός προγράμματος μετρικών ασφάλειας θα μπορούσε να χρειάζεται σημαντική προσπάθεια και να εκτρέψει πόρους από άλλες δραστηριότητες ασφάλειας, είναι σημαντικό οι στόχοι του

Πανεπιστήμιο Πειραιώς

προγράμματος να είναι επαρκώς καθορισμένοι και συμφωνημένοι εκ των προτέρων.

Αν και δεν υπάρχει κανένας αυστηρός κανόνας για αυτό, μια καλή προσέγγιση είναι να αναφερθεί ο τρόπος με τον οποίο πρέπει να επικεντρωθούν όλες οι προσπάθειες συγκέντρωσης μετρήσεων και μετρικών.

Μια τέτοια δήλωση στόχου θα μπορούσε να είναι, για παράδειγμα: Η παροχή μετρικών που απλά και με σαφήνεια περιγράφουν πόσο αποτελεσματικά και αποδοτικά η εταιρεία εξισορροπεί ανάμεσα σε προβλήματα ασφαλείας και προληπτικά μέτρα, έτσι ώστε οι επενδύσεις στο πρόγραμμα ασφάλειάς να είναι κατάλληλου μεγέθους και να στοχεύουν στην επίτευξη των γενικών στόχων ασφάλειας της εταιρίας [8].

Οι δηλώσεις των στόχων θα πρέπει να αναφέρονται σε υψηλού επιπέδου δράσεις που πρέπει να ολοκληρωθούν συλλογικά, έτσι ώστε να επιτευχθούν οι προκαθορισμένοι στόχοι. Το σχέδιο δράσης πρέπει να απορρέει άμεσα από τις δηλώσεις αυτές.

Βήμα 2ο: Επιλογή των μετρικών που θα παραχθούν

Σε περίπτωση ύπαρξης υποκείμενου εταιρικού πλαισίου, όπως συζητήθηκε και στην αρχή αυτής της ενότητας, οι μετρικές που θα χρησιμοποιηθούν, προκύπτουν από το ίδιο το εταιρικό πλαίσιο.

Ελλείψει προϋπάρχοντος πλαισίου, μπορεί να χρησιμοποιήσει είτε μια top-down είτε μια bottom-up προσέγγιση για τον προσδιορισμό των μετρικών.

Η top-down προσέγγιση, ξεκινά με τους στόχους του προγράμματος ασφάλειας, και στη συνέχεια λειτουργεί προς τα κάτω για να προσδιορίσει συγκεκριμένες μετρικές που θα μπορούσαν να βοηθήσουν στον καθορισμό του κατά πόσο οι εν λόγω στόχοι επιτυγχάνονται, και τελικά να

Πανεπιστήμιο Πειραιώς

προσδιοριστούν οι μετρήσεις που απαιτούνται για την παραγωγή αυτών των μετρικών.

Ακολουθεί ένα παράδειγμα [8]:

TOP-DOWN APPROACH	
a. Define/list objectives of the overall security program	Example objective: *To reduce the number of virus infections within the company by 30% by 2002*
b. Identify metrics that would indicate progress toward each objective	Example metric: *Current ratio of virus alerts to actual infections as compared to the baseline 2000 figure*
c. Determine measurements needed for each metric	Example measurement: *Number of virus alerts issued to the organization by month* Example measurement: *Number of virus infections reported*

Πίνακας 1: Μέθοδος Top-Down

Η bottom-up προσέγγιση, πρέπει καταρχήν να καθορίζει ποιες διεργασίες ασφάλειας, προϊόντα, υπηρεσίες, κλπ. μπορούν να μετρηθούν ή έχουν ήδη μετρηθεί. Στη συνέχεια εξετάζει ποιες σημαντικές μετρικές θα μπορούσαν να προκύψουν από αυτές τις μετρήσεις και τελικά αξιολογεί πόσο καλά οι μετρικές αυτές σχετίζονται με τους στόχους του συνολικού προγράμματος ασφαλείας.

Ακολουθεί ένα παράδειγμα [8]:

BOTTOM-UP APPROACH	
a. Identify measurements that are/could be collected for this process	Example measurement: *Average number of Level 1 vulnerabilities detected per server by department using our xyz scanning tool*
b. Determine metrics that could be generated from the measurements	Example metric: *Change in number of critical vulnerabilities detected on servers by department since last reporting period*
c. Determine the association between the derived metrics and established objectives of the overall security program	Example objective: *To reduce the level of detectable vulnerabilities on servers in every department within the company.*

Πίνακας 2: Μέθοδος Bottom-Up

Η top-down προσέγγιση θα εντοπίσει πιο εύκολα τις μετρικές που θα πρέπει να χρησιμοποιηθούν λαμβάνοντας υπόψη τους στόχους του συνολικού προγράμματος για την ασφάλεια, ενώ η bottom-up προσέγγιση παράγει τις πιο εφικτές μετρήσεις. Και οι δύο προσεγγίσεις προϋποθέτουν πως έχουν καθοριστεί οι στόχοι του προγράμματος ασφάλειας.

Βήμα 3ο: Ανάπτυξη στρατηγικής για τη δημιουργία των μετρικών

Στο βήμα αυτό, οι μετρήσεις που πρέπει να γίνουν έχουν ήδη καθοριστεί, συνεπώς πρέπει να αναπτυχθούν οι στρατηγικές που απαιτούνται για τη συλλογή δεδομένων και την εξαγωγή των μετρήσεων. Οι στρατηγικές αυτές θα πρέπει να προσδιορίζουν την πηγή των δεδομένων καθώς και την συχνότητα συλλογής δεδομένων, και να ορίζουν ποίος είναι ο υπεύθυνος για την ακρίβεια των μη επεξεργασμένων δεδομένων, τη συλλογή τους σε μετρήσεις, και την παραγωγή του μετρικού.

Αν και μια τυπική αξιολόγηση του κινδύνου είναι μία μέθοδος για τη συλλογή μερικών από τα δεδομένα που ενδέχεται να χρειαστούν, οι ειδικοί διαφωνούν σχετικά με την αξία της για τη δημιουργία μετρικών. Υπάρχουν, ωστόσο, άλλες προτεινόμενες πηγές δεδομένων, όπως αρχεία καταγραφής του help desk, τα αρχεία καταγραφής του συστήματος, των firewall, καθώς και ερευνών μεταξύ των χρηστών.

Αρχικά υπήρχαν λίγα αυτοματοποιημένα εργαλεία διαθέσιμα για τη συλλογή δεδομένων, την ανάλυση και την παραγωγή εκθέσεων (reporting), αλλά τα τελευταία χρόνια έχουν εισαχθεί στην αγορά προϊόντα που καθιστούν αυτές τις δραστηριότητες ευκολότερες.

Πανεπιστήμιο Πειραιώς

Βήμα 4ο: Δημιουργία πειραμάτων-δοκιμών και στόχων (benchmarking)

Benchmarking (συγκριτική αξιολόγηση) είναι η διαδικασία σύγκρισης, της απόδοσης των πρακτικών ενός οργανισμού με αντίστοιχους οργανισμούς του κλάδου ή με γνωστές «βέλτιστες πρακτικές».

Η διαδικασία αυτή παρέχει νέες ιδέες για τη διαχείριση μιας δραστηριότητας. Επίσης μπορεί να οδηγήσει στην παροχή συγκριτικών δεδομένων που απαιτούνται για να παραχθούν μετρικές με περισσότερο νόημα. Η συγκριτική αξιολόγηση μπορεί να συμβάλει στη δημιουργία εφικτών στόχων για την παροχή βελτιώσεων στις υπάρχουσες πρακτικές.

Βήμα 5ο: Καθορισμός του τρόπου αναφοράς των μετρήσεων (reporting)

Προφανώς, αν δεν υπάρχει αξιόλογος τρόπος εμφάνισης και παροχής των μετρικών ασφαλείας δεν έχει νόημα όλη η προηγούμενη διαδικασία. Η υπάρχουσα βιβλιογραφία στις μετρικές ασφάλειας δεν παρέχει κάποια ιδιαίτερη καθοδήγηση σε αυτόν τον τομέα. Ένας αναλυτής [20] , προειδοποιεί ότι η υπερβολική απλούστευση, για λόγους σαφήνειας, είναι λανθασμένη πρακτική. Τα στελέχη έχουν συνηθίσει να ασχολούνται με την οικονομική πλευρά, συνεπώς, περίπλοκα δεδομένα που αφορούν την ασφάλεια μπορεί να τους φανούν ιδιαίτερα χρήσιμα, αν παρουσιαστούν καλά. Οι γραφικές αναπαραστάσεις είναι επίσης ιδιαίτερα αποδοτικές.

Μερικές μετρικές μπορεί να είναι ουσιαστικά μόνο για το διευθυντή και το προσωπικό ασφαλείας και δεν θα πρέπει να δοθούν σε τρίτους. Οι διαχειριστές ασφάλειας μπορούν, ωστόσο, να χρησιμοποιήσουν άλλες μετρικές προκειμένου να προκαλέσουν διορθωτικές ενέργειες μέσα στην

Πανεπιστήμιο Πειραιώς

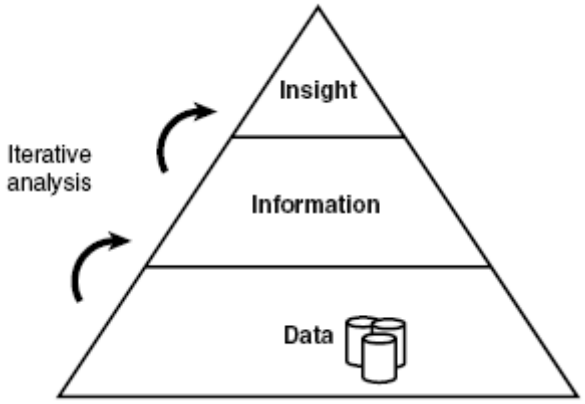
οργάνωση. Για παράδειγμα, μια μετρική που δείχνει τα επίπεδα ευπάθειας ασφάλειας για κάθε τμήμα σε ένα οργανισμό, θα μπορούσε να προκαλέσει υγιή ανταγωνισμό μεταξύ των τμημάτων και τελικά να βελτιωθεί η συνολική ασφάλεια του οργανισμού.

Σε κάθε περίπτωση, το πλαίσιο, η μορφή, η συχνότητα, η μέθοδος διανομής και η ευθύνη για την παροχή αναφορών σχετικά με τις μετρικές ασφάλειας πρέπει να καθοριστούν εκ των προτέρων, έτσι ώστε το τελικό προϊόν να μπορεί να απεικονιστεί έγκαιρα και να εγκριθεί από εκείνους που θα συμμετάσχουν στην παραγωγή των μετρικών και εκείνους οι οποίοι θα το χρησιμοποιούν για τη λήψη αποφάσεων.

Πανεπιστήμιο Πειραιώς

3. Τεχνικές Ανάλυσης Μετρικών Ασφάλειας

Οι οργανισμοί που προσπαθούν να μετρήσουν τις διαδικασίες ασφάλειας τους, μπορούν να αντλήσουν πληροφορίες από πολλές πιθανές πηγές δεδομένων, συμπεριλαμβανομένων των συστημάτων, των ανθρώπων, και των διαδικασιών ελέγχου. Σε όλες σχεδόν τις περιπτώσεις, οι αναλυτές χρειάζονται να φιλτράρουν, να ταξινομούν, να αναλύουν, ή να μετατρέπουν τα δεδομένα έτσι ώστε αυτά να εμφανίζονται σε μια χρήσιμη μορφή. Στην ενότητα αυτή θα παρουσιαστούν διάφορες τεχνικές επεξεργασίας και ανάλυσης δεδομένων, που χρησιμοποιούνται στις μετρικές ασφάλειας.



Εικόνα 1: Διαδικασία συλλογής πληροφοριών

Στο παραπάνω σχήμα φαίνεται χαρακτηριστικά η πυραμίδα που περιγράφει τη διαδικασία συλλογής των δεδομένων, την εξαγωγή της πληροφορίας και τελικά την απόκτηση της γνώσης για την κατάσταση του συστήματος.

Πανεπιστήμιο Πειραιώς

Παρακάτω θα περιγραφούν διάφορες κοινές τεχνικές για την ανάλυση δεδομένων ασφαλείας [19]:

- Μέσος όρος (αριθμητικός μέσος όρος)
- Διάμεσος
- Τυπική απόκλιση
- Ομαδοποίηση και συνάθροιση
- Ανάλυση Χρονοσειρών
- Συγχρονική ανάλυση
- Ανάλυση ανά τεταρτημόριο
- Πίνακες συνδιακύμανσης

Στη συνέχεια θα γίνει περιγραφή βασικών εννοιών της κάθε τεχνικής: τι σημαίνουν και πώς κατασκευάζονται. Οι τεχνικές τους είναι γενικού χαρακτήρα και δεν αφορούν μονάχα την ασφάλεια.

3.1.Μέσος Όρος

Ο μέσος όρος στηρίζει τον πυρήνα βασικών στατιστικών εννοιών, όπως η τυπική απόκλιση, η διακύμανση και η συσχέτιση.

Ο μέσος όρος συνήθως δεν είναι αποδεκτός για τη δημιουργία μετρικών από δεδομένα με μεγάλη διακύμανση καθώς:

- αποκρύπτει την πιθανή ποικιλία των αρχικών δεδομένων

Πανεπιστήμιο Πειραιώς

- δίνει εσφαλμένη εντύπωση για το ποια είναι η τυπική τιμή σε μια σειρά δεδομένων.

Ο αριθμητικός μέσος είναι αποδεκτός σε ορισμένες περιπτώσεις, όταν το πεδίο των δεδομένων που εκπροσωπούνται από το μέσο όρο είναι περιορισμένο. Για παράδειγμα, η συγχρονική ανάλυση (η οποία θα συζητηθεί αργότερα σε αυτό το κεφάλαιο) αθροίζει κάθε υποσύνολο δεδομένων με τη χρήση αριθμητικών μέσων. Είναι πολύ πιο λογικό και πολύ πιο ενδιαφέρον, να γίνεται σύγκριση των μέσων δαπανών για μικρές, μεσαίες και μεγάλες επενδυτικές τράπεζες (και εμπορικές τράπεζες, ασφαλιστικές εταιρείες και εταιρείες πιστωτικών καρτών) αντί για σύγκριση των απόλυτων τιμών.

3.2. Διάμεσος

Όπως αναφέρθηκε, οι περισσότεροι αναλυτές χρησιμοποιούν αριθμητικούς μέσους προκειμένου να χαρακτηρίσουν κάτι ως "τυπικό". Σε πολλές περιπτώσεις, η χρήση της διάμεσου είναι καλύτερη από τη χρήση του μέσου όρου. Η διάμεσος βοηθάει στην άθροιση των συνόλων δεδομένων σε μικρότερα σύνολα, συνοψίζοντας μια σειρά/εύρος από εγγραφές. Ωστόσο, η διάμεσος προσφέρει μεγαλύτερη γνώση για τη κατανομή των δεδομένων, ιδίως εάν οι ακραίες τιμές, τα δύο άκρα του συνόλου, των δεδομένων παραποιούν το μέσο όρο.

Για παράδειγμα, έστω ένα εργαλείο ελέγχου κωδικών ασφαλείας (password-auditing tool), το οποίο καθορίζει τον αριθμό των δευτερολέπτων που απαιτούνται για να σπάσει ο κωδικός πρόσβασης στο λογαριασμού του χρήστη. Έστω ότι μερικοί χρήστες με μεγαλύτερη επίγνωση της ασφάλειας επιλέγουν κωδικούς πρόσβασης τους οποίους δύσκολα μπορεί να τους μαντέψει κανείς. Ο χρόνος που απαιτείται για να σπάσουν αυτοί οι κωδικοί

Πανεπιστήμιο Πειραιώς

ενδέχεται να είναι τεράστιος, με αποτέλεσμα να αυξάνεται ο μέσος όρος σημαντικά. Η χρήση της διάμεσου αντί του μέσου όρου προσφέρει καλύτερη εικόνα για το πόσο αποτελεσματικοί είναι οι κωδικοί πρόσβασης των χρηστών, επειδή προσδιορίζει πόσο χρόνο χρειάστηκε προκειμένου να σπάσει κάθε ένας από τους μισούς πιο αδύνατους κωδικούς.

Συμπερασματικά, οι διάμεσοι προσφέρουν σημαντικά πλεονεκτήματα σε σχέση με τους μέσους όρους, ιδίως όσον αφορά τη μέτρηση των επιδόσεων.

3.3. Τυπική Απόκλιση

Η τυπική απόκλιση μετράει το βαθμό της στατιστικής διασποράς ενός συνόλου δεδομένων από τον μέσο όρο. Όσο μικρότερη είναι η τυπική απόκλιση, τόσο μεγαλύτερος είναι ο βαθμός ομαδοποίησης. Μεγάλες τυπικές αποκλίσεις υποδηλώνουν ότι τα δεδομένα μπορεί να είναι πολύ ασύμμετρα ή απρόβλεπτα. Ακριβώς επειδή δίνει στοιχεία για την «ομαλότητα» των δεδομένων, πρέπει να χρησιμοποιείται μαζί με τον μέσο όρο.

3.4. Ομαδοποίηση και Συνάθροιση

Όπως αναφέρθηκε και στην αρχή του κεφαλαίου, οι μετρικές απαιτούν τη μετατροπή του μεγάλου αριθμού πρωτογενών δεδομένων σε χρήσιμες πληροφορίες. Υπάρχουν δύο αρχικές μέθοδοι οι οποίες περιλαμβάνουν την ομαδοποίηση (τοποθέτηση παρόμοιων εγγραφών μαζί) και τη συνάθροιση (υπολογισμός συνοπτικών στατιστικών στοιχείων για κάθε ομάδα). Για αυτές τις μεθόδους θα γίνει αναφορά στη συνέχεια, αλλά πρώτα θα διευκρινιστούν μερικοί όροι.

Πανεπιστήμιο Πειραιώς

3.4.1. Εγγραφές και ιδιότητες

Έστω ότι οποιαδήποτε διαδικασία ή πηγή δεδομένων στο πλαίσιο της ανάλυσης έχει μια σειρά από χαρακτηριστικά που αξίζει να μετρηθούν. Μία μόνο παρατήρηση αυτής της διαδικασίας που συλλαμβάνει όλα τα επιθυμητά χαρακτηριστικά (συμπεριλαμβανομένης και της ημερομηνίας της παρατήρησης) αποτελεί μια εγγραφή. Σε γενικές γραμμές, οι περισσότερες εγγραφές ενσωματώνουν ένα γεγονός που αφορά την ασφάλειας ή την έλλειψη της, όπως για παράδειγμα μια ευπάθεια, η παραβίαση προσωπικών δεδομένων, ή η ανίχνευση ενός ιού.

3.4.2. Ομαδοποίηση

Μετά τη συλλογή των στοιχείων για τις επιθυμητές περιόδους παρατήρησης, το πρώτο βήμα περιλαμβάνει την επιλογή του τρόπου ομαδοποίησης των εγγραφών. Συνήθως στο τομέα της ασφάλειας, η έννοια της ομαδοποίησης αφορά την τοποθέτηση μαζί, όλων εκείνων των εγγραφών οι οποίες έχουν κοινό ενδιαφέρον από άποψη ασφάλειας, όπως για παράδειγμα αφορούν το ίδιο τμήμα μιας επιχείρησης.

Οι ομάδες θα πρέπει να περιλαμβάνουν όλα τα χαρακτηριστικά που θα μπορούσαν να χρησιμεύσουν ως μονάδες μέτρησης. Επίσης, η ομαδοποίηση γίνεται πολλές φορές «ανά περίοδο», εκτός από «ανά εφαρμογή», προκειμένου να είναι ευκολότερη η ανάλυσή των δεδομένων ως χρονοσειρές.

Πανεπιστήμιο Πειραιώς

3.4.3. Συνάθροιση

Μόλις οι αναλυτές ομαδοποιήσουν τις εγγραφές, το επόμενο βήμα είναι η συνάθροιση: δηλαδή η ενοποίηση των εγγραφών σε συνοπτικά στατιστικά στοιχεία για κάθε ομάδα. Όταν δημιουργεί κανείς μια "στατιστική περίληψη," για όλες τις εγγραφές σε κάθε ομάδα τότε εκτελούνται μία ή περισσότερες από τις ακόλουθες ενέργειες για κάθε χαρακτηριστικό:

- Άθροισμα
- Μέσος όρος/ Διάμεσος
- Τυπική απόκλιση
- Υψηλότερη τιμή
- Χαμηλότερη τιμή
- Πλήθος

Στις περισσότερες περιπτώσεις, ο συνυπολογισμός τυπικά περιλαμβάνει τη σύνοψη ή το μέσο όρο αριθμητικών χαρακτηριστικών και το πλήθος για αυτά που δεν είναι αριθμητικά. Αυτό μας επιτρέπει να μειωθεί ο αριθμός των εγγραφών, διατηρώντας παράλληλα πολύτιμες πληροφορίες για κάθε ομάδα.

Μια σημαντική ερώτηση είναι πως μπορεί να μάθει κανείς αν έχει ομαδοποιήσει και αθροίσει σωστά τα δεδομένα του. Ένας καλός εμπειρικός κανόνας είναι να εξετάσει τα μη αριθμητικά χαρακτηριστικά . Ο συνδυασμός δυο οποιονδήποτε εγγραφών θα ανάγκαζε τον αναλυτή να συγχωνεύσει ή να απορρίψει κάποιο από αυτά τα χαρακτηριστικά (επειδή δεν μπορούν να συνοψιστούν ή να προσμετρηθούν); Αν ναι, θα πρέπει να λάβει υπ' όψιν του

Πανεπιστήμιο Πειραιώς

και την ομαδοποίηση των μη αριθμητικών χαρακτηριστικών. Εάν, μετά την εξέταση, αντιληφθεί ότι δεν χρειάζεται τις υποομάδες, πρέπει απλά να μετρήσει τον αριθμό των μοναδικών περιπτώσεων, ή απορρίψει το συγκεκριμένο χαρακτηριστικό.

3.5. Ανάλυση Χρονοσειρών

Η ανάλυση χρονοσειρών αναφέρεται στην τεχνική που έχει ως στόχο να περιγράψει πώς ένα σύνολο δεδομένων συμπεριφέρεται με την πάροδο του χρόνου. Πιο συγκεκριμένα, μια χρονολογική σειρά περιλαμβάνει μια σειρά από παρατηρήσεις για ένα συγκεκριμένο χαρακτηριστικό, το οποίο μετράται σε τακτά χρονικά διαστήματα. Η ανάλυση αναφέρεται στα βήματα που ακολουθούνται για τη μέτρηση των επιδόσεων σε αυτό το διάστημα.

Οι χρονοσειρές κατατάσσονται γενικά και ομαδοποιούνται σε ένα επιθυμητό χρονικό διάστημα, στο οποίο θα γίνει η ανάλυση. Το διάστημα πρέπει να είναι αρκετά ακριβές ώστε να παρέχει διορατικότητα, αλλά να μην είναι τόσο ακριβής ώστε η λεπτομέρεια να 'κουράσει' τον ενδιαφερόμενο. Για παράδειγμα, με σχετικά σπάνια εμφάνιση γεγονότων όπως τρύπες ασφαλείας σε μια εφαρμογή, έχει νόημα η μηνιαία ή η τριμηνιαία παρατήρηση.

Στην πραγματικότητα, οι περισσότερες μετρικές ασφαλείας δεν απαιτούν περισσότερη ακρίβεια από την προαναφερθείσα. Έτσι, το πρώτο βήμα περιλαμβάνει την ομαδοποίηση και τη συνάθροιση όλων των εγγραφών στο επιθυμητό χρονικό διάστημα περιόδου μήνα, τριμήνου ή έτους. Μετά την συγκέντρωση, ο αναλυτής ταξινομεί το αποτέλεσμα με βάση την ημερομηνία, κατά κανόνα σε αύξουσα σειρά, έτσι ώστε παλιότερες καταχωρήσεις να εμφανίζονται πρώτα.

Πανεπιστήμιο Πειραιώς

Η ανάλυση χρονοσειρών είναι ένα απαραίτητο εργαλείο του αναλυτή ασφαλείας καθώς είναι η βάση για άλλους τύπους ανάλυσης. Σε συνδυασμό με τη Συγχρονική ανάλυση και την Quartile ανάλυση, παρέχει τη βάση για συγκριτική αξιολόγηση (benchmarking).

3.6.Συγχρονική ανάλυση (Cross-sectional Analysis)

Αν με την ανάλυση χρονοσειρών προσπαθεί να καταλάβει κανείς πώς ένα χαρακτηριστικό διαφοροποιείται με την πάροδο του χρόνου, με την συγχρονική ανάλυση εξετάζει πώς τα δεδομένα διαφέρουν στη διατομή συγκρίσιμων παρατηρήσεων. Δηλαδή, είναι η διαδικασία κατά την οποία κόβει κανείς ένα κομμάτι από ένα σύνολο εγγραφών που έχουν ένα κοινό χαρακτηριστικό και στη συνέχεια εξετάζει τι συμβαίνει με τα υπόλοιπα χαρακτηριστικά.

Η συγχρονική ανάλυση περιλαμβάνει τρία στάδια. Πρώτον, ο αναλυτής επιλέγει ένα χαρακτηριστικό που θα χρησιμοποιηθεί για τη δημιουργία της διατομής. Συνήθως τα μη αριθμητικά χαρακτηριστικά, όπως οι κατηγορίες, είναι χαρακτηριστικά που ταιριάζουν στην ανάλυση αυτή. Μετά την επιλογή ενός κατάλληλου χαρακτηριστικού, ο αναλυτής ομαδοποιεί και συναθροίζει τα δεδομένα και τελικά προχωρά στην ανάλυσή τους.

Οι τεχνικές που βασίζονται στην ανάλυση αυτή παρέχουν ένα ισχυρό μέσο για τη σύγκριση της αποτελεσματικότητα της ασφάλειας ενός οργανισμού. Για παράδειγμα, ας υποθέσουμε ότι ένα δείγμα δεδομένων περιέχει ένα χαρακτηριστικό όπου ταξινομεί κάθε ελάττωμα ασφαλείας (όπως ο έλεγχος ταυτότητας, κρυπτογράφησης και επικύρωσης χρήστη εισόδου). Μια συγχρονική ανάλυση θα μπορούσε να συγκρίνει τη συχνότητα εμφάνισης των συμβάντων ανά υπηρεσία για κάθε τύπο ευπάθειας. Οι υπεύθυνοι για την ασφάλεια του οργανισμού θα μπορούσαν να

Πανεπιστήμιο Πειραιώς

χρησιμοποιήσουν τη γνώση των «προβληματικών σημείων» για την καλύτερη κατάρτιση των χρηστών.

3.7. Ανάλυση ανά τεταρτημόριο (Quartile Analysis)

Από όλες τις τεχνικές που περιγράφονται σε αυτό το κεφάλαιο, η ανάλυση ανά τεταρτημόριο μπορεί να είναι η πιο ισχυρή. Πρόκειται για μια παλιά τεχνική συμβούλων σε θέματα διαχείρισης. Η ανάλυση ανά τεταρτημόριο μοιράζεται πολλά κοινά χαρακτηριστικά με τη συγχρονική ανάλυση. Οι δύο τεχνικές, απαιτούν ο αναλυτής να επιλέξει μια συλλογή χαρακτηριστικών γνωρισμάτων προς εξέταση. Και στις δύο τεχνικές, ο αναλυτής πρέπει να προσδιορίσει την κατάλληλη ομαδοποίηση και τη στρατηγική συνάθροισης. Και τέλος, και στις δύο περιπτώσεις η γνώση πηγάζει άμεσα από τις αντιθέσεις που αποκαλύφθηκαν από τις συγκρίσεις χαρακτηριστικό-προς-χαρακτηριστικό.

Σε αντίθεση με μια καθαρή συγχρονική ανάλυση, η οποία λαμβάνει υπόψη όλες τις εγγραφές στο συναθροισμένο σύνολο αποτελεσμάτων, η ανάλυση ανά τεταρτημόριο έχει ένα επιπλέον βήμα: για κάθε χαρακτηριστικό με βάση την επιθυμητή σειρά ταξινόμησης, κατατάσσει τα αποτελέσματα σε τέσσερις «κάδους» ή τεταρτημόρια (εξ ου και το όνομα). Το πρώτο τεταρτημόριο αντιπροσωπεύει το καλύτερο 25% των αποτελεσμάτων, το δεύτερο τεταρτημόριο «κόβει» τα αποτελέσματα στο 50%, και το τρίτο τεταρτημόριο αποκόπτει την κορυφή του 75%. Το τέταρτο τεταρτημόριο αντιπροσωπεύει το χειρότερο 25% του συνόλου των αποτελεσμάτων. Συνήθως για την εξαγωγή των ποσοστών χρησιμοποιείται η διάμεσος αντί του μέσου όρου.

Πανεπιστήμιο Πειραιώς

Με την κατάταξη κάθε χαρακτηριστικού σε τεταρτημόρια, ο αναλυτής αποκτά μια ευρεία αντίληψη για τη κατάταξη κάθε εγγραφής: σε ποιο τεταρτημόριο εμπίπτει (καλύτερο, το χειρότερο, ή κάπου στο ενδιάμεσα).

3.8.Πίνακες συσχέτισης

Μέχρι στιγμής, οι μέθοδοι που παρουσιάζονται σε αυτό το κεφάλαιο έχουν επικεντρωθεί στη μείωση, τη συνάθροιση, την ομαδοποίηση και τη σύνοψη μεγάλων συνόλων δεδομένων σε μικρότερα, με στόχο την απόκτηση διορατικότητας στη διαχείριση. Μερικές από τις τελευταίες τεχνικές, ιδιαίτερα η ανάλυση ανά τεταρτημόριο, βοηθά τους αναλυτές να κατανοήσουν τις «σιωπηρές» σχέσεις μεταξύ χαρακτηριστικών, δηλαδή το πώς κάποιο χαρακτηριστικό επηρεάζει τα υπόλοιπα. Ωστόσο, οι τεχνικές αυτές δεν παρέχουν πληροφορία σχετικά με τις σχέσεις μεταξύ των χαρακτηριστικών. Για παράδειγμα, η εμφάνιση υψηλότερου ρυθμού ευπαθειών ασφαλείας στο λογισμικό σχετίζεται με την ποσότητα του χρόνου που δαπανάται κατά την αξιολόγηση του κώδικα.

Γνωρίζοντας πόσο καλά συσχετίζονται δύο σύνολα δεδομένων, κατανοείτε καλύτερα η σχέση ανάμεσα σε δύο χαρακτηριστικά. Τα χαρακτηριστικά ασφαλείας, ωστόσο, δεν έχει νόημα να ελέγχονται μόνο ανά ζεύγη. Οι περισσότεροι αναλυτές θέλουν να διερευνήσουν τις σχέσεις μεταξύ περισσότερων από ένα ζευγάρι χαρακτηριστικών, ανά πάσα στιγμή. Για το λόγο αυτό χρησιμοποιούν τους πίνακες συνδιακύμανσης. Η στατιστική έννοια της συνδιακύμανσης παραπέμπει στη τάση ενός συνόλου τιμών να κινηθεί με την ίδια ή προς την αντίθετη κατεύθυνση ενός άλλου συνόλου. Η συνδιακύμανση είναι μεγάλη και θετική, όταν δύο μεταβλητές κινούνται προς την ίδια κατεύθυνση (και τα δύο αυξάνονται ή μειώνονται). Όταν από την άλλη δυο μεταβλητές κινούνται προς κατεύθυνση αντίθετη τότε η

Πανεπιστήμιο Πειραιώς

συνδιακύμανση είναι μεγάλη και αρνητική. Όταν δεν υπάρχει κάποια σχέση, η συνδιακύμανση είναι μικρή, με τιμή κοντα στο 0.

Οι πίνακες συνδιακύμανσης παρέχουν ένα διαρθρωμένο και γρήγορο τρόπο για την ανάλυση πολλών ζευγαριών χαρακτηριστικών ταυτόχρονα. Οι πίνακες συνδιακύμανσης βοηθούν τους αναλυτές να κατανοήσουν ποιες μεταβλητές τείνουν να κινούνται μαζί, χωρίς να χρειάζεται να γνωρίζουν εκ των προτέρων ποια ζεύγη πρέπει να ελέγξουν.

Πανεπιστήμιο Πειραιώς

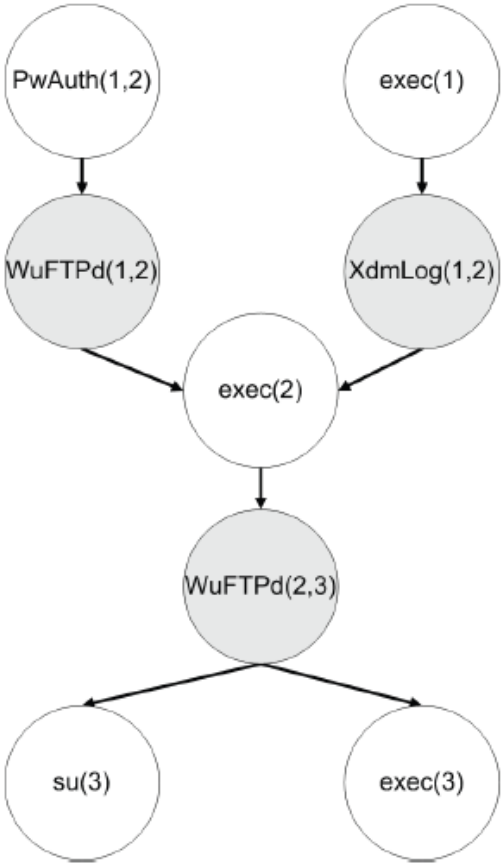
4. Χρήση Μετρικών ασφαλείας

Στο κεφάλαιο αυτό θα παρουσιαστούν διάφορες προτάσεις για την χρήση μετρικών ασφαλείας από τη βιβλιογραφία.

4.1. Μετρικές ασφάλειας που βασίζονται σε γράφημα επίθεσης

Στο [21] γίνεται η χρήση μετρικών ασφαλείας που βασίζονται στο γράφημα επίθεσης. Το γράφημα επίθεσης είναι μια αφηρημένη έννοια που αποκαλύπτει τους τρόπους με τους οποίους ένας εισβολέας μπορεί να ανακαλύψει τρωτά σημεία σε ένα δίκτυο και να καταφέρει να παραβιάσει την πολιτικής ασφάλειας. Σε συνδυασμό με κατάλληλές μετρικές ασφάλειας, το γράφημα επίθεσης μπορεί να χρησιμοποιηθεί για να εκτιμηθεί ποσοτικά η κατάσταση ασφάλειας του δικτύου.

Πανεπιστήμιο Πειραιώς



Εικόνα 2: Γράφημα επίθεσης

Η μετρική συντομότερης διαδρομής, ο αριθμός των μονοπατιών, και η μέση τιμή του μήκους της διαδρομής είναι τρία μετρικά που μπορούν να εξάγουν πληροφορία σχετική με την ασφάλεια.

Για παράδειγμα, η μετρική συντομότερης διαδρομής αναπαριστά το μήκος του μικρότερου μονοπατιού επίθεσης. Η μικρότερη διαδρομή επίθεσης είναι η μικρότερη απόσταση από την αρχική κατάσταση ενός επιτιθέμενου μέχρι την επιθυμητή κατάσταση (δηλαδή την παραβίαση της ασφάλειας του δικτύου και την απόκτηση πρόσβασης σε κάποιο σύστημα). Η συνάρτηση μήκους που καθορίζει την απόσταση, εξαρτάται από τον μηχανικό ασφάλειας που κάνει την ανάλυση του γραφήματος επίθεσης. Το μήκος σε

ένα μονοπάτι επίθεσης μπορεί να είναι ο αριθμός των βημάτων (security exploits) που πρέπει να κάνει ο επιτιθέμενος προκειμένου να πετύχει τον στόχο του.

Ωστόσο, η χρήση κάποιου από αυτά τα μετρικά συστήματα μπορεί να οδηγήσει σε παραπλανητικά αποτελέσματα. Για παράδειγμα, η μετρική συντομότερης διαδρομής δε λαμβάνει επαρκώς υπόψη τον αριθμό των τρόπων με τους οποίους ένας εισβολέας μπορεί να παραβιάσει την πολιτική ασφάλειας. Για το λόγο αυτό προτείνεται η συνδυασμένη χρήση αυτών των μετρικών ασφαλείας.

4.2.Μετρικές ασφάλειας για τη διαχείριση αναβαθμίσεων

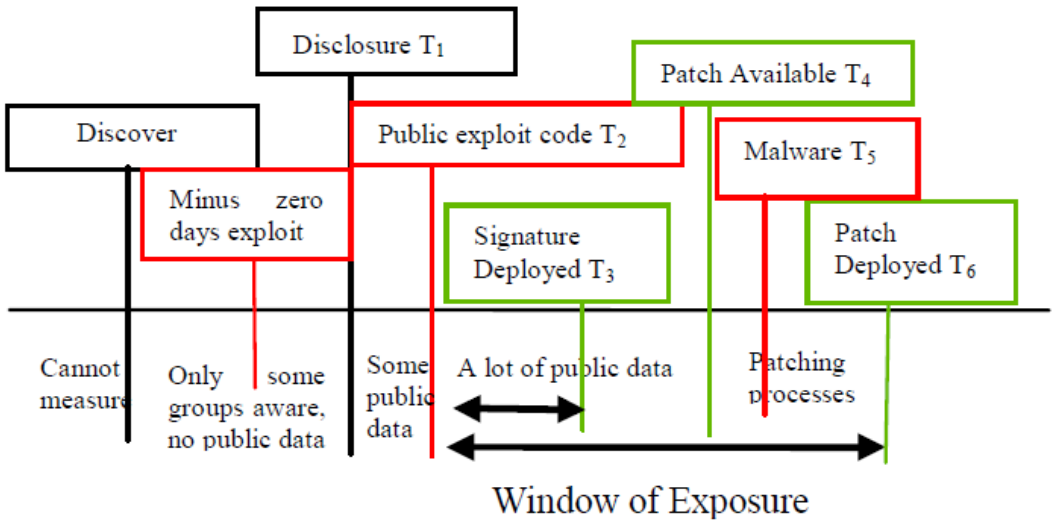
Στη δημοσίευση [22] παρουσιάζεται ένα case study συνδυασμού μετρικών ασφάλειας με μοντελοποίηση για την εξαγωγή προβλέψεων, το οποίο δείχνει πώς πολλαπλές μετρικές μπορούν να χρησιμοποιηθούν για να αξιολογήσει κανείς την αποτελεσματικότητα της τρέχουσας διεργασίας ασφάλειας.

Οι έλεγχοι ασφαλείας που συνήθως χρησιμοποιούνται για την αντιμετώπιση των ευπαθειών λογισμικού και των σχετικών απειλών, όπως κακόβουλο λογισμικό και ιοί, περιλαμβάνουν τη διαχείριση αναβαθμίσεων, το λογισμικό προστασίας από ιούς, καθώς και συστήματα πρόληψης εισβολής (Intrusion Prevention Systems), με την κύρια πρόληψη να είναι οι αναβαθμίσεις. Συνήθως, ειδικά σε ένα μεγάλο οργανισμό, χιλιάδες συστήματα που χρησιμοποιούν δημοφιλή λειτουργικά συστήματα, όπως Windows μπορεί ενδεχομένως να απαιτούν συχνή εγκατάσταση αναβαθμίσεων ασφαλείας (security patches). Η έγκαιρη εγκατάσταση των αναβαθμίσεων σε όλα αυτά τα συστήματα δεν είναι απλή. Οι διαχειριστές αντιμετωπίζουν συχνά περιορισμούς στην εισαγωγή και εγκατάσταση των

Πανεπιστήμιο Πειραιώς

αναβαθμίσεων από τις απαιτήσεις των επιχειρήσεων όσον αφορά τον περιορισμό του downtime των συστημάτων ή τη χρήση παλιών εφαρμογών που αναγκάζουν τη χρήση παλιότερων και λιγότερο ασφαλών λειτουργικών συστημάτων.

Για την κατασκευή του μοντέλου του συστήματος για τη διαδικασία διαχείρισης αναβαθμίσεων, πρέπει πρώτα να εξεταστεί η «vulnerability time line» για τον εντοπισμό τους. Το παρακάτω σχήμα δείχνει ένα χρονοδιάγραμμα γεγονότων του κύκλου ζωής μιας τυπικής ευπάθειας.



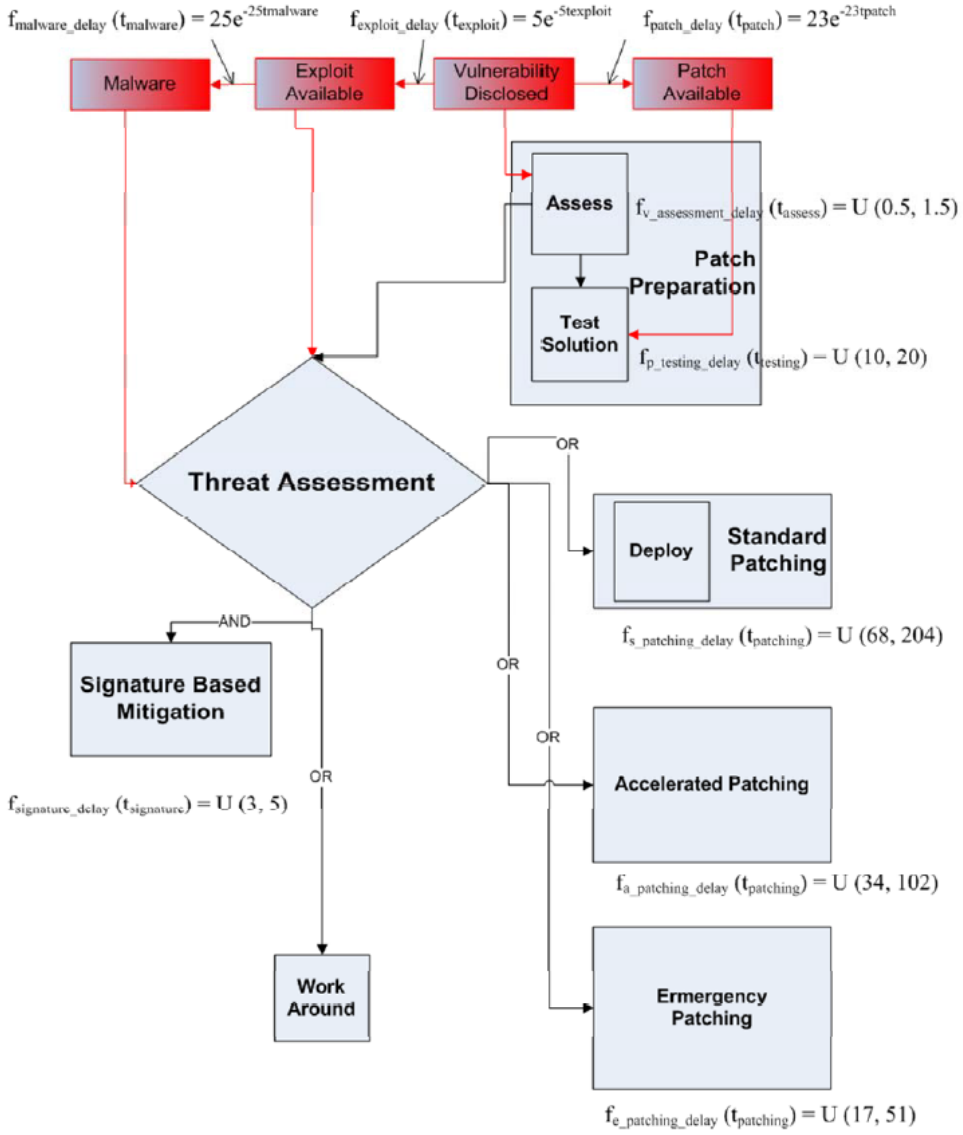
Εικόνα 3: Χρονοδιάγραμμα γεγονότων

Μέσα σε αυτό το χρονοδιάγραμμα το κύριο μέγεθος που δείχνει πόσο καλές είναι οι διαδικασίες αναβάθμισης που αφορούν στην ελαχιστοποίηση της έκθεσης του συστήματος σε ευπάθειες είναι ο χρόνος που απαιτείται από τους διαχειριστές είτε (α) για την εγκατάσταση των

αναβαθμίσεων είτε (β) για την ανάπτυξη κατάλληλων αντιμέτρων μετά την ανακάλυψη κάποιας ευπάθειας. Αυτό συμβολίζεται ως το παράθυρο της έκθεσης στο χρονοδιάγραμμα στο παραπάνω σχήμα. Όσο μεγαλύτερο είναι αυτό το παράθυρο, τόσο περισσότερο ο οργανισμός είναι εκτεθειμένος σε πιθανές επιθέσεις.

Για την αξιολόγηση των διαδικασιών ασφαλείας του οργανισμού και για τη διερεύνηση των αποτελεσμάτων για τις επιλεγμένες μετρικές, οι ερευνητές προτείνουν ένα μοντέλο για τις διαδικασίες αυτές, σε συνδυασμό με τα χαρακτηριστικά των εξωτερικών απειλών. Στο μοντέλο περιγράφονται οι ρυθμοί με τους οποίους εμφανίζονται νέες ευπάθειες, παράγονται αναβαθμίσεις, και εμφανίζεται κακόβουλο λογισμικό με βάση τις δημόσιες εκθέσεις για νέες απειλές. Παράλληλα, στο μοντέλο αυτό περιγράφονται οι αποφάσεις για τη διαχείριση των ευπαθειών, τα χρονοδιαγράμματα και οι διαδικασίες στο εσωτερικό του οργανισμού.

Πανεπιστήμιο Πειραιώς



Εικόνα 4: Μοντέλο για την αξιολόγηση των διαδικασιών ασφάλειας

Μια πιο λεπτομερή περιγραφή αυτού του μοντέλου μπορεί να βρεθεί στη δημοσίευση [23].

4.3. Μετρικές ασφάλειας για τη διαχείριση χρηστών

Στη συνέχεια θα παρουσιαστεί ένα διαφορετικό case study. Οι λύσεις δαιχείρισης ταυτότητας και πρόσβασης (Identity and Access Management - IAM) για τις επιχειρήσεις έχουν αντίκτυπο σε πολλές πτυχές της πληροφορικής και αφορούν την ταυτοποίηση (authentication), διαδικασίες single-sign-on (SSO), την εξουσιοδότηση (authorization) , τον έλεγχο-παρακολούθηση (security auditing) κλπ.

Στη συγκεκριμένη περίπτωση που μελετάται, οι ερευνητές εστίασαν σε λύσεις διαχείρισης του λογαριασμού χρηστών. Αυτές οι λύσεις χρησιμοποιούνται από τις επιχειρήσεις για την διαχείριση του κύκλου ζωής των ταυτοτήτων των χρηστών και των λογαριασμών σε προστατευόμενους πόρους. Ένα λάθος στη διαδικασία θα μπορούσε να δώσει περισσότερα δικαιώματα από ότι είναι απαραίτητο στους χρήστες ή να απαγορεύσει λανθασμένα την πρόσβαση.

Διαφορετικοί ενδιαφερόμενοι εστιάζουν σε διαφορετικές μετρικές σχετικά με τη διαδικασία IAM. Χαμηλού επιπέδου μετρικές περιλαμβάνουν:

- τον αριθμό σωστών ή εσφαλμένων ρυθμισμένων λογαριασμών χρηστών,
- τον αριθμό των λογαριασμών που εκκρεμούν (του ανθρώπινου δυναμικού που έχει εγκαταλείψει την επιχείρηση),
- τον συνολικό χρόνο έγκρισης (καθυστερήσεις) για την επίλυση αιτημάτων που σχετίζονται με τους λογαριασμούς χρηστών,

Πανεπιστήμιο Πειραιώς

- τον αριθμό απολεσθέντων αιτημάτων που ήταν προς έγκριση και διαμόρφωση,

- τον αριθμό αιτημάτων που παρακάμπτουν τις διαδικασίες έγκρισης.

Αυτές οι μετρήσεις μπορούν συνήθως να εντοπιστούν άμεσα από τα συστήματα IAM, αλλά συχνά είναι χρήσιμα μονάχα σε ένα υποσύνολο από τα ενδιαφερόμενα μέρη (π.χ. διαχειριστές ασφάλειας και εμπειρογνώμονες).

Για να συλλάβει κανείς τις απαιτήσεις όλων των ενδιαφερομένων που εμπλέκονται στην αξιολόγηση του συστήματος διαχείρισης λογαριασμών, χρειάζεται ένα πιο ευρύ σύνολο των μετρήσεων. Ως εκ τούτου, με τη διεξαγωγή συνεντεύξεων και την επικύρωση με ειδικούς του χώρου, οι ερευνητές εντόπισαν ένα ολοκληρωμένο σύνολο από υψηλού επιπέδου μετρικές, οι οποίες παρουσιάζονται στη συνέχεια [22]:

- Ενδιαφερόμενος: Διαχειριστής ασφάλειας
    - Ακρίβεια πρόσβασης: ο αριθμός των σωστά ρυθμισμένων λογαριασμών χρηστών, έναντι του συνολικού αριθμού των λογαριασμών που δημιουργήθηκαν, συμπεριλαμβανομένων και των λανθασμένα ρυθμισμένων λογαριασμών και των λογαριασμών που εκκρεμούν.
    - Ακρίβεια έγκρισης: ο αριθμός των εγκεκριμένων δραστηριοτήτων βάσει της εξουσιοδότησης του χρήστη, έναντι του συνολικού αριθμού δραστηριοτήτων, συμπεριλαμβανομένης των μη εξουσιοδοτημένων δραστηριοτήτων.

Πανεπιστήμιο Πειραιώς

- Ενδιαφερόμενος : Ιδιοκτήτης Εφαρμογής (Business/Application Owner)
    - Κόστος Παραγωγικότητας: αυτά είναι τα κόστη που προκύπτουν από την απώλεια παραγωγικότητας των εργαζομένων, λόγω καθυστερήσεων κατά τις φάσεις έγκρισης και διαμόρφωσης της διαδικασία διαχείρισης χρηστών.

- Ενδιαφερόμενος: IT Operations
    - Κόστος εγκατάστασης συστήματος IAM: αυτό είναι το κόστος της ανάπτυξης αυτοματοποιημένου συστήματος IAM, για ένα καθορισμένο χρονικό διάστημα (σταθερό και μεταβλητό κόστος)
    - Κόστος διαχείρισης: αυτός είναι ο πραγματικός αριθμός λειτουργιών διαχείρισης από τον οργανισμό, σε ένα συγκεκριμένο χρονικό διάστημα.

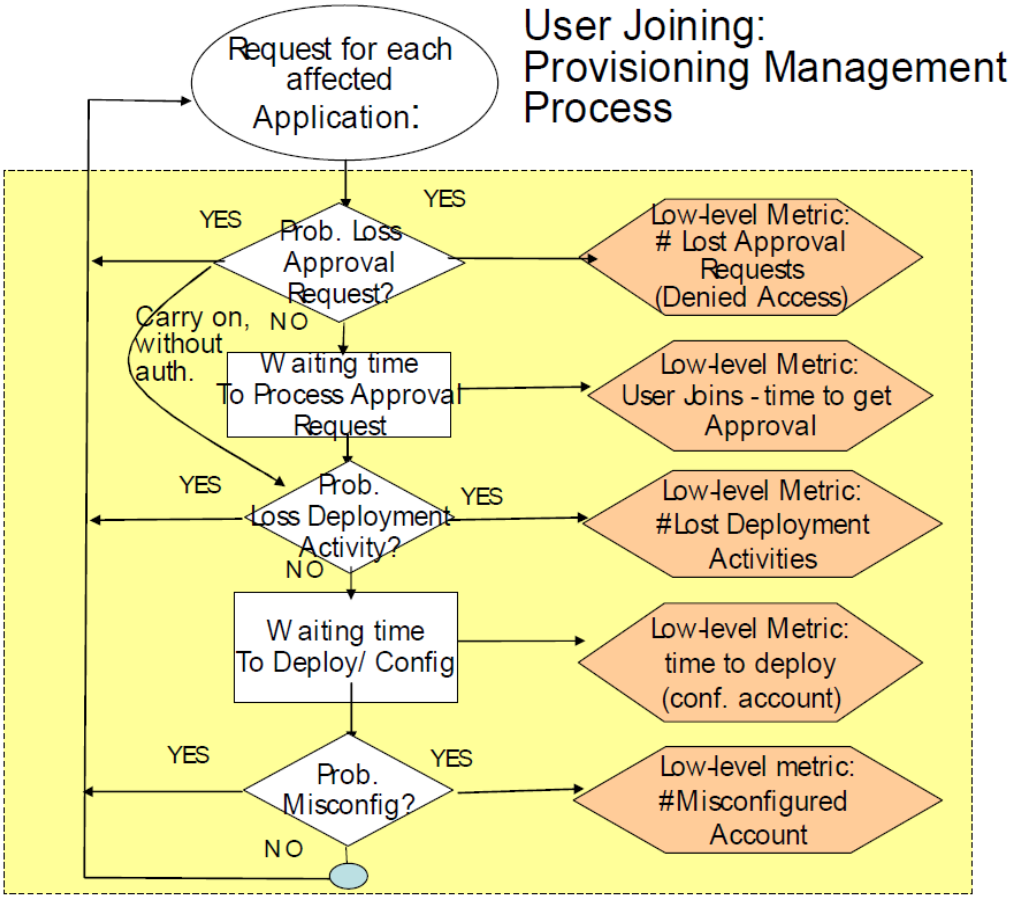
Θα μπορούσε να υποστηριχθεί ότι ορισμένες από τις παραπάνω υψηλού επιπέδου μερτικές, π.χ., το κόστος της παραγωγικότητας, δεν είναι μετρική ασφαλείας στην πραγματικότητα, ωστόσο, έχουν άμεση σχέση με τα ενδιαφερόμενα μέρη και είναι απαραίτητα για τη λήψη αποφάσεων και τη συνεχή αξιολόγηση του συστήματος IAM.

Για να αξιολογήσει κανείς τις επιπτώσεις αυτοματοποίησης της διαδικασίας διαχείρισης λογαριασμών, χτίστηκε ένα λεπτομερές μοντέλο που προσπαθεί να μοντελοποιήσει στοχαστικά διάφορα γεγονότα, όπως η δημιουργία ενός νέου χρήστη, η διαγραφή του ή η αλλαγή των ρόλων του. Σε απάντηση κάθε περίπτωσης, δημιουργήθηκε ένα σχετικό σύνολο εφαρμογών

Πανεπιστήμιο Πειραιώς

στα οποία οι λογαριασμοί των χρηστών πρέπει να διαμορφωθούν, με βάση το ρόλο και το προφίλ του χρήστη.

Το παρακάτω σχήμα δείχνει λεπτομέρεια της ροής της διαδικασίας που προκαλεί η αίτηση για δημιουργία ενός νέου χρήστη και η αίτηση για πρόσβαση σε διάφορες εφαρμογές.



Εικόνα 5: Διάγραμμα ροής

5. Συμπεράσματα

Η έννοια της ασφάλειας των Δικτύων και Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του.

Οι μετρικές ασφάλειας είναι ένας τομέας της ασφάλειας υπολογιστών που συγκεντρώνει μεγάλο ερευνητικό ενδιαφέρον τον τελευταίο καιρό. Οι πληροφορίες από τις μετρικές ασφάλειας θεωρούνται σημαντικός παράγοντας στη λήψη ορθών αποφάσεων σχετικά με διάφορες πτυχές της ασφάλειας, όπως ο σχεδιασμός των αρχιτεκτονικών ασφάλειας καθώς και οι έλεγχοι για την αποτελεσματικότητα και την αποδοτικότητα λειτουργιών που σχετίζονται με την ασφάλεια δικτύων και υπολογιστών.

Βασικά θέματα για την αξιολόγηση μιας μετρικής ασφάλειας είναι τα παρακάτω:

- **Ορθότητα και αποτελεσματικότητα**: Η ασφάλεια ενός πληροφοριακού συστήματος αποτελείται από δύο αλληλένδετες έννοιες: την ορθότητα και την αποτελεσματικότητα. Η ορθότητα παρέχει τη διαβεβαίωση ότι ο κάθε μηχανισμός έχει εφαρμοστεί σωστά (δηλαδή, πως λειτουργεί ακριβώς όπως έχει σχεδιαστεί για να λειτούργει, όπως για παράδειγμα για την εκτελεί άριστα κάποιο υπολογισμό). Η αποτελεσματικότητα παρέχει τη διαβεβαίωση ότι ο κάθε μηχανισμός του συστήματος ανταποκρίνεται στους επιδιωκόμενους στόχους ασφαλείας (δηλαδή, δεν κάνει τίποτα διαφορετικό από αυτό που προορίζεται να κάνει, ικανοποιώντας παράλληλα τις προσδοκίες για ανθεκτικότητα).

Πανεπιστήμιο Πειραιώς

- **Leadding / Lagging Indicators**: Οι μετρικές ασφάλειας μπορεί δυνητικά να είναι δείκτες οι οποίοι σε σχέση με την πραγματική κατάστασης της ασφάλειας του συστήματος είτε υστερούν χρονικά (Lagging Indicators), είτε είναι σύγχρονοι και συμπίπτουν, είτε προτρέχουν (Leading indicators). Είναι σημαντικό να αναγνωρίζει κανείς ποιοι δείκτες παρουσιάζουν ασύγχρονη συμπεριφορά και αν αυτοί χρησιμοποιούνται, θα πρέπει αντιμετωπιστούν κατάλληλα οι συναφείς περιορισμοί.

- **Ποιοτικά και Ποσοτικά Μετρικά**

Ανεξάρτητα με τα χαρακτηριστικά της κάθε επιχείρησης, θα μπορούσαν να χρησιμοποιηθούν τα παρακάτω επτά βασικά βήματα για τον σχεδιασμό και την ανάπτυξη ενός προγράμματος μετρικών ασφάλειας:

- Καθορισμός του στόχου του προγράμματος
- Επιλογή των μετρικών που θα παραχθούν
- Ανάπτυξη στρατηγικών για τη δημιουργία των μετρικών
- Δημιουργία πειραμάτων/δοκιμών και στόχων (benchmarking)
- Καθορισμός του τρόπου αναφοράς των μετρήσεων (reporting)

Οι επιχειρήσεις που προσπαθούν να μετρήσουν τις διαδικασίες ασφάλειας τους, μπορούν να αντλήσουν πληροφορίες από πολλές πιθανές πηγές δεδομένων, συμπεριλαμβανομένων των συστημάτων, του ανθρώπινου

Πανεπιστήμιο Πειραιώς

δυναμκού, και των διαδικασιών ελέγχου. Σε όλες σχεδόν τις περιπτώσεις, οι αναλυτές χρειάζονται να φιλτράρουν, να ταξινομούν, να αναλύουν, ή να μετατρέπουν τα δεδομένα έτσι ώστε αυτά να εμφανίζονται σε μια χρήσιμη μορφή.

Γνωστές στατιστικές μέθοδοι για την επεξεργασία δεδομένων, που χρησιμοποιούνται συχνά στις μετρικές ασφαλείας είναι οι παρακάτω:

- Ομαδοποίηση και Συνάθροιση μετρήσεων: δηλαδή η ενοποίηση των εγγραφών σε συνοπτικά στατιστικά στοιχεία για κάθε ομάδα. Όταν δημιουργεί κανείς μια "στατιστική περίληψη," για όλες τις εγγραφές σε κάθε ομάδας που ερευνά, τότε εκτελούνται μία ή περισσότερες από τις ακόλουθες ενέργειες για κάθε χαρακτηριστικό:
    - Άθροισμα
    - Μέσος όρος/ Διάμεσος
    - Τυπική απόκλιση
    - Υψηλότερη τιμή/ Χαμηλότερη τιμή
    - Πλήθος
- Ανάλυση Χρονοσειρών
- Συγχρονική ανάλυση (Cross-sectional Analysis)
- Ανάλυση ανά τεταρτημόριο (Quartile Analysis)
- Πίνακες Συσχέτισης

Πανεπιστήμιο Πειραιώς

Αναφορές

[1] Scott Berinato, A Few Good Information Security Metrics, CSO Magazine, July 01, 2005, http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics?contentId=220462&slug=&

[2] The CIS Security Metrics Service, The Center for Internet Security (CIS), July 1, 2008, http://securitymetrics.org/content/attach/Metricon3.0/metricon3-kreitner%20handout.pdf

[3] George Jelen, SSE-CMM Security Metrics, The National Institute of Standards and Technology (NIST) and Computer System Security and Privacy Advisory Board (CSSPAB) Workshop, Washington, D.C., June 13-14, 2000

[4] Rayford Vaughn Jr., Ronda Henning, Ambareen Siraj, Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, 30th Hawaii International Conference on System Sciences, Big Island, Hawaii, January 7-10, 2002

[5] Reijo M. Savola, Towards a Taxonomy for Information Security Metrics, International Conference on Software Engineering Advances (ICSEA 2007), Cap Esterel, France, August 2007

[6] Felix Salmon, Recipe for Disaster: The Formula That Killed Wall Street Wired Magazine, February 23, 2009,

[7] SSE-CMM: Systems Security Engineering Capability Maturity Model, International Systems Security Engineering Association (ISSEA), referenced on July 7, 2008

[8] Shirley C. Payne, A Guide to Security Metrics, SANS Security Essentials GSEC Practical Assignment, Version 1.2e, June 19, 2006

Πανεπιστήμιο Πειραιώς

[9] Wayne Jansen, Directions in Security Metrics Research, NIST, April 2009

http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf

[10] Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom, Commission of the European Communities Directorate XIII/F SOG-IS, June 1991, http://www.iwar.org.uk/comsec/resources/standards/itsec.htm

[11] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Common Criteria Portal, September 2006, Version 3.1 Revision 1, http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

[12] Steven Bellovin, On the Brittleness of Software and the Infeasibility of Security Metrics, IEEE Security and Privacy, Volume 4, Issue 4, July-Aug. 2006

[13] National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior: An Industry, Academic and Government Perspective, The Institute for Information Infrastructure Protection (I3P), 2009, http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf

[14] National Institute of standards and technology (NIST), U.S Department of commerce (Nistir 7564),
Wayne Jansen , Directions in Security Metrics Research, April 2009

[15] Mark Torgerson, Security Metrics, 12th International Command and Control Research and Technology Symposium, Newport, Rhode Island, June 20, 2007

[16] Mark Torgerson, Security Metrics for Communication Systems, 12th International Command and Control Research and Technology Symposium, Newport, Rhode Island, June 19-21, 2007

[17] Ronda Henning et al., Proceedings of the Workshop on Information

Πανεπιστήμιο Πειραιώς

Security System Scoring and Ranking, Applied Computer Security Associates, Williamsburg, Virginia, May 21-23, 2001,

[18] Gavin Reid, Peter Mell, Karen Scarfone, CVSS-SIG Version 2 History, Forum of Incident Response and Security Teams, June 13, 2007,

[19] Andrew Jaquith, Security Metrics: REPLACING FEAR, UNCERTAINTY,AND DOUBT, Addison-Wesley, 2007

[20] Berinato, Scott. "A Few Good Metrics," CSO Magazine, 1 July 2005. URL: http://www.csoonline.com/read/070105/metrics.htmlhttp://www.csoonline.com/read/070105/metrics.html (16 July 2006).

[21] Nwokedi Idika and Bharat Bhargava, Extending Attack Graph-based Security Metrics and Aggregating Their Application, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. X, NO. Y, Z 2010

[22] Yolanta Beres, Marco Casassa Mont, Jonathan Griffin, Simon Shiu, Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes, Third International Symposium on Empirical Software Engineering and Measurement, 2009

[23] Y. Beres, J. Griffin, S. Shiu, M. Heitman, D. Markle, P Ventura, "Analysing the Performance of Security Solutions to Reduce Vulnerability Exposure Window", ACSAC 08 and HP Labs Technical Report HPL-2008-121, December 2008.

[24] Department of defense trusted computer system evaluation criteria December 1985 http://csrc.nist.gov/publications/history/dod85.pdf

Πανεπιστήμιο Πειραιώς