Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακή Εργασία

Ενίσχυση της Ασφάλειας Πληροφοριακών Συστημάτων μέσω Συστημάτων Ειδοποίησης Αξιολόγησης Κινδύνων και Μηχανικής Μάθησης

Επιβλέπων Καθηγητής: Σ. Γκρίτζαλης

Άγγελος Κοκοβίδης a.kokovidis@ssl-unipi.gr mte2207

Πειραιάς
22/12/2023

Πρόλογος

Η παρούσα εργασία, με τίτλο «Ενίσχυση της Ασφάλειας Πληροφοριακών Συστημάτων μέσω Συστημάτων Προειδοποίησης Κινδύνων και Μηχανικής Μάθησης», στοχεύει να αντιμετωπίσει την αυξανόμενη σημασία της ασφάλειας συστημάτων πληροφοριών στο σημερινό ψηφιακό τοπίο. Υπό το πρίσμα του συνεχώς εξελισσόμενου τοπίου των απειλών στον κυβερνοχώρο, η έρευνα επιδιώκει να καθιερώσει μια ολοκληρωμένη προσέγγιση για την προστασία ευαίσθητων δεδομένων και τη διασφάλιση της επιχειρηματικής συνέχειας. Η κεντρική εστίαση περιλαμβάνει την ανάπτυξη ενός έξυπνου συστήματος ειδοποίησης που χρησιμοποιεί αλγόριθμους μηχανικής μάθησης για την κατηγοριοποίηση και την ιεράρχηση των εντοπισμένων κινδύνων.

Για την επίτευξη αυτού του στόχου, η μελέτη θα ξεκινήσει με μια εκτενή ανασκόπηση της υπάρχουσας βιβλιογραφίας σχετικά με την ασφάλεια συστημάτων πληροφοριών, τις μεθοδολογίες αξιολόγησης κινδύνου και την εφαρμογή της μηχανικής μάθησης στο πεδίο. Στη συνέχεια, η έρευνα θα προχωρήσει στη δημιουργία ενός πρωτότυπου συστήματος ειδοποιήσεων που θα ενσωματώνεται με τα τρέχοντα συστήματα πληροφοριών. Οι αλγόριθμοι μηχανικής μάθησης θα διαδραματίσουν κεντρικό ρόλο στην αυτόματη κατηγοριοποίηση των κινδύνων με βάση τον πιθανό αντίκτυπο, την πιθανότητα και τη συνάφειά τους με τον οργανισμό, βάσει των πεδίων εισόδου στους αλγορίθμους.

Η αναμενόμενη συμβολή της έρευνας έγκειται στην παροχή ενός πρακτικού πλαισίου για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων μέσω έξυπνης αξιολόγησης κινδύνου και συστημάτων ειδοποίησης σε πραγματικό χρόνο.

Πίνακας Περιεχομένων

1. Εισαγωγή

Εξέλιξη της ασφάλειας των συστημάτων πληροφοριών

Το ιστορικό τμήμα αυτής της εισαγωγής παρέχει μια αναδρομική άποψη της εξέλιξης της ασφάλειας των συστημάτων πληροφοριών. Ανιχνεύει τις ιστορικές εξελίξεις που οδήγησαν στο σημερινό τοπίο των απειλών στον κυβερνοχώρο. Κατανοώντας τις ρίζες των προκλήσεων ασφάλειας των συστημάτων πληροφοριών, η έρευνα στοχεύει να προσδιορίσει τη σημασία της υιοθέτησης προηγμένων εργαλείων αξιολόγησης κινδύνου και έξυπνων συστημάτων προειδοποίησης. Στην συνέχεια, αναφέρονται επιγραμματικά, τα στάδια εξέλιξης της ασφάλειας των πληροφοριακών συστημάτων.

- Πρώιμες προκλήσεις κυβερνοασφάλειας: Εξέταση των αρχικών προκλήσεων που αντιμετωπίζουν τα πρώιμα συστήματα και τα δίκτυα υπολογιστών. Αυτό μπορεί να περιλαμβάνει ζητήματα όπως μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων και έλλειψη ισχυρών μέτρων ασφαλείας.
- Ανάπτυξη πρωτοκόλλων ασφαλείας: Παρακολούθηση της ανάπτυξης θεμελιωδών πρωτοκόλλων και προτύπων ασφάλειας. Για παράδειγμα, η καθιέρωση προτύπων κρυπτογράφησης, ασφαλών πρωτοκόλλων επικοινωνίας και μηχανισμών ελέγχου ταυτότητας.
- Αξιοσημείωτα περιστατικά ασφαλείας: Μελέτη σημαντικών περιστατικών ασφαλείας και παραβιάσεων που έχουν συμβεί όλα αυτά τα χρόνια. Η κατανόηση αυτών των περιστατικών βοηθά στην αναγνώριση των τακτικών που χρησιμοποιούνται από κακόβουλους παράγοντες και των τρωτών σημείων που χρησιμοποιήθηκαν.
- Evolution of Threat Landscape: Αναλύοντας πώς έχει εξελιχθεί η φύση των απειλών στον κυβερνοχώρο. Αυτό περιλαμβάνει αλλαγές στους τύπους απειλών, από πρώιμους ιούς και κακόβουλο λογισμικό σε πιο εξελιγμένες μορφές επιθέσεων στον κυβερνοχώρο, όπως ransomware και προηγμένες επίμονες απειλές.
- Ρυθμιστικά Πλαίσια και Συμμόρφωση: Εξέταση της ανάπτυξης κανονιστικών πλαισίων και πλαισίων συμμόρφωσης. Αυτό περιλαμβάνει τη θέσπιση νόμων και προτύπων που διέπουν τις πρακτικές ασφάλειας πληροφοριών, με έμφαση στην προστασία του απορρήτου και των δεδομένων των χρηστών.
- Τεχνολογικές εξελίξεις: Παρακολούθηση των τεχνολογικών εξελίξεων που έχουν επηρεάσει την ασφάλεια των πληροφοριακών συστημάτων. Αυτό θα μπορούσε να περιλαμβάνει την ανάπτυξη συστημάτων ανίχνευσης εισβολών, τείχη προστασίας, λογισμικό προστασίας από ιούς και άλλα εργαλεία ασφαλείας.

- Ευαισθητοποίηση και Εκπαίδευση: Αναγνωρίζοντας την αύξηση της ευαισθητοποίησης και της εκπαίδευσης στον τομέα της κυβερνοασφάλειας. Αυτό συνεπάγεται την καθιέρωση της κυβερνοασφάλειας ως ξεχωριστού κλάδου και την αυξανόμενη έμφαση στην εκπαίδευση επαγγελματιών για την καταπολέμηση των απειλών στον κυβερνοχώρο.

Εικόνα 1: Εξέλιξη της ασφάλειας των συστημάτων πληροφοριών

Η κατανόηση της ιστορικής διάστασης της ασφάλειας συστημάτων πληροφοριών παρέχει τη βάση για την αναγνώριση προτύπων, τη διδαχή από λάθη του παρελθόντος και την προσαρμογή των μέτρων ασφαλείας για την αντιμετώπιση των τρεχουσών και μελλοντικών προκλήσεων. Ενημερώνει επίσης την ανάγκη για συνεχή καινοτομία και βελτίωση στις πρακτικές κυβερνοασφάλειας.

Σημασία της Ασφάλειας Πληροφοριακών Συστημάτων

Σε μια εποχή που κυριαρχούν οι ψηφιακές εξελίξεις, η σημασία της ασφάλειας των συστημάτων πληροφοριών δεν μπορεί να υπερεκτιμηθεί. Η παράγραφος υπογραμμίζει τον κρίσιμο ρόλο που διαδραματίζουν τα ασφαλή συστήματα πληροφοριών στη διαφύλαξη ευαίσθητων δεδομένων και στη διασφάλιση της επιχειρηματικής συνέχειας. Καθώς οι απειλές

στον κυβερνοχώρο συνεχίζουν να εξελίσσονται, η έμφαση στη σημασία των ισχυρών μέτρων ασφαλείας καθίσταται επιτακτική τόσο για άτομα όσο και για οργανισμούς.

Σκοπός και Πεδίο της Έρευνας

Ο σκοπός αυτής της έρευνας είναι διπλός. Πρώτον, στοχεύει να εμβαθύνει στη σφαίρα της ασφάλειας των πληροφοριακών συστημάτων, εστιάζοντας στις βασικές πτυχές των μεθοδολογιών αξιολόγησης κινδύνου και των μελετών ευπάθειας. Δεύτερον, η έρευνα φιλοδοξεί να συνεισφέρει μια απτή λύση με τη μορφή ενός έξυπνου συστήματος προειδοποίησης που θα τροφοδοτείται από αλγόριθμους μηχανικής μάθησης. Το πεδίο εφαρμογής είναι ευρύ και περιλαμβάνει μια ολοκληρωμένη εξερεύνηση της υπάρχουσας βιβλιογραφίας, την ανάπτυξη ενός πρωτότυπου συστήματος ειδοποιήσεων και την ενσωμάτωση της μηχανικής μάθησης για την κατηγοριοποίηση κινδύνων σε πραγματικό χρόνο.

Στόχοι της έρευνας

Οι στόχοι της έρευνας είναι σαφώς καθορισμένοι για να καθοδηγούν συστηματικά τη μελέτη. Πρωταρχικός στόχος είναι η συμβολή στον τομέα της κυβερνοασφάλειας με την ανάπτυξη ενός ευφυούς συστήματος προειδοποίησης. Για να επιτευχθεί αυτό, η μελέτη θα πραγματοποιήσει μια εκτενή βιβλιογραφική ανασκόπηση σχετικά με την ασφάλεια συστημάτων πληροφοριών, τις μεθοδολογίες αξιολόγησης κινδύνου και τις εφαρμογές μηχανικής μάθησης στο πεδίο. Οι επόμενοι στόχοι περιλαμβάνουν την ανάπτυξη ενός πρωτότυπου συστήματος ειδοποιήσεων ενσωματωμένου άψογα με τα υπάρχοντα συστήματα πληροφοριών και την εφαρμογή αλγορίθμων μηχανικής μάθησης για αυτόματη κατηγοριοποίηση κινδύνων με βάση τον αντίκτυπο, την πιθανότητα και τη συνάφεια.

2. Ανασκόπηση της βιβλιογραφίας

2.1 Επισκόπηση Ασφάλειας Πληροφοριακών Συστημάτων

Τα τελευταία χρόνια, η ασφάλεια μηχανικής μάθησης έχει κερδίσει σημαντική προσοχή στην ερευνητική κοινότητα [1], [2]. Αυτό το αυξημένο ενδιαφέρον μπορεί να αποδοθεί σε ένα σημαντικό σύνολο εργασιών που ασχολούνται με την ασφάλεια των αλγορίθμων βαθιάς μάθησης, ιδιαίτερα από τότε που οι Szegedy et al. [1] υπογράμμισε τα τρωτά σημεία που σχετίζονται με τα αντίθετα παραδείγματα σε μοντέλα βαθιάς μάθησης. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η έννοια της ασφάλειας μηχανικής μάθησης δεν είναι νέα [3], με προηγούμενες συνεισφορές που μπορούν να εντοπιστούν στους Dalvi et al. [4] το 2004. Αυτά τα πρωτοποριακά έργα, όπως τα [4] και [5], εμβαθύνουν στη σφαίρα της αντίθετης μηχανικής μάθησης, εστιάζοντας κυρίως σε αλγόριθμους μη βαθιάς μηχανικής μάθησης σε περιβάλλοντα όπως η ανίχνευση ανεπιθύμητων μηνυμάτων, η ανίχνευση κακόβουλου λογισμικού PDF και η εισβολή ανίχνευση [3]. Αυτές οι πρώιμες επιθέσεις κατηγοριοποιήθηκαν κυρίως ως επιθέσεις αποφυγής, ενώ ένα υποσύνολο αναγνωρίστηκε ως επιθέσεις δηλητηρίασης.

Ωστόσο, παρά την αυξανόμενη σημασία της ασφάλειας μηχανικής εκμάθησης, εξακολουθεί να υπάρχει έλλειψη περιεκτικών εγγράφων ανασκόπησης και έρευνας που να αντιμετωπίζουν ζητήματα απορρήτου και ασφάλειας. Για παράδειγμα, το 2010, οι Barreno et al. [6] εξέτασε τις επιθέσεις αποφυγής σε αλγόριθμους μη βαθιάς μάθησης, παρέχοντας πληροφορίες μέσω του φακού ενός φίλτρου ανεπιθύμητης αλληλογραφίας. Οι Akhtar και Mian [7] επικέντρωσαν την ανασκόπησή τους σε αντίπαλα παραδείγματα επιθέσεων εντός του τομέα της όρασης υπολογιστή που εφαρμόζεται στη βαθιά μάθηση. Εν τω μεταξύ, οι Yuan et al. [8] διεξήγαγε μια περιεκτική ανασκόπηση των αντίπαλων παραδειγμάτων στη βαθιά μάθηση, περιλαμβάνοντας τις μεθόδους παραγωγής και τα πιθανά αντίμετρα. Οι Riazi και Koushanfar [9] εμβάθυναν στη σφαίρα των αποδεδειγμένα ασφαλών τεχνικών διατήρησης της ιδιωτικής ζωής στο πλαίσιο της βαθιάς μάθησης, εστιάζοντας ιδιαίτερα στην προστασία του απορρήτου στη μηχανική μάθηση μέσω μεθόδων που βασίζονται σε κρυπτογραφικά συστήματα.

Οι προαναφερθείσες εργασίες ανασκόπησης έδωσαν έμφαση κυρίως σε συγκεκριμένους τύπους επιθέσεων, με κυρίαρχη εστίαση σε αντίθετες επιθέσεις. Αντίθετα, οι Biggio και Roli [3] παρείχαν μια εκτεταμένη ανασκόπηση που περιελάμβανε ένα ευρύτερο πεδίο της αντίθετης μηχανικής μάθησης. Η περιεκτική τους επισκόπηση καλύπτει την τελευταία δεκαετία και περιλαμβάνει συζητήσεις για την ασφάλεια τόσο των παλαιότερων αλγορίθμων μη βαθιάς μηχανικής μάθησης όσο και των πρόσφατων αλγορίθμων βαθιάς μάθησης στην όραση υπολογιστών και την ασφάλεια στον κυβερνοχώρο. Η αναθεώρησή τους καλύπτει επιθέσεις αποφυγής καθώς και επιθέσεις δηλητηρίασης, συνοδευόμενες από συζητήσεις για τους

αντίστοιχους αμυντικούς μηχανισμούς. Οι Liu et al. [10] έλαβε μια ξεχωριστή προοπτική αναλύοντας τις απειλές και τις άμυνες ασφαλείας στη μηχανική μάθηση, με ιδιαίτερη έμφαση στην αξιολόγηση της ασφάλειας και στην ασφάλεια των δεδομένων. Από την άλλη, οι Papernot et al. [11] συστηματοποίησε τα πολύπλευρα ζητήματα ασφάλειας και απορρήτου γύρω από τη μηχανική εκμάθηση. Κατηγοριοποίησαν τις επιθέσεις σύμφωνα με τρία κλασικά χαρακτηριστικά ασφαλείας - εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα - ενώ διερευνούσαν τις άμυνες όσον αφορά την ευρωστία, την υπευθυνότητα και το απόρρητο [11].

Εικόνα 2: Μέρη Security

Συνοπτικά, το τοπίο της ασφάλειας μηχανικής μάθησης έχει σημειώσει σημαντική ανάπτυξη τα τελευταία χρόνια, με μια ποικιλία εγγράφων ανασκόπησης και έρευνας που ρίχνουν φως σε διαφορετικές πτυχές αυτού του δυναμικού πεδίου. Ενώ πολλά από αυτά τα έργα έχουν δώσει έμφαση στις αντίπαλες επιθέσεις, ορισμένα έχουν αποτολμήσει σε ευρύτερες περιοχές, εξερευνώντας διάφορους τύπους επιθέσεων, στρατηγικές άμυνας και ζητήματα απορρήτου στο πεδίο της ασφάλειας μηχανικής μάθησης.

Γιατί η Μηχανική Μάθηση μπορεί να δεχτεί επίθεση;

Το παράδειγμα μηχανικής μάθησης, λόγω των χαρακτηριστικών του, είναι επιρρεπές σε ποικίλες επιθέσεις. Κατά τη φάση της εκπαίδευσης, η χρήση τεράστιων δεδομένων εκπαίδευσης και οι υπολογιστικές περιπλοκές που εμπλέκονται στα δίκτυα βαθιάς μάθησης εισάγουν τρωτά σημεία. Αυτά τα τρωτά σημεία εκδηλώνονται σε διάφορα σενάρια:

- Η διαδικασία εκπαίδευσης συχνά ανατίθεται σε τρίτους [12].
- Προεκπαιδευμένα μοντέλα, που χρησιμεύουν ως IPs, ενσωματώνονται στο δίκτυο.
- Ένας σημαντικός όγκος δεδομένων προέρχεται από μη αξιόπιστους χρήστες ή τρίτους χωρίς να υποβάλλονται σε αυστηρές διαδικασίες επικύρωσης δεδομένων.

Ενώ αυτά τα πρότυπα εργασίας ενισχύουν την αποτελεσματικότητα της μηχανικής μάθησης, εισάγουν ταυτόχρονα νέες απειλές για την ασφάλεια. Επιπλέον, ο πολλαπλασιασμός των μοντέλων μηχανικής μάθησης ως υπηρεσίας, όπου τα μοντέλα μηχανικής μάθησης λειτουργούν σε διακομιστές ή στο cloud, επιτρέποντας στους πελάτες να αναζητήσουν τα μοντέλα μέσω API πρόβλεψης, παρουσιάζει ένα μοναδικό σύνολο προκλήσεων. Τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση αυτών των μοντέλων είναι συχνά ευαίσθητα και οι παράμετροι του μοντέλου έχουν σημαντική εμπορική αξία και, κατά συνέπεια, πρέπει να παραμένουν εμπιστευτικές. Κατά συνέπεια, αυτά γίνονται δελεαστικοί στόχοι για τους επιτιθέμενους κατά τη φάση της δοκιμής.

Εικόνα 3: Μηχανική Μάθηση και Ασφάλεια ΠΣ

Η διερεύνηση των κινήτρων πίσω από αυτές τις επιθέσεις παραμένει ένα ανοιχτό πρόβλημα. Ενώ υπάρχουν συνεχείς συζητήσεις σχετικά με τους παράγοντες που συμβάλλουν στην επιτυχία των επιθέσεων σε μοντέλα μηχανικής μάθησης, δεν έχει ακόμη επιτευχθεί συναίνεση.

Περαιτέρω πολυπλοκότητα προκύπτει από την επίδραση της υπερπροσαρμογής και την επιρροή της στην ικανότητα ενός αντιπάλου να ανακτήσει ευαίσθητα δεδομένα ή χαρακτηριστικά εκπαίδευσης. Έρευνα των Yeom et al. [13] εμβαθύνει στον ρόλο της υπερπροσαρμογής και στον αντίκτυπό της στην ενεργοποίηση επιθέσεων συμπερασμάτων μέλους. Η περίπλοκη και ανεξήγητη φύση των μοντέλων μηχανικής μάθησης έχει οδηγήσει σε επίμονα ερωτήματα, όπως εάν τα αντίθετα παραδείγματα είναι εγγενή στο μοντέλο ή απλές ανωμαλίες. Επιπλέον, οι λόγοι πίσω από την ανάκτηση ευαίσθητων δεδομένων εκπαίδευσης μέσω κανονικών ερωτημάτων παραμένουν άλυτοι, υπογραμμίζοντας τις συνεχιζόμενες προκλήσεις στην κατανόηση και την αντιμετώπιση αυτών των τρωτών σημείων μηχανικής μάθησης.

2.2 Μεθοδολογίες Αξιολόγησης Κινδύνων και Μηχανική Μάθηση στην Ασφάλεια Πληροφοριακών Συστημάτων

Ανίχνευση και Πρόληψη Εισβολών

Τα τελευταία χρόνια, η υπηρεσία Διαδικτύου έχει διαδραματίσει σημαντικό ρόλο στα επιχειρηματικά μοντέλα. Δεδομένου ότι τόσο ο πελάτης όσο και η επιχείρηση χρησιμοποιούν εφαρμογές Διαδικτύου, η ασφάλεια των δεδομένων κατά τη χρήση του Διαδικτύου ως μέσου έχει γίνει πρωταρχικό μέλημα [14]. Το σύστημα ανίχνευσης εισβολής (IDS) παρέχει μια άμυνα για την αντιμετώπιση των επιθέσεων [15], [16]. Στο IDS, προτείνονται διάφορες προσεγγίσεις όπως η ανάλυση ωφέλιμου φορτίου πακέτων [17], η διάδοση προτύπων [18] και η γλώσσα bro [19]. Επιπλέον, προτείνονται διάφορα σχήματα για ad-hoc δίκτυα για την ανίχνευση προτύπων επίθεσης και την παροχή ενός αμυντικού μηχανισμού στο δίκτυο [20]-[24]. Τα IDS που είναι παθητικά από τη φύση τους έχουν ένα βασικό ζήτημα την αδυναμία τους να διαμορφώσουν στοχευμένη, αξιόπιστη και προσαρμοστική απόκριση [25]. Ως εκ τούτου, μερικές φορές το IDS σε επίπεδο κεντρικού υπολογιστή δεν διασφαλίζει τον τρόπο επεξεργασίας ενός πακέτου που μπορεί να οδηγήσει σε λανθασμένες αποφάσεις [26] και γι' αυτό απαιτείται το προσαρμοστικό και προληπτικό σύστημα μέσω του IDS. Στο [27], οι συγγραφείς αναφέρουν προσεγγίσεις που βασίζονται σε ανωμαλίες και βασισμένες σε υπογραφές για το IDS ως εξής.

Προσεγγίσεις συστήματος ανίχνευσης εισβολής

Σε αυτό το τμήμα, εξετάζουμε τους τύπους προσεγγίσεων για το IDS. Στο IDS, βασικοί παράγοντες προκαλούν σφάλμα στην εκμάθηση ταξινομητή λόγω θορύβου, προκατάληψης και διακύμανσης. Ως εκ τούτου, οι ταξινομητές συνόλου και οι υβριδικοί ταξινομητές είναι οι τύποι ταξινομητών πολλαπλών κλάσεων που βοηθούν στην ελαχιστοποίηση αυτών των παραγόντων λόγω των ιδιοτήτων ενίσχυσης και στοίβαξης στα μοντέλα ταξινομητών. Με βάση αυτά τα κριτήρια, έχουμε αναλύσει μια προσέγγιση που βασίζεται σε υπογραφές και βασίζεται σε ανωμαλίες.

Προσέγγιση με βάση την υπογραφή

Μια τεχνική ανίχνευσης εισβολής που βασίζεται σε υπογραφές χρησιμοποιεί ένα προκαθορισμένο μοτίβο για τον εντοπισμό κακόβουλης δραστηριότητας [15] ενώ στις παραδοσιακές μεθόδους, ενδέχεται να μην είναι σε θέση να ενημερώσει το σύστημα σχετικά με νέες απειλές.

Ενιαίος ταξινομητής

Σε αυτόν τον τύπο τεχνικής ανίχνευσης εισβολής, χρησιμοποιείται μόνο ένας αλγόριθμος ML για την ανίχνευση της εισβολής. Οι Akira et al. [28] πρότεινε έναν αλγόριθμο δέντρου αποφάσεων με τον δείκτη Gini, ο οποίος δημιουργεί εκλεπτυσμένα δεδομένα που χρησιμοποιούνται για την εκμάθηση των ταξινομητών για την αύξηση των ειδοποιήσεων ως έξοδο IDS που βασίζεται στην υπογραφή. Οι Lippmann et al. [29] αντιπροσωπεύουν μια θεωρία που ανιχνεύει την υπογραφή μιας γνωστής επίθεσης εξετάζοντας βασικές λέξεις-κλειδιά προσανατολισμένες στην επίθεση στο δίκτυο. Τα δεδομένα ανίχνευσης δικτύου χρησιμοποιούνται για την παραγωγή του αριθμού των λέξεων-κλειδιών σε κάθε περίοδο λειτουργίας telnet. Η καταμέτρηση των εμφανίσεων κάθε λέξης-κλειδιού χρησιμοποιείται για ανίχνευση από τον ταξινομητή νευρωνικού δικτύου. Οι Wong et al. [30] απεικόνισε ένα τεχνητό νευρωνικό δίκτυο (ANN) καθώς και μια προσέγγιση ταξινομητή που βασίζεται σε διανύσματα υποστήριξης για την πρόβλεψη των τύπων επιθέσεων, οι οποίες βασίζονται σε τεχνικές κωδικοποίησης που βασίζονται στη συχνότητα. Το ANN εκπαιδεύεται με τον αλγόριθμο backpropagation για την πρόβλεψη της εισβολής. Επιπλέον, ένα μοντέλο μηχανής διανύσματος υποστήριξης (SVM) έχει επίσης κατασκευαστεί για την ταξινόμηση της επίθεσης. Από την παρατήρηση και των δύο τεχνικών, δείχνει ότι το SVM δίνει καλύτερα αποτελέσματα από το ANN για την ίδια μέθοδο κωδικοποίησης ανίχνευσης.

Στο [38], οι συγγραφείς παρουσίασαν ένα σχήμα για τη δημιουργία βάσης δεδομένων εισβολής με κύριο στόχο τη δημιουργία ενός εύκολου στην ενημέρωση εργαλείου βάσης δεδομένων που παράγει ταυτόχρονα πραγματικά δεδομένα κίνησης. Για να καταστεί αποτελεσματικό το σχήμα ML, η προτεινόμενη μέθοδος χρησιμοποιείται ως τεχνική επιλογής χαρακτηριστικών πολλαπλών στόχων που αναγνωρίζει σημαντικά χαρακτηριστικά δικτύου που αποδίδουν υψηλότερη ακρίβεια. Οι Ghanem et al. [39] θεώρησε ότι το IDS που βασίζεται σε ανωμαλίες στοχεύει στην επίτευξη υπερβολικού αριθμού ψευδών συναγερμών. Κατασκεύασαν μια τεχνική εκμάθησης με βάση το SVM που συμπληρώνει την απόδοση του IDS και επίσης μειώνει δραστικά το ποσοστό ψευδών συναγερμών. Στην προβλεπόμενη αξιολόγηση απόδοσης, η μη εποπτευόμενη προσέγγιση IDS εντοπίζει όλη την κακόβουλη κυκλοφορία και μειώνει τους ψευδείς συναγερμούς σε σύγκριση με τις γραμμικές και μη γραμμικές προσεγγίσεις SVM μίας και δύο κλάσεων.

Υβριδικός ταξινομητής

Αυτός ο τύπος ταξινομητή είναι κυρίως ένα μείγμα του ετερογενούς περιβάλλοντος ή/και ταξινομητών ως μηχανισμός ανίχνευσης στον οποίο καλύπτεται από τη φάση κανονικοποίησης δεδομένων έως τη φάση της τελικής απόφασης. Borges et al. [31] παρουσίασε μια μονάδα ελέγχου επικοινωνίας, μια μονάδα παρακολούθησης, μια μονάδα κινητής συσχέτισης και εξαρτήματα του κέντρου εντολών και ελέγχου (C&C) που περιγράφονται στα οποία το κέντρο του κέντρου εντολών και ελέγχου (C&C) αποτελείται από έναν υβριδικό ταξινομητή. Η μονάδα παρακολούθησης είναι υπεύθυνη για την παρακολούθηση κανονικών και μη φυσιολογικών μοτίβων πρόσβασης και χρήσης αρχείων, παρατηρητή περιεχομένου και δέκτη εκπομπής. Όλες οι πληροφορίες που συλλέγονται με αυτόν τον τρόπο χρησιμοποιούνται στη συνέχεια από τους ταξινομητές ML για πρόσβαση εάν οποιοσδήποτε χρήστης ή εφαρμογή κινητής συσκευής αντιμετωπίζει απειλές ασφαλείας. Οι Karthick et al. [32] παρουσίασε ένα πλαίσιο δύο σταδίων: ο πρωτοβάθμιος ταξινομητής Bayes χρησιμοποιείται για να υψώσει μια σημαία (flag) που προσδιορίζει κακόβουλες δραστηριότητες στο δίκτυο και την εισερχόμενη κίνηση που τροφοδοτείται ως είσοδος στο κρυφό μοντέλο Markov (HMM). Το HMM είναι μια αποτελεσματική προσέγγιση στη μαύρη λίστα διευθύνσεων IP με βάση ύποπτα χαρακτηριστικά της κίνησης. Το μοντέλο γραφικής παράστασης [33] που προτείνεται από τους Tsai et al. [34] (πλησιέστεροι γείτονες με βάση την περιοχή τριγώνου) χρησιμοποιεί ομαδοποίηση K-means για να ολοκληρώσει το κέντρο συμπλέγματος που αντιστοιχεί στις κλάσεις επίθεσης. Δύο κέντρα συμπλέγματος και ένα δεδομένα μεταξύ των συνόλων δεδομένων χρησιμοποιούνται για τον υπολογισμό του εμβαδού του τριγώνου και για να σχηματίσουν μια υπογραφή από αυτόν τον ταξινομητή K-Nearest Neighbor που χρησιμοποιείται για τον εντοπισμό απειλών.

Οι Al-Yaseen et al. [49] απεικόνισε έναν τροποποιημένο αλγόριθμο k-means που στοχεύει στην επίτευξη υψηλής απόδοσης και εξετάζει όλα τα πιθανά ενδεχόμενα αντιμετωπίζοντας όλα τα αποκλίνοντα σημεία στα σύνολα δεδομένων ως το αρχικό κέντρο του συμπλέγματος αντί να επιλέγει ένα συγκεκριμένο σύνολο αρχικών κεντροειδών τυχαία. Επιπλέον, η τροποποιημένη τυπική τεχνική C4.5 ομαδοποίησης k-means [50] δημιουργεί ένα δέντρο από τα συμπλέγματα που μπορεί να ανιχνεύσει την ανωμαλία χρησιμοποιώντας τη μέγιστη πληροφορία που αποκτάται από την επιλογή χαρακτηριστικών. Κατά συνέπεια, οι ελάχιστες πληροφορίες διαχωρίζονται για να δημιουργηθεί μια δομή δέντρου κανονικών και κακόβουλων συμπεριφορών. Abadeh et al. [51] πρότεινε έναν παράλληλο αλγόριθμο τοπικής γενετικής αναζήτησης που είναι ικανός να δημιουργεί ασαφείς κανόνες για την ανίχνευση παρεμβατικής συμπεριφοράς στα δίκτυα. Σε αυτή την προσέγγιση, ο πληθυσμός χωρίζεται σε υποπληθυσμούς, οι οποίοι είναι ο αριθμός των τάξεων για την ανάλυση ταξινόμησης ή το πρόβλημα, και το σύνολο εκπαίδευσης για κάθε ταξινομητή είναι διαφορετικό μεταξύ τους. Το ασαφές σύνολο κανόνων εξελίσσεται ανεξάρτητα με παράλληλο τρόπο και χρησιμοποιείται ως πηγή γνώσης για κάθε ταξινομητή για ανίχνευση εισβολής.

Ταξινομητής συνόλου

Το σύνολο είναι ένας συνδυασμένος ταξινομητής πολλαπλών αδύναμων ταξινομητών. Σε αυτή τη μέθοδο, οι αδύναμοι εκπαιδεύονται έτσι ώστε η συμπεριληπτική δράση του μοντέλου να μπορεί να μετριαστεί επαρκώς. Για τη βελτίωση της απόδοσης του αδύναμου εκπαιδευόμενου, adaptive boosting [35], bagging [36], wagging [35], random forest [36] and cross validators committees [35] παίζουν κρίσιμο ρόλο. Οι Ma et al. [37] πρότεινε ένα σχήμα που συνδυάζει το βαθύ νευρωνικό δίκτυο (DNN) και τους αλγόριθμους φασματικής ομαδοποίησης. Τα σύνολα δεδομένων εντάσσονται στα υποσύνολα K χρησιμοποιώντας κέντρα συμπλέγματος. Με βάση τα χαρακτηριστικά ομοιότητας, η απόσταση μετράται μεταξύ των σημείων δεδομένων σε σετ εκπαίδευσης και σετ δοκιμών που χρησιμοποιούνται στο μοντέλο του DNN για την ανίχνευση της εισβολής.

Προσέγγιση που βασίζεται στην ανωμαλία

Αυτός ο τύπος τεχνικής παρατηρεί τη συμπεριφορά του συστήματος και προσδιορίζει την ανωμαλία από την απόκλιση του κανονικού συστήματος. Ως εκ τούτου, αυτός ο τύπος συστήματος έχει την ικανότητα να ανιχνεύει την επίθεση zero-day [26]. Χρησιμοποιώντας αυτήν την τεχνική, η κανονική συμπεριφορά του συστήματος μπορεί να προσαρμοστεί έτσι ώστε, για τον αντίπαλο, να είναι δύσκολο να καταλάβει την κανονική συμπεριφορά του συστήματος.

Εικόνα 4: Μεθοδολογίες Αξιολόγησης Κινδύνων και Μηχανική Μάθηση

Πρόληψη εισβολής

Η πρόληψη εισβολής είναι μια τεχνική πρόληψης ευπάθειας που παρακολουθεί τη ροή του δικτύου για να ανιχνεύσει και να αποτρέψει την κακή χρήση της κυκλοφορίας. Η πρόληψη εισβολής είναι μια επέκταση του IDS, ωστόσο, και οι δύο ερευνούν κακόβουλη δραστηριότητα στην κίνηση του δικτύου. Μια κρίσιμη διαφορά στην πρόληψη εισβολής έναντι της ανίχνευσης εισβολής είναι ότι η πρόληψη εισβολής είναι η κατασκευή και ο σχεδιασμός πιο ενεργής προστασίας για τη βελτίωση της ανίχνευσης εισβολής. Αυτός ο τύπος προσέγγισης είναι πιο κατάλληλος όταν είναι απαραίτητο να αντιδράσουμε σε πραγματικό χρόνο για να αποτρέψουμε ή να αποκλείσουμε κακόβουλες δραστηριότητες. Στο [54], οι συγγραφείς ασχολήθηκαν με το θέμα της κυβερνοτρομοκρατίας και τόνισαν ότι ο μηχανισμός απόκρισης και άμυνας οποιουδήποτε συστήματος πρέπει να είναι ισχυρός, προσαρμοστικός και αποτελεσματικός. Πρότειναν έναν μηχανισμό γενετικού προγραμματισμού για την απαγόρευση του εγκλήματος στον κυβερνοχώρο. Τα βασικά όπλα των κυβερνοτρομοκρατών είναι μια τροποποιημένη έκδοση μεθόδων εισβολής, όπως πλαστογράφηση, βόμβες email, sniffing δεδομένων, παράσιτα, σκουλήκια, κερκόπορτες, επιθέσεις DoS [55], Δούρειος ίππος [56].

Ανίχνευση phishing

Το ηλεκτρονικό ψάρεμα (phishing) είναι μια τεχνική για την κλοπή προσωπικών και ευαίσθητων πληροφοριών του θύματος, δελεάζοντας τους χρήστες να επισκεφτούν ένα ψεύτικο email ή ιστοσελίδες για να μιμηθούν την οπτική ταυτότητα της ίδιας της σελίδας του θύματος. Οι επιθέσεις phishing προκαλούν ζημιά στις προσωπικές και ευαίσθητες πληροφορίες ενός θύματος με πλαστογράφηση email [57], ψεύτικους λογαριασμούς κοινωνικών δικτύων [58] και εισβολή [59]. Για τον εντοπισμό επιθέσεων phishing, έχουν προταθεί πολλές προσεγγίσεις, όπως η μαύρη λίστα που βασίζεται σε DNS, η αυτοματοποιημένη μεμονωμένη λευκή λίστα, η ευρετική και οπτική ομοιότητα και τεχνικές που βασίζονται σε ML.

Διατήρηση απορρήτου

Ο πρωταρχικός στόχος μιας τεχνικής ML είναι να εξάγει τις απαραίτητες πληροφορίες από τα δεδομένα από τους ταξινομητές της, διατηρώντας παράλληλα το απόρρητο καλύπτοντας/απόκρυψη των ευαίσθητων δεδομένων από τον αντίπαλο [59]. Επομένως, υπάρχει ανάγκη να εξισορροπηθούν αυτές οι πτυχές, ενώ τα ευαίσθητα δεδομένα πρόκειται να εξορυχθούν. Για την ανάλυση των τρωτών σημείων στη διατήρηση της ιδιωτικής ζωής, αρκετοί ερευνητές έχουν προτείνει τεχνικές επίθεσης, όπως ελάχιστες επιθέσεις, επιθέσεις γνώσης υποβάθρου [60], διαταραχές αθροιστικών δεδομένων και επιθέσεις ομοιογένειας.

Ανίχνευση ανεπιθύμητων μηνυμάτων

Τα τελευταία χρόνια, το ερευνητικό ενδιαφέρον έχει αυξηθεί για υπηρεσίες και συστήματα που βασίζονται στο διαδίκτυο, την κοινωνική δικτύωση και τα μέσα κοινωνικής δικτύωσης που ενσωματώνουν δεδομένα μεγάλης κλίμακας [61]. Πολλές τεχνικές ανίχνευσης έχουν προταθεί με βάση την ταξινόμησή τους. Στο [62], οι συγγραφείς πρότειναν μια τεχνική για την αποφυγή της διανομής ανεπιθύμητων μηνυμάτων. Προτάθηκαν αρκετοί αλγόριθμοι, όπως ανίχνευση ανεπιθύμητου περιεχομένου βάσει περιεχομένου [63], ανίχνευση ανεπιθύμητων μηνυμάτων βάσει συνδέσμων [64], ανίχνευση βάσει αξιοπιστίας στο IoT [65], ανίχνευση ανεπιθύμητης αλληλογραφίας σε πραγματικό χρόνο [66] και ανίχνευση ανεπιθύμητων μηνυμάτων κλικ [67] για ανίχνευση ανεπιθύμητων μηνυμάτων.

Εκτίμηση Κινδύνου

Η αξιολόγηση κινδύνου παρέχει μια ολοκληρωμένη εικόνα του υπάρχοντος οργανισμού ή συστήματος για την απόκτηση συνεπειών κινδύνου, κινδύνου ασφάλειας [68] και αντίμετρα για την αντιμετώπισή τους. Σύμφωνα με το [69], οι τεχνικές εκτίμησης κινδύνου χωρίζονται σε δύο τύπους κινδύνου: (1) ποιοτικό κίνδυνο και (2) ποσοτικός κίνδυνος. Ο

ποιοτικός κίνδυνος πραγματοποιείται από την κατεύθυνση πολιτικής και τις ποσοτικές πληροφορίες, τη γνώση των ενδιαφερομένων και τα μαθήματα ιστορίας για το σύστημα, το προφίλ κινδύνου και τον αντίκτυπο [70]. Το συμπέρασμα που προκύπτει από την ποιοτική αξιολόγηση είναι πιο ολοκληρωμένο και διανοητικό. Η μέθοδος αναλυτικής ιεραρχίας [71], η μέθοδος ανάλυσης παραγόντων [72], η μέθοδος κατάταξης [73] και η μέθοδος delphi [72] είχαν προταθεί στο παρελθόν για την αξιολόγηση κινδύνου.

Δοκιμή ιδιοτήτων ασφαλείας

Οι ιδιότητες ασφαλείας διαδραματίζουν βασικό ρόλο σε οποιαδήποτε κατανεμημένα συστήματα, όπως η στρατιωτική υποδομή, οι τράπεζες, το ηλεκτρονικό εμπόριο, τα κρίσιμα για την ασφάλεια αυτόνομα συστήματα, τα κινητά ad-hoc και άλλα [74]. Πολλές τεχνικές ανάλυσης και μοντελοποίησης έχουν προταθεί για να διασφαλιστεί η ορθότητα του πρωτοκόλλου ασφαλείας. Αυτές οι εργασίες αποσκοπούσαν στην επικύρωση των προδιαγραφών του πρωτοκόλλου. Μια αναφορά [75] δείχνει ότι τα σφάλματα και τα σφάλματα κατά τον προγραμματισμό είναι κοινά στο κρίσιμο για την ασφάλεια σύστημα, το οποίο πρέπει να εντοπιστεί και να αντιμετωπιστεί σωστά.

2.3 Υφιστάμενα συστήματα προειδοποίησης και οι περιορισμοί τους

Πλαίσιο Διαχείρισης Κινδύνων NIST (RMF):

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) παρέχει ένα ολοκληρωμένο Πλαίσιο Διαχείρισης Κινδύνων που βοηθά τους οργανισμούς να αξιολογούν και να διαχειρίζονται τους κινδύνους για τα πληροφοριακά τους συστήματα. Χρησιμοποιείται ευρέως στην κυβέρνηση των Ηνωμένων Πολιτειών και από οργανισμούς που πρέπει να συμμορφώνονται με τα πρότυπα NIST.

Εικόνα 5: NIST

FAIR (Ανάλυση παραγόντων του κινδύνου πληροφοριών):

Το FAIR είναι ένα πλαίσιο για την κατανόηση, την ανάλυση και την ποσοτικοποίηση του κινδύνου πληροφοριών από οικονομική άποψη. Παρέχει μια δομημένη προσέγγιση για την αξιολόγηση του κινδύνου και τη λήψη τεκμηριωμένων αποφάσεων.

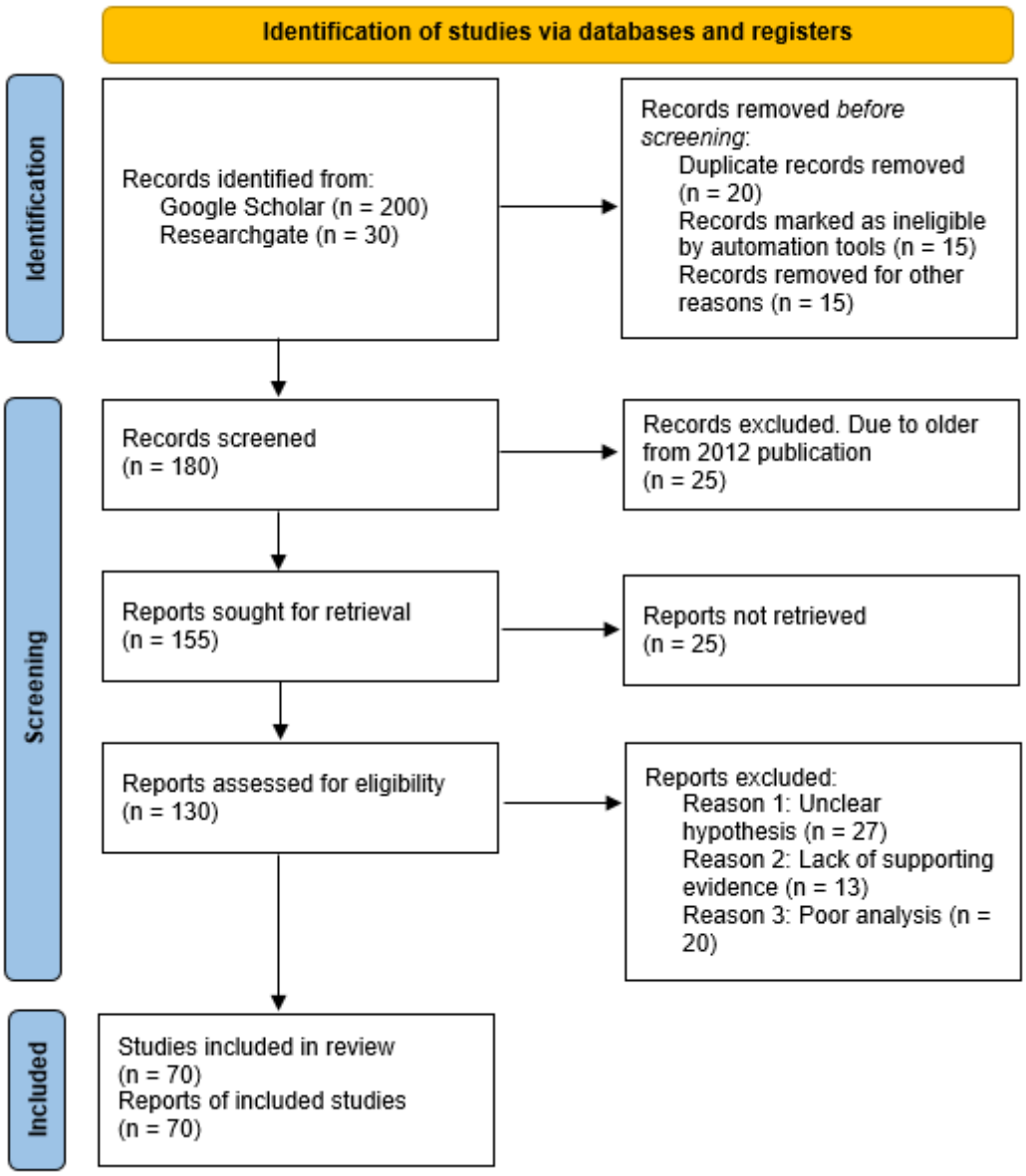
Μεθοδολογία αξιολόγησης κινδύνου OWASP:

Το Open Web Application Security Project (OWASP) προσφέρει μια μεθοδολογία αξιολόγησης κινδύνου που επικεντρώνεται ειδικά στην ασφάλεια εφαρμογών Ιστού. Βοηθά τους οργανισμούς να αξιολογήσουν και να ιεραρχήσουν τους κινδύνους ασφαλείας που σχετίζονται με τις διαδικτυακές εφαρμογές.

3. Μεθοδολογία

3.1 Σχεδιασμός Έρευνας

Η παρακάτω εικόνα είναι ένα διάγραμμα ροής που χρησιμοποιείται συνήθως σε συστηματικές αναθεωρήσεις και μετα-αναλύσεις για την αναφορά της ροής πληροφοριών στις διάφορες φάσεις μιας τέτοιας αναθεώρησης. Παρουσιάζει τη μεθοδολογία PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses).



Εικόνα 6: Μεθοδολογία έρευνας PRISMA

Ακολουθεί μια ανάλυση των σταδίων στο διάγραμμα ροής PRISMA που απεικονίζεται στην εικόνα:

- Identification: Εδώ αναγνωρίζονται οι εγγραφές μέσω της αναζήτησης στη βάση δεδομένων. Για παράδειγμα, το γράφημα σημειώνει ότι 200 εγγραφές εντοπίστηκαν από το Google Scholar και 30 από το ResearchGate.
- Screening: Μετά την αναγνώριση, τα αρχεία ελέγχονται. Το γράφημα δείχνει ότι εξετάστηκαν 180 εγγραφές. Τα αρχεία μπορούν να αφαιρεθούν πριν από τον έλεγχο για διάφορους λόγους, όπως διπλότυπα, μη καταλληλότητα ή άλλους λόγους που δεν προσδιορίζονται.
- Eligibility: Από τις εγγραφές που ελέγχθηκαν, αναζητείται ένας αριθμός για ανάκτηση. Στην περίπτωση αυτή αναζητήθηκαν 155 αναφορές. Στη συνέχεια, οι εργασίες αξιολογούνται ως προς την επιλεξιμότητα βάσει κριτηρίων ένταξης. Το διάγραμμα δείχνει ότι 130 εργασίες αξιολογήθηκαν ως προς την καταλληλότητα και αρκετές αποκλείστηκαν για λόγους όπως ασαφής υπόθεση, έλλειψη αποδεικτικών στοιχείων ή κακή ανάλυση.
- Included: Τέλος, οι μελέτες που πληρούν όλα τα κριτήρια επιλεξιμότητας περιλαμβάνονται στην ανασκόπηση. Το διάγραμμα δείχνει 70 μελέτες που συμπεριλήφθηκαν στην ανασκόπηση.

Για τον τομέα "Βελτίωση της ασφάλειας πληροφοριακών συστημάτων μέσω συστημάτων ειδοποίησης αξιολόγησης κινδύνου και μηχανικής μάθησης", μπορείτε να χρησιμοποιήσετε πολλές λέξεις-κλειδιά σε συνδυασμό για να αναζητήσετε σχετικές μελέτες στο Google Scholar και στο ResearchGate:

- Ασφάλεια Πληροφοριακών Συστημάτων (Information Systems Security)
- Συστήματα προειδοποίησης αξιολόγησης κινδύνου (Risk Assessment Alert Systems)
- Ασφάλεια μηχανικής μάθησης (Machine Learning Security)
- Διαχείριση Κινδύνων Κυβερνοασφάλειας (Cybersecurity Risk Management)
- AI στην αξιολόγηση κινδύνου (AI in Risk Assessment)
- Μηχανική Μάθηση στην Ασφάλεια Πληροφοριών (Machine Learning in Information Security)
- Συστήματα ανίχνευσης απειλών (Threat Detection Systems)
- Πληροφορική Ασφαλείας (Security Informatics)
- Προγνωστικά Αναλύσεις Ασφαλείας (Predictive Security Analytics)
- Ανάλυση Κινδύνων Ασφαλείας (Security Risk Analysis)

Χρησιμοποιώντας έναν συνδυασμό αυτών των λέξεων-κλειδιών και φιλτράρισμα με βάση τα τελευταία 10 χρόνια.

3.2 Συλλογή και Πηγές Δεδομένων

Παρακάτω αναφέρονται τα δεδομένα που συλλέχθηκαν και εκπαιδεύτηκαν στα πλαίσια ανάπτυξης των μοντέλων μηχανικής μάθησης [14]-[25].

1. **Server Configuration:**
    - Operating System: Windows, Linux, macOS
    - Server Version: Apache, Nginx, Microsoft IIS
    - Virtualization: Yes, No
2. **Network Security:**
    - Firewall Status: Enabled, Disabled
    - Intrusion Detection System (IDS): Installed, Not Installed
    - Network Segmentation: VLAN, Subnet, No Segmentation
3. **User Authentication:**
    - Password Policy: Strong, Moderate, Weak
    - Multi-factor Authentication: Enabled, Disabled
4. **Access Controls:**
    - Role-Based Access Control (RBAC): Implemented, Not Implemented
    - Least Privilege Principle: Followed, Not Followed
    - Access Control Lists (ACLs): Configured, Not Configured
5. **Security Software:**
    - Antivirus Status: Updated, Outdated
    - Anti-malware Tools: Installed, Not Installed
6. **Logs and Monitoring:**
    - Monitoring Tools: SIEM, Syslog, Custom
7. **Incident Response:**
    - Incident Response Plan: Developed, Not Developed
8. **Patch Management:**

- Patching Frequency: Daily (In days)
- Critical Patch Installation Time: Immediate, Scheduled

9. **Encryption:**
    - Data Encryption: Full Disk, File Level, Database Level
    - Communication Encryption: TLS, SSL
10. **Vulnerability Assessment:**
    - Regular Scans: Yes, No
    - Known Vulnerabilities: Patched, Unpatched
11. **Server Workload:**
    - Resource Utilization: Low, Moderate, High
    - Anomalous Behavior: Detected, Not Detected
12. **External Connections:**
    - Allowed IP Addresses: Whitelisted, Blacklisted
    - Suspicious Connections: Identified, Not Identified
13. **Historical Security Incidents:**
    - Previous Security Breaches: Yes, No
    - Severity of Past Incidents: Low, Moderate, High
14. **Machine Learning Target Variable:**
    - Risk Level: Low, Moderate, High (or binary: No Risk, Risk)

3.3 Επιλογή αλγορίθμων μηχανικής μάθησης

Στον τομέα της ασφάλειας των πληροφοριακών συστημάτων, αυτοί οι αλγόριθμοι επιλέγονται λόγω των διαφορετικών προσεγγίσεών τους στη μοντελοποίηση της πιθανότητας πιθανών κινδύνων [26]:

- Logistic Regression: Χρησιμοποιείται επειδή μοντελοποιεί αποτελεσματικά την πιθανότητα ενός δυαδικού αποτελέσματος, καθιστώντας το κατάλληλο για την

πρόβλεψη κινδύνου (κίνδυνος έναντι μη κινδύνου) με βάση συγκεκριμένες παραμέτρους όπως μοτίβα πρόσβασης στο σύστημα και βαθμολογίες ανωμαλιών.

- Random Forest Classifier: Αυτή η μέθοδος συνόλου επιλέγεται για την ευρωστία της και την ικανότητά της να χειρίζεται μη γραμμικές σχέσεις με τη συγκέντρωση πολλαπλών δέντρων αποφάσεων, οδηγώντας σε ακριβέστερες προβλέψεις σε πολύπλοκα σύνολα δεδομένων ασφαλείας.
- Classifier K-Neighbors: Το KNN χρησιμοποιείται για την απλότητα και την αποτελεσματικότητά του σε εργασίες ταξινόμησης όπου η εκτίμηση κινδύνου μπορεί να συναχθεί από την ομοιότητα μιας νέας παρουσίας με γνωστές περιπτώσεις στο σύνολο δεδομένων.
- Gaussian Naive Bayes: Το GaussianNB προτιμάται όταν η κατανομή χαρακτηριστικών θεωρείται κανονική, χρησιμοποιείται συχνά στην αξιολόγηση κινδύνου όπου οι παράμετροι ακολουθούν μια καμπύλη καμπάνας, βοηθώντας έτσι σε πιθανοτικές προβλέψεις.
- Bernoulli Naive Bayes: Το BernoulliNB είναι ιδανικό για δυαδικά ή boolean χαρακτηριστικά, καθιστώντας το κατάλληλο για σύνολα δεδομένων όπου οι παράμετροι έχουν τη μορφή δυαδικών εισόδων, όπως ερωτήσεις "ναι/όχι" σε λίστες ελέγχου κινδύνου.

3.4. Μετρήσεις αξιολόγησης

Στο πλαίσιο της ενίσχυσης της ασφάλειας των πληροφοριακών συστημάτων μέσω συστημάτων προειδοποίησης αξιολόγησης κινδύνου και μηχανικής μάθησης, η επιλογή των μετρήσεων είναι ζωτικής σημασίας για την αξιολόγηση της απόδοσης και της αξιοπιστίας των μοντέλων. Δείτε γιατί επιλέγονται συνήθως αυτές οι μετρήσεις:

- Train Score: Το Train Score ενός εκπαιδευμένου μοντέλου υποδεικνύει πόσο καλά ταιριάζει το μοντέλο στα δεδομένα εκπαίδευσης. Είναι μια αρχική ένδειξη της ικανότητας του μοντέλου να καταγράφει τα υποκείμενα μοτίβα στα δεδομένα στα οποία εκπαιδεύτηκε [27].
- Validation Score: Η βαθμολογία επικύρωσης είναι κρίσιμη για τον συντονισμό των υπερπαραμέτρων του μοντέλου χωρίς τη χρήση του συνόλου δοκιμής. Βοηθά στην αξιολόγηση του πόσο καλά το μοντέλο γενικεύεται σε νέα, αόρατα δεδομένα, τα οποία είναι ζωτικής σημασίας για ένα σύστημα που θα αντιμετωπίσει εξελισσόμενες απειλές ασφαλείας [28].

- Test Score: Η βαθμολογία δοκιμής ενός εκπαιδευμένου μοντέλου είναι το απόλυτο μέτρο για το πόσο καλά αποδίδει το μοντέλο σε εντελώς αόρατα δεδομένα. Αυτή η βαθμολογία είναι ενδεικτική της αποτελεσματικότητας του μοντέλου σε ένα πραγματικό σενάριο, όπου θα χρησιμοποιηθεί για την πρόβλεψη κινδύνων ασφαλείας.
- Μήτρα σύγχυσης (Confusion Matrix): Ένας πίνακας σύγχυσης προσφέρει μια λεπτομερή ανάλυση της απόδοσης του μοντέλου, δείχνοντας τον αριθμό των αληθινών θετικών, ψευδώς θετικών, αληθινών αρνητικών και ψευδώς αρνητικών.
- Accuracy: Αυτό μετρά τη συνολική ορθότητα του μοντέλου υπολογίζοντας τον λόγο των σωστά προβλεπόμενων περιπτώσεων προς τις συνολικές περιπτώσεις. Στα συστήματα ασφαλείας, η υψηλή ακρίβεια είναι σημαντική, αλλά δεν είναι η μόνη εκτίμηση, ειδικά εάν το κόστος των ψευδώς θετικών ή των ψευδώς αρνητικών είναι υψηλό [29].
- Precision: Το Precision μετρά την αναλογία των αληθινών θετικών προς όλα τα προβλεπόμενα θετικά. Η υψηλή ακρίβεια είναι ζωτικής σημασίας σε περιβάλλοντα ασφαλείας όπου το κόστος των ψευδών συναγερμών (ψευδώς θετικά) πρέπει να ελαχιστοποιηθεί, όπως στα συστήματα συναγερμών αξιολόγησης κινδύνου όπου οι πόροι για την αντιμετώπιση ειδοποιήσεων είναι περιορισμένοι.
- Recall: Γνωστή και ως ευαισθησία (Sensitivity), η ανάκληση μετρά την αναλογία των αληθινών θετικών προς όλα τα πραγματικά θετικά. Η υψηλή ανάκληση είναι απαραίτητη για την ασφάλεια, προκειμένου να διασφαλιστεί ότι το μοντέλο δεν παραλείπει τους πραγματικούς κινδύνους.
- F1-Score: Η βαθμολογία F1 είναι η αρμονική μέση ακρίβεια και ανάκληση. Χρησιμοποιείται επειδή εξισορροπεί την αντιστάθμιση μεταξύ ακρίβειας και ανάκλησης. Σε μια ρύθμιση ασφαλείας, η ισορροπία μεταξύ της μη απώλειας πραγματικών απειλών (υψηλή ανάκληση) και της μη εμφάνισης πολλών ψευδών συναγερμών (υψηλής ακρίβειας) είναι ζωτικής σημασίας [30].
- Specificity: Το Specificity μετρά την αναλογία των αληθινών αρνητικών προς όλα τα πραγματικά αρνητικά. Υποδεικνύει την ικανότητα του συστήματος να εντοπίζει σωστά την απουσία κινδύνου. Στην ασφάλεια των συστημάτων πληροφοριών, η υψηλή εξειδίκευση σημαίνει ότι το σύστημα είναι αποτελεσματικό στον εντοπισμό περιπτώσεων που δεν αποτελούν κίνδυνο, κάτι που είναι σημαντικό για την αποφυγή περιττών ενεργειών ή ερευνών.

4. Βασικές Αρχές Ασφάλειας Πληροφοριακών Συστημάτων

4.1 Απειλές και τρωτά σημεία

Η κατανόηση των απειλών και των τρωτών σημείων είναι θεμελιώδης για την ασφάλεια των συστημάτων πληροφοριών. Σε αυτή την ενότητα, θα διεξαχθεί μια λεπτομερής διερεύνηση διαφόρων τύπων απειλών και τρωτών σημείων μέσω μιας διεξοδικής βιβλιογραφικής ανασκόπησης. Οι βασικές πτυχές περιλαμβάνουν:

- Τοπίο απειλής: Το εξελισσόμενο τοπίο των απειλών στον κυβερνοχώρο, συμπεριλαμβανομένων κακόβουλου λογισμικού, phishing, ransomware και προηγμένων επίμονων απειλών. Κατανόηση των απειλών που στοχεύουν συστήματα πληροφοριών και τις τακτικές που χρησιμοποιούν [31].
- Κοινά τρωτά σημεία: Κοινά τρωτά σημεία στα συστήματα πληροφοριών, όπως τρωτά σημεία λογισμικού, εσφαλμένες διαμορφώσεις και τρωτά σημεία που σχετίζονται με τον άνθρωπο. Αυτά τα τρωτά σημεία μπορούν να εκμεταλλευτούν οι εισβολείς.
- Μέθοδοι εκτίμησης κινδύνου: Διερεύνηση μεθοδολογιών για την αξιολόγηση και την κατηγοριοποίηση απειλών και τρωτών σημείων. Αυτό περιλαμβάνει την κατανόηση του τρόπου με τον οποίο οι οργανισμοί μπορούν συστηματικά να εντοπίζουν, να αναλύουν και να ιεραρχούν τους πιθανούς κινδύνους για τα πληροφοριακά τους συστήματα.
- Αναδυόμενες απειλές: Ενήμεροι για τις αναδυόμενες απειλές και τα τρωτά σημεία. Η ανασκόπηση της βιβλιογραφίας θα πρέπει να υπογραμμίσει τις πρόσφατες τάσεις στις απειλές στον κυβερνοχώρο, παρέχοντας πληροφορίες για το πώς τα μέτρα ασφαλείας μπορούν να προσαρμοστούν για την αντιμετώπιση νέων προκλήσεων [32].
- Κακόβουλο λογισμικό: Κακόβουλο λογισμικό που έχει σχεδιαστεί για να διεισδύει και να βλάπτει συστήματα ή να κλέβει δεδομένα. Αυτό μπορεί να περιλαμβάνει ιούς, worms, Trojans και spyware.
- Phishing: Παραπλανητικές προσπάθειες εξαπάτησης ατόμων ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, συχνά παριστάνοντας ως αξιόπιστες οντότητες μέσω email ή ιστοτόπων.
- Ransomware: Κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί λύτρα για την απελευθέρωσή τους, αποτελώντας σημαντική απειλή για την ακεραιότητα των δεδομένων [33].

- Προηγμένες επίμονες απειλές (APTs): Συγκαλυμμένες και παρατεταμένες επιθέσεις στον κυβερνοχώρο από καλά χρηματοδοτούμενους αντιπάλους που στοχεύουν συγκεκριμένους οργανισμούς ή οντότητες.

Εικόνα 7: Βασικές αρχές ασφάλειας Πληροφοριακών Συστημάτων

4.2 Πολιτικές και πρακτικές ασφάλειας

Η καθιέρωση και η επιβολή πολιτικών και πρακτικών ασφαλείας είναι ζωτικής σημασίας για τη διατήρηση της ακεραιότητας και του απορρήτου των συστημάτων πληροφοριών. Αυτή η ενότητα θα εμβαθύνει στα ακόλουθα:

Ανάπτυξη Πολιτικών Ασφαλείας

Διαδικασία δημιουργίας ολοκληρωμένων πολιτικών ασφάλειας που ευθυγραμμίζονται με τους στόχους του οργανισμού. Αυτό περιλαμβάνει πολιτικές που σχετίζονται με το χειρισμό δεδομένων, τον έλεγχο πρόσβασης, την απόκριση συμβάντων και άλλα.

Η ανάπτυξη ολοκληρωμένων πολιτικών ασφάλειας αποτελεί ακρογωνιαίο λίθο της αποτελεσματικής ασφάλειας συστημάτων πληροφοριών. Αυτή η διαδικασία περιλαμβάνει τη δημιουργία ενός συνόλου κατευθυντήριων γραμμών και κανόνων που ευθυγραμμίζονται με τους στόχους και τις απαιτήσεις ασφάλειας του οργανισμού. Αυτές οι πολιτικές καλύπτουν ένα ευρύ φάσμα τομέων, συμπεριλαμβανομένου του χειρισμού δεδομένων, του ελέγχου πρόσβασης, της απόκρισης περιστατικών και άλλων.

Η ανάπτυξη πολιτικών ασφαλείας ξεκινά με την αξιολόγηση των μοναδικών αναγκών και των τρωτών σημείων του οργανισμού. Απαιτεί τη συμβολή διαφόρων ενδιαφερομένων, συμπεριλαμβανομένων των επαγγελματιών πληροφορικής, των νομικών εμπειρογνωμόνων και

της διοίκησης. Οι πολιτικές θα πρέπει να είναι προσαρμοσμένες για την αντιμετώπιση συγκεκριμένων απειλών και κινδύνων που αντιμετωπίζει ο οργανισμός. Για παράδειγμα, οι πολιτικές διαχείρισης δεδομένων μπορεί να καθορίζουν τον τρόπο με τον οποίο θα πρέπει να κρυπτογραφούνται ή να αποθηκεύονται ευαίσθητες πληροφορίες, οι πολιτικές ελέγχου πρόσβασης μπορεί να ορίζουν ποιος έχει πρόσβαση σε κρίσιμα συστήματα και οι πολιτικές αντιμετώπισης περιστατικών μπορεί να περιγράφουν τα βήματα που πρέπει να ληφθούν σε περίπτωση παραβίασης ασφάλειας [34].

Εκπαίδευση και ευαισθητοποίηση χρηστών

Σημασία των προγραμμάτων εκπαίδευσης και ευαισθητοποίησης των χρηστών για την προώθηση μιας κουλτούρας με συνείδηση της ασφάλειας σε έναν οργανισμό. Κατανόηση για το πώς οι ενημερωμένοι και μορφωμένοι χρήστες συμβάλλουν στη συνολική ασφάλεια.

Τα προγράμματα εκπαίδευσης και ευαισθητοποίησης των χρηστών διαδραματίζουν καθοριστικό ρόλο στην προώθηση μιας κουλτούρας με συνείδηση της ασφάλειας σε έναν οργανισμό. Αυτά τα προγράμματα έχουν σχεδιαστεί για να εκπαιδεύουν τους υπαλλήλους και τους χρήστες σχετικά με τις βέλτιστες πρακτικές ασφάλειας στον κυβερνοχώρο, τις απειλές και τους ρόλους τους στη διατήρηση της ασφάλειας.

Η σημασία της εκπαίδευσης των χρηστών δεν μπορεί να υπερεκτιμηθεί. Οι καλά ενημερωμένοι και μορφωμένοι χρήστες είναι η πρώτη γραμμή άμυνας ενάντια σε διάφορες απειλές στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων phishing και της κοινωνικής μηχανικής [35]. Τα εκπαιδευτικά προγράμματα καλύπτουν συνήθως θέματα όπως η υγιεινή του κωδικού πρόσβασης, η αναγνώριση ύποπτων email, οι συνήθειες ασφαλούς περιήγησης και ο σωστός χειρισμός ευαίσθητων δεδομένων.

Η δημιουργία μιας κουλτούρας με συνείδηση της ασφάλειας απαιτεί συνεχείς προσπάθειες. Οι οργανισμοί θα πρέπει να ενημερώνουν τακτικά το εκπαιδευτικό υλικό ώστε να αντικατοπτρίζουν τις εξελισσόμενες απειλές και τεχνολογίες. Επιπλέον, θα πρέπει να ενθαρρύνουν τους υπαλλήλους να αναφέρουν τα περιστατικά ασφαλείας αμέσως και να παρέχουν σαφή κανάλια για να το κάνουν.

Μηχανισμοί Ελέγχου Πρόσβασης

Εξέταση σε μηχανισμούς και πρακτικές ελέγχου πρόσβασης, συμπεριλαμβανομένου του ελέγχου πρόσβασης βάσει ρόλων (RBAC) και της αρχής του ελάχιστου προνομίου. Συνεπώς, κατανόηση για το πώς αυτοί οι μηχανισμοί συμβάλλουν στον περιορισμό της μη εξουσιοδοτημένης πρόσβασης.

Οι μηχανισμοί ελέγχου πρόσβασης είναι θεμελιώδεις για τη διασφάλιση ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε κρίσιμα συστήματα και δεδομένα. Αυτοί οι

μηχανισμοί καθορίζουν τον τρόπο με τον οποίο χορηγούνται, διαχειρίζονται και παρακολουθούνται τα δικαιώματα πρόσβασης σε έναν οργανισμό [36].

Μια κοινή προσέγγιση είναι ο Έλεγχος Πρόσβασης βάσει Ρόλων (RBAC), ο οποίος αναθέτει συγκεκριμένους ρόλους στους χρήστες με βάση τις ευθύνες τους εντός του οργανισμού. Κάθε ρόλος έχει προκαθορισμένα δικαιώματα πρόσβασης, διασφαλίζοντας ότι τα άτομα έχουν πρόσβαση μόνο στους πόρους που απαιτούνται για τις λειτουργίες της εργασίας τους. Το RBAC βοηθά στον περιορισμό της πιθανής ζημιάς που προκαλείται από εσωτερικές απειλές και μη εξουσιοδοτημένη πρόσβαση.

Η αρχή του ελάχιστου προνομίου (PoLP) είναι μια άλλη κρίσιμη έννοια. Υπαγορεύει ότι οι χρήστες πρέπει να έχουν το ελάχιστο επίπεδο πρόσβασης που απαιτείται για την εκτέλεση των καθηκόντων τους. Αυτό μειώνει την επιφάνεια επίθεσης και ελαχιστοποιεί τον πιθανό αντίκτυπο των παραβιάσεων της ασφάλειας.

Οι αποτελεσματικοί μηχανισμοί ελέγχου πρόσβασης συχνά ενσωματώνονται με συστήματα διαχείρισης ταυτότητας, επιβάλλοντας κανόνες ελέγχου ταυτότητας και εξουσιοδότησης. Οι τακτικές αναθεωρήσεις των αδειών πρόσβασης είναι απαραίτητες για τη διατήρηση της αρχής των ελάχιστων προνομίων και την προσαρμογή στις μεταβαλλόμενες οργανωτικές ανάγκες [37].

Σχέδια αντιμετώπισης περιστατικών

Ανάπτυξη και εφαρμογή σχεδίων αντιμετώπισης περιστατικών. Κατανόηση της σημασίας της ύπαρξης ενός καλά καθορισμένου σχεδίου για τον μετριασμό και την αποτελεσματική αντιμετώπιση περιστατικών ασφαλείας.

Τα σχέδια αντιμετώπισης συμβάντων αποτελούν ζωτικό συστατικό της στρατηγικής ασφαλείας οποιουδήποτε οργανισμού. Αυτά τα σχέδια περιγράφουν τα βήματα που πρέπει να ληφθούν υπόψη ή παραβίαση της ασφάλειας, με στόχο την ελαχιστοποίηση της ζημιάς και διακοπής.

Η ανάπτυξη και η εφαρμογή σχεδίων αντιμετώπισης περιστατικών περιλαμβάνει πολλά βασικά στοιχεία. Οι οργανισμοί πρέπει να εντοπίζουν πιθανά συμβάντα ασφαλείας, να κατηγορούν τη σοβαρότητά τους και να ορίζουν σαφείς διαδικασίες για περιορισμό, εκρίζωση και ανάκτηση. Αυτά τα σχέδια που πρέπει επίσης να προσδιορίσουν τους ρόλους και τις ευθύνες των ατόμων που εμπλέκονται στην προσπάθεια απόκρισης.

Η επικαιρότητα είναι κρίσιμη για την απόκριση σε περιστατικά. Τα σχέδια περιλαμβάνουν συχνά προκαθορισμένα κανάλια επικοινωνίας για να διασφαλίσουν ότι τα σχετικά μέρη ενημερώνονται έγκαιρα. Αυτό μπορεί να περιλαμβάνει ειδοποίηση ομάδων πληροφορικής, νομικών τμημάτων, εξωτερικών εμπειρογνωμόνων ασφαλείας, ακόμη και υπηρεσιών επιβολής του νόμου, ανάλογα με τη σοβαρότητα του συμβάντος [38].

Οι τακτικές δοκιμές και οι ασκήσεις των σχεδίων αντιμετώπισης περιστατικών βοηθούν τους οργανισμούς να βελτιώσουν τις διαδικασίες τους και να διασφαλίσουν ότι το προσωπικό είναι εξοικειωμένο με τους ρόλους του κατά τη διάρκεια ενός περιστατικού. Ο στόχος είναι να ελαχιστοποιηθεί ο αντίκτυπος των παραβιάσεων της ασφάλειας και να επιστρέψουμε γρήγορα στις κανονικές λειτουργίες, ενώ παράλληλα μαθαίνουμε από το περιστατικό για την πρόληψη των μελλοντικών περιστατικών.

4.3 Συμμόρφωση και Κανονισμοί

Η συμμόρφωση με τα πρότυπα και τους κανονισμούς συμμόρφωσης είναι απαραίτητη για την ασφάλεια των πληροφοριακών συστημάτων. Αυτή η ενότητα θα πρέπει να καλύπτει τις ακόλουθες πτυχές:

Επισκόπηση των πλαισίων συμμόρφωσης

Επισκόπηση των βασικών πλαισίων και προτύπων συμμόρφωσης, όπως ISO/IEC 27001, NIST, GDPR, HIPAA κ.λπ. Κατανόηση σχετικά με τις απαιτήσεις που επιβάλλονται από αυτά τα πλαίσια.

Τα πλαίσια και τα πρότυπα συμμόρφωσης είναι βασικές κατευθυντήριες γραμμές που ακολουθούν οι οργανισμοί για να διασφαλίσουν ότι οι πρακτικές ασφάλειας, απορρήτου και διαχείρισης δεδομένων των συστημάτων πληροφοριών τους πληρούν τις αναγνωρισμένες βιομηχανικές και νομικές απαιτήσεις. Μια ολοκληρωμένη επισκόπηση των βασικών πλαισίων συμμόρφωσης είναι ζωτικής σημασίας σε αυτό το πλαίσιο [39].

Μερικά από τα γνωστά πλαίσια και πρότυπα συμμόρφωσης περιλαμβάνουν ISO/IEC 27001, NIST (Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας), GDPR (Γενικός Κανονισμός Προστασίας Δεδομένων), HIPAA (Health Insurance Portability and Accountability Act) και άλλα. Κάθε ένα από αυτά τα πλαίσια παρέχει συγκεκριμένες κατευθυντήριες γραμμές και απαιτήσεις που πρέπει να τηρούν οι οργανισμοί σε διάφορους τομείς ασφάλειας συστημάτων πληροφοριών.

Η κατανόηση αυτών των πλαισίων περιλαμβάνει τη διερεύνηση των βασικών αρχών τους και των ειδικών ελέγχων που επιβάλλουν. Για παράδειγμα, το ISO/IEC 27001 εστιάζει στα συστήματα διαχείρισης ασφάλειας πληροφοριών, ενώ ο GDPR δίνει έμφαση στην προστασία δεδομένων και την ιδιωτικότητα. Το NIST παρέχει ένα ολοκληρωμένο σύνολο προτύπων κυβερνοασφάλειας και το HIPAA είναι προσαρμοσμένο για τη βιομηχανία υγειονομικής περίθαλψης [40]. Η εις βάθος κατανόηση αυτών των πλαισίων βοηθά τους

οργανισμούς να ευθυγραμμίσουν τις πρακτικές ασφαλείας τους με τις βέλτιστες πρακτικές του κλάδου και τις νομικές απαιτήσεις.

Νομικό και ρυθμιστικό τοπίο

Το νομικό και ρυθμιστικό τοπίο που διέπει την ασφάλεια των συστημάτων πληροφοριών. Αυτό περιλαμβάνει την κατανόηση των νομικών υποχρεώσεων και των συνεπειών που σχετίζονται με παραβιάσεις δεδομένων και μη συμμόρφωση.

Εικόνα 8: Συμμόρφωση και Κανονισμοί

Το νομικό και ρυθμιστικό τοπίο που διέπει την ασφάλεια των πληροφοριακών συστημάτων είναι πολύπλοκο και συνεχώς εξελίσσεται. Περιλαμβάνει ένα ευρύ φάσμα νόμων, κανονισμών και οδηγιών τόσο σε εθνικό όσο και σε διεθνές επίπεδο.
Οι βασικές πτυχές αυτού του τοπίου περιλαμβάνουν:

- Νόμοι για την Προστασία Δεδομένων: Κατανόηση των νόμων περί προστασίας δεδομένων όπως ο GDPR και των επιπτώσεων του χειρισμού προσωπικών δεδομένων. Αυτοί οι νόμοι απαιτούν από τους οργανισμούς να προστατεύουν τα δικαιώματα απορρήτου των ατόμων και να αναφέρουν έγκαιρα παραβιάσεις δεδομένων [41].
- Ειδικοί κανονισμοί κλάδου: Αναγνώριση ειδικών κανονισμών του κλάδου, όπως HIPAA για την υγειονομική περίθαλψη ή PCI DSS (Payment Card Industry Data Security Standard) για το χειρισμό δεδομένων πιστωτικών καρτών.

- Νομοθεσία για την ασφάλεια στον κυβερνοχώρο: Ενημερωθείτε σχετικά με νόμους και οδηγίες που σχετίζονται με την κυβερνοασφάλεια που επιβάλλουν απαιτήσεις ασφάλειας και υποχρεώσεις αναφοράς.

Η μη συμμόρφωση με αυτές τις νομικές υποχρεώσεις μπορεί να έχει σοβαρές συνέπειες, όπως πρόστιμα, νομικές ενέργειες και ζημιά στη φήμη. Ως εκ τούτου, οι οργανισμοί πρέπει να γνωρίζουν καλά τις νομικές πτυχές της ασφάλειας των πληροφοριακών συστημάτων και να καθιερώνουν διαδικασίες για τη διασφάλιση της συμμόρφωσης.

Προκλήσεις συμμόρφωσης

Προκλήσεις που αντιμετωπίζουν οι οργανισμοί στη διατήρηση της συμμόρφωσης. Αυτό μπορεί να περιλαμβάνει ζητήματα που σχετίζονται με την πολυπλοκότητα, την αλλαγή των ρυθμιστικών τοπίων και την ανάγκη για συνεχή παρακολούθηση και προσαρμογή.
Η διατήρηση της συμμόρφωσης μπορεί να είναι ένα δύσκολο έργο για τους οργανισμούς λόγω πολλών προκλήσεων. Αυτές οι προκλήσεις μπορεί να περιλαμβάνουν [42]:

- Πολυπλοκότητα: Οι απαιτήσεις συμμόρφωσης μπορεί να είναι περίπλοκες και πολύπλευρες, ιδιαίτερα για οργανισμούς που δραστηριοποιούνται σε πολλαπλές δικαιοδοσίες ή κλάδους με μοναδικές ρυθμιστικές απαιτήσεις.
- Αλλαγή ρυθμιστικών τοπίων: Οι κανονισμοί υπόκεινται σε συχνές ενημερώσεις και αλλαγές. Οι οργανισμοί πρέπει να παραμείνουν σε επαγρύπνηση για να διασφαλίσουν ότι οι πρακτικές τους παραμένουν ευθυγραμμισμένες με τις πιο πρόσφατες απαιτήσεις.
- Κατανομή πόρων: Η επίτευξη και η διατήρηση της συμμόρφωσης απαιτεί σημαντικούς πόρους, συμπεριλαμβανομένου χρόνου, προσωπικού και οικονομικών επενδύσεων.
- Συνεχής παρακολούθηση και προσαρμογή: Η συμμόρφωση είναι μια διαρκής προσπάθεια. Οι οργανισμοί πρέπει να παρακολουθούν συνεχώς τις πρακτικές τους, να προσαρμόζονται στις αλλαγές των κανονισμών και να αντιμετωπίζουν εγκαίρως τυχόν κενά συμμόρφωσης.

Η αντιμετώπιση αυτών των προκλήσεων περιλαμβάνει μια προορατική προσέγγιση που συνδυάζει ρυθμιστική εμπειρογνωμοσύνη, αφοσιωμένες ομάδες συμμόρφωσης και χρήση τεχνολογίας για τον εξορθολογισμό των διαδικασιών συμμόρφωσης.

Ενσωμάτωση της συμμόρφωσης στις πρακτικές ασφάλειας

Στρατηγικές για την απρόσκοπτη ενσωμάτωση των απαιτήσεων συμμόρφωσης στις καθημερινές πρακτικές ασφάλειας. Κατανόηση για το πώς οι οργανισμοί μπορούν να οικοδομήσουν μια κουλτούρα ασφάλειας προσανατολισμένη στη συμμόρφωση [43].

Για την επιτυχή πλοήγηση στις απαιτήσεις συμμόρφωσης, οι οργανισμοί πρέπει να τις ενσωματώσουν απρόσκοπτα στις καθημερινές πρακτικές ασφαλείας τους. Αυτό συνεπάγεται τη δημιουργία μιας κουλτούρας συμμόρφωσης όπου όλοι οι εργαζόμενοι κατανοούν και τηρούν τους σχετικούς κανονισμούς. Οι στρατηγικές ένταξης περιλαμβάνουν:

- Εκπαίδευση και ευαισθητοποίηση: Διασφάλιση ότι οι εργαζόμενοι σε όλα τα επίπεδα γνωρίζουν τις απαιτήσεις συμμόρφωσης και κατανοούν τον ρόλο τους στη διατήρηση της συμμόρφωσης.
- Τεκμηρίωση και τήρηση αρχείων: Τήρηση ενδελεχών αρχείων των προσπαθειών συμμόρφωσης, των εκτιμήσεων κινδύνου και των ελέγχων ασφαλείας για την απόδειξη της συμμόρφωσης κατά τη διάρκεια ελέγχων ή ερευνών.
- Αυτοματοποιημένα Εργαλεία Συμμόρφωσης: Αξιοποίηση τεχνολογίας, όπως λογισμικό διαχείρισης συμμόρφωσης, για τον εξορθολογισμό των διαδικασιών συμμόρφωσης, την παρακολούθηση της τήρησης και τη δημιουργία απαραίτητων αναφορών.
- Τακτικοί έλεγχοι και αξιολογήσεις: Διεξαγωγή τακτικών εσωτερικών και εξωτερικών ελέγχων για την αξιολόγηση της συμμόρφωσης και τον εντοπισμό τομέων προς βελτίωση.

Ένα καλά ενοποιημένο πρόγραμμα συμμόρφωσης όχι μόνο διασφαλίζει ότι οι οργανισμοί πληρούν τις κανονιστικές απαιτήσεις, αλλά επίσης ενισχύει τη συνολική ασφάλεια των συστημάτων πληροφοριών ενσταλάσσοντας μια κουλτούρα επαγρύπνησης και υπευθυνότητας σε ολόκληρο τον οργανισμό.

5. Εκτίμηση Κινδύνων σε Πληροφοριακά Συστήματα

5.1 Αναγνώριση κινδύνου

Μέθοδοι αναγνώρισης

Οι μέθοδοι αναγνώρισης είναι ζωτικής σημασίας για την αναγνώριση κινδύνων και πιθανών απειλών στα συστήματα πληροφοριών. Αυτές οι μέθοδοι περιλαμβάνουν συστηματικές προσεγγίσεις, λίστες ελέγχου και μεθοδολογίες που βοηθούν τους οργανισμούς να εντοπίζουν αποτελεσματικά τους κινδύνους. Είναι απαραίτητη μια ολοκληρωμένη έρευνα για διάφορες μεθόδους ταυτοποίησης [44].

- Συστηματικές Προσεγγίσεις: Οι οργανισμοί συχνά χρησιμοποιούν συστηματικές προσεγγίσεις για τον εντοπισμό των κινδύνων. Αυτό περιλαμβάνει τη διεξαγωγή διεξοδικών αξιολογήσεων των πληροφοριακών συστημάτων, συμπεριλαμβανομένων των στοιχείων, των διαδικασιών και των τρωτών σημείων τους. Μέθοδοι όπως η σάρωση ευπάθειας, οι δοκιμές διείσδυσης και οι εκτιμήσεις κινδύνου είναι συστηματικές τεχνικές που χρησιμοποιούνται για την αποκάλυψη πιθανών απειλών.
- Λίστες ελέγχου: Οι λίστες ελέγχου παρέχουν έναν δομημένο τρόπο εντοπισμού κοινών κινδύνων και κινδύνων [45]. Οι οργανισμοί μπορούν να αναπτύξουν λίστες ελέγχου προσαρμοσμένες στα συγκεκριμένα περιβάλλοντα και τις απαιτήσεις του κλάδου τους. Αυτές οι λίστες ελέγχου καλύπτουν πτυχές όπως ο έλεγχος πρόσβασης, ο χειρισμός δεδομένων, τα τρωτά σημεία λογισμικού και άλλα.
- Μεθοδολογίες: Αναγνωρισμένες μεθοδολογίες, όπως το STRIDE (Πλαστεύσεις, Παραβίαση, Απόρριψη, Αποκάλυψη Πληροφοριών, Άρνηση Υπηρεσίας, Ανύψωση Προνομίων), χρησιμοποιούνται για την ταξινόμηση και τον εντοπισμό απειλών συστηματικά. Αυτές οι μεθοδολογίες βοηθούν τους οργανισμούς να κατηγοριοποιήσουν και να ιεραρχήσουν τους κινδύνους με βάση τον πιθανό αντίκτυπο και την πιθανότητα τους [46].

Ταξινόμηση των κινδύνων

Η ταξινόμηση των κινδύνων στα συστήματα πληροφοριών είναι ένα κρίσιμο βήμα στη διαδικασία αξιολόγησης κινδύνου. Οι κίνδυνοι μπορούν να κατηγοριοποιηθούν με βάση

διάφορα χαρακτηριστικά για την καλύτερη κατανόηση της φύσης και της πιθανής επίδρασής τους.

- Εξωτερικοί έναντι εσωτερικών κινδύνων: Οι κίνδυνοι μπορούν να ταξινομηθούν σε εξωτερικούς ή εσωτερικούς. Οι εξωτερικοί κίνδυνοι προέρχονται από πηγές εκτός του οργανισμού, όπως οι επιθέσεις στον κυβερνοχώρο ή οι φυσικές καταστροφές. Οι εσωτερικοί κίνδυνοι προέρχονται από το εσωτερικό του οργανισμού και μπορεί να περιλαμβάνουν ακούσιες ενέργειες από υπαλλήλους ή αστοχίες συστήματος.
- Σκόπιμες εναντίον ακούσιων απειλών: Οι κίνδυνοι μπορούν περαιτέρω να κατηγοριοποιηθούν ως σκόπιμες ή ακούσιες απειλές. Οι σκόπιμες απειλές περιλαμβάνουν κακόβουλες ενέργειες, όπως κυβερνοεπιθέσεις ή εσωτερικές απειλές. Οι ακούσιες απειλές προκύπτουν από ανθρώπινο λάθος, ευπάθειες συστήματος ή απρόβλεπτες περιστάσεις [47].
- Φυσικοί έναντι ανθρωπογενείς κίνδυνοι: Οι κίνδυνοι μπορούν επίσης να ταξινομηθούν ως φυσικοί ή ανθρωπογενείς κίνδυνοι. Οι φυσικοί κίνδυνοι περιλαμβάνουν γεγονότα όπως σεισμούς, πλημμύρες και καταιγίδες. Οι ανθρωπογενείς κίνδυνοι περιλαμβάνουν γεγονότα που προκαλούνται από τον άνθρωπο, όπως παραβιάσεις δεδομένων, ευπάθειες λογισμικού και ατυχήματα.

Η κατανόηση αυτών των ταξινομήσεων είναι ζωτικής σημασίας για την προσαρμογή των στρατηγικών μετριασμού του κινδύνου για την αποτελεσματική αντιμετώπιση συγκεκριμένων τύπων κινδύνων.

Εικόνα 9: Αναγνώριση κινδύνου

Ανθρώπινοι παράγοντες

Οι ανθρώπινοι παράγοντες διαδραματίζουν σημαντικό ρόλο στον προσδιορισμό των κινδύνων στα συστήματα πληροφοριών. Η κατανόηση του τρόπου με τον οποίο οι ανθρώπινες ενέργειες, τόσο εσκεμμένες όσο και ακούσιες, συμβάλλουν στους κινδύνους είναι απαραίτητη [48].

- Ανθρώπινο σφάλμα: Το ανθρώπινο σφάλμα μπορεί να οδηγήσει σε τρωτά σημεία και συμβάντα ασφαλείας. Τα κοινά σφάλματα περιλαμβάνουν εσφαλμένες ρυθμίσεις παραμέτρων, τυχαία έκθεση δεδομένων και αδυναμία τήρησης των πρωτοκόλλων ασφαλείας. Ο εντοπισμός περιοχών όπου είναι πιθανό να συμβεί ανθρώπινο λάθος είναι ζωτικής σημασίας για τον μετριασμό του κινδύνου.
- Κακόβουλη πρόθεση: Η κακόβουλη πρόθεση, συχνά από έμπιστους, αποτελεί σημαντική απειλή. Ο εντοπισμός δεικτών εσωτερικών απειλών και η εφαρμογή μηχανισμών παρακολούθησης μπορεί να βοηθήσει στην ανίχνευση και την πρόληψη σκόπιμης βλάβης στα συστήματα πληροφοριών.
- Κοινωνική Μηχανική: Οι τακτικές κοινωνικής μηχανικής, όπως το phishing και το προσχήματα, βασίζονται στον χειρισμό της ανθρώπινης συμπεριφοράς. Η αναγνώριση των ενδείξεων των προσπαθειών κοινωνικής μηχανικής και η εκπαίδευση των εργαζομένων σχετικά με το πώς να ανταποκριθούν είναι ουσιαστικής σημασίας για τον εντοπισμό των κινδύνων [49].

Ενοποίηση με Πλαίσια Ασφαλείας

Ο προσδιορισμός κινδύνου είναι βασικό συστατικό ευρύτερων πλαισίων και προτύπων ασφαλείας. Η διερεύνηση του τρόπου με τον οποίο η αναγνώριση κινδύνου ευθυγραμμίζεται με αυτά τα πλαίσια και τις απαιτήσεις συμμόρφωσης είναι απαραίτητη για ολοκληρωμένες πρακτικές ασφάλειας.

- Πλαίσια διαχείρισης κινδύνου: Ο προσδιορισμός κινδύνου είναι αναπόσπαστο μέρος πλαισίων διαχείρισης κινδύνου όπως το ISO/IEC 27001 και το NIST SP 800-53 [50]. Αυτά τα πλαίσια παρέχουν κατευθυντήριες γραμμές για τον εντοπισμό, την αξιολόγηση και τον μετριασμό των κινδύνων στα συστήματα πληροφοριών.
- Απαιτήσεις συμμόρφωσης: Η συμμόρφωση με ειδικούς κανονισμούς του κλάδου, όπως ο GDPR ή το HIPAA, απαιτεί συχνά από τους οργανισμούς να διεξάγουν αναγνώριση κινδύνου ως μέρος των πρακτικών ασφαλείας τους [51]. Η

ενσωμάτωση της αναγνώρισης κινδύνου στις προσπάθειες συμμόρφωσης διασφαλίζει την τήρηση τόσο των νομικών όσο και των υποχρεώσεων ασφάλειας.

- Συνεχής Βελτίωση: Οι οργανισμοί θα πρέπει να υιοθετήσουν μια κουλτούρα συνεχούς βελτίωσης όταν πρόκειται για τον προσδιορισμό των κινδύνων. Αυτό περιλαμβάνει την τακτική αναθεώρηση και ενημέρωση των μεθόδων αναγνώρισης κινδύνου για την ευθυγράμμιση με τις εξελισσόμενες απειλές, τις τεχνολογίες και τις οργανωτικές αλλαγές. Περιλαμβάνει επίσης μάθηση από προηγούμενα συμβάντα για τη βελτίωση των διαδικασιών αναγνώρισης κινδύνου.
- Διερευνώντας διεξοδικά αυτές τις πτυχές της αναγνώρισης κινδύνων, οι οργανισμοί μπορούν να προστατεύσουν καλύτερα τα συστήματα πληροφοριών τους και να μειώσουν τον πιθανό αντίκτυπο των απειλών για την ασφάλεια.

5.2 Ανάλυση κινδύνου

Ποσοτική έναντι Ποιοτικής Ανάλυσης

Οι ποσοτικές και ποιοτικές αναλύσεις κινδύνου είναι δύο διαφορετικές προσεγγίσεις που χρησιμοποιούνται στην αξιολόγηση κινδύνου, η καθεμία από τις οποίες προσφέρει τα πλεονεκτήματά της και τα κατάλληλα πλαίσια.

- Ποσοτική ανάλυση: Αυτή η προσέγγιση περιλαμβάνει την ανάθεση αριθμητικών τιμών σε διάφορες πτυχές των κινδύνων, όπως η πιθανότητα εμφάνισης, οι πιθανές επιπτώσεις και οι οικονομικές επιπτώσεις. Στοχεύει στην παροχή μιας ποσοτικής εκτίμησης του κινδύνου, που συνήθως μετράται σε όρους χρηματικής αξίας ή αριθμητικών πιθανοτήτων [52]. Η ποσοτική ανάλυση είναι ιδιαίτερα χρήσιμη όταν υπάρχουν διαθέσιμα ακριβή δεδομένα και μετρήσεις. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για την αξιολόγηση οικονομικών κινδύνων, όπως η πιθανή απώλεια λόγω παραβίασης της ασφάλειας στον κυβερνοχώρο. Περιλαμβάνει τεχνικές όπως προσομοιώσεις Monte Carlo και υπολογισμούς αναμενόμενης νομισματικής αξίας (EMV).
- Ποιοτική Ανάλυση: Η ποιοτική ανάλυση, από την άλλη πλευρά, δεν βασίζεται σε αριθμητικά δεδομένα αλλά στην κρίση των ειδικών και στις υποκειμενικές εκτιμήσεις. Περιλαμβάνει την κατηγοριοποίηση των κινδύνων με βάση τον αντίκτυπό τους, την πιθανότητα και άλλα ποιοτικά χαρακτηριστικά. Αυτή η προσέγγιση είναι πολύτιμη όταν τα ποσοτικά δεδομένα είναι σπάνια ή όταν

αντιμετωπίζουμε σύνθετους, αβέβαιους ή αναδυόμενους κινδύνους [53]. Η ποιοτική ανάλυση συχνά χρησιμοποιεί πίνακες κινδύνου, θερμικούς χάρτες ή συστήματα βαθμολόγησης κινδύνου για την κατηγοριοποίηση και την ιεράρχηση των κινδύνων. Παρέχει ποιοτική κατανόηση των κινδύνων και βοηθά στον εντοπισμό ζητημάτων υψηλής προτεραιότητας που απαιτούν προσοχή.

Η επιλογή μεταξύ ποσοτικής και ποιοτικής ανάλυσης εξαρτάται από τη διαθεσιμότητα των δεδομένων, την πολυπλοκότητα του τοπίου κινδύνου και τους συγκεκριμένους στόχους της αξιολόγησης κινδύνου. Στην πράξη, οι οργανισμοί μπορούν να χρησιμοποιούν συνδυασμό και των δύο μεθόδων για να επιτύχουν μια ολιστική άποψη των κινδύνων.

Μέθοδοι συλλογής δεδομένων:

Η συλλογή δεδομένων είναι ένα κρίσιμο βήμα στην ανάλυση κινδύνου, καθώς παρέχει τη βάση για την αξιολόγηση και την αποτελεσματική αξιολόγηση των κινδύνων.

- Δεδομένα ιστορικού περιστατικού: Η ανάλυση δεδομένων ιστορικού περιστατικού είναι απαραίτητη για την κατανόηση προηγούμενων παραβιάσεων ασφαλείας, των τρωτών σημείων εκμετάλλευσης και των επιπτώσεών τους. Αυτά τα δεδομένα βοηθούν στον εντοπισμό επαναλαμβανόμενων μοτίβων και τάσεων που μπορούν να ενημερώσουν τις εκτιμήσεις κινδύνου [54].
- Τροφοδοσίες ευφυΐας απειλών: Οι ροές πληροφοριών απειλών παρέχουν πληροφορίες σε πραγματικό ή σχεδόν πραγματικό χρόνο σχετικά με αναδυόμενες απειλές, τρωτά σημεία και τακτικές επίθεσης. Η ενσωμάτωση πληροφοριών απειλών στην ανάλυση κινδύνου διασφαλίζει ότι οι αξιολογήσεις λαμβάνουν υπόψη τους τρέχοντες και τους εξελισσόμενους κινδύνους.
- Έρευνες και συνεντεύξεις: Οι έρευνες και οι συνεντεύξεις με βασικά ενδιαφερόμενα μέρη, ειδικούς σε θέματα και χρήστες του συστήματος μπορούν να αποφέρουν πολύτιμα ποιοτικά δεδομένα σχετικά με τους κινδύνους και τις ευπάθειες. Αυτές οι μέθοδοι μπορούν να αποκαλύψουν ιδέες που μόνο τα ποσοτικά δεδομένα μπορεί να μην καταγράψουν.
- Τεχνικές αξιολογήσεις: Οι τεχνικές αξιολογήσεις, όπως η σάρωση ευπάθειας και οι δοκιμές διείσδυσης, παρέχουν συγκεκριμένα δεδομένα σχετικά με τα τρωτά σημεία που υπάρχουν στα συστήματα πληροφοριών ενός οργανισμού. Αυτά τα δεδομένα είναι ζωτικής σημασίας για την κατανόηση των πιθανών αδυναμιών που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς [55].
- Οι αποτελεσματικές μέθοδοι συλλογής δεδομένων θα πρέπει να προσαρμόζονται στις ειδικές ανάγκες του οργανισμού και στη φύση των κινδύνων που

αξιολογούνται. Ο συνδυασμός πολλαπλών πηγών δεδομένων διασφαλίζει μια ολοκληρωμένη και ακριβή ανάλυση κινδύνου.

Αξιολόγηση της ευπάθειας

Η αξιολόγηση τρωτότητας αποτελεί αναπόσπαστο μέρος της ανάλυσης κινδύνου, συμβάλλοντας στην αξιολόγηση των επιπτώσεων και της πιθανότητας των πιθανών κινδύνων. Προσδιορισμός τρωτών σημείων: Οι αξιολογήσεις ευπάθειας περιλαμβάνουν τον εντοπισμό αδυναμιών και τρωτών σημείων στα συστήματα πληροφοριών ενός οργανισμού. Αυτή η διαδικασία περιλαμβάνει τον εντοπισμό τρωτών σημείων λογισμικού, εσφαλμένων διαμορφώσεων και άλλων πιθανών σημείων εισόδου για εισβολείς.

- Εκτίμηση της πιθανότητας εκμετάλλευσης: Μόλις εντοπιστούν τα τρωτά σημεία, αξιολογείται η πιθανότητα εκμετάλλευσης τους. Αυτή η αξιολόγηση λαμβάνει υπόψη παράγοντες όπως η ευκολία εκμετάλλευσης, η παρουσία γνωστών εκμεταλλεύσεων και τα μέτρα ασφαλείας του οργανισμού [56].
- Εκτίμηση επιπτώσεων: Οι αξιολογήσεις ευπάθειας λαμβάνουν επίσης υπόψη τον πιθανό αντίκτυπο των τρωτών σημείων που χρησιμοποιούνται. Αυτός ο αντίκτυπος μπορεί να κυμαίνεται από παραβιάσεις δεδομένων και διακοπές λειτουργίας του συστήματος έως οικονομικές απώλειες και ζημιές στη φήμη.
- Η ενσωμάτωση των αξιολογήσεων τρωτότητας στην ανάλυση κινδύνου επιτρέπει στους οργανισμούς να ιεραρχούν και να αντιμετωπίζουν τις ευπάθειες που αποτελούν τις πιο σημαντικές απειλές. Βοηθά στη λήψη τεκμηριωμένων αποφάσεων σχετικά με τις στρατηγικές μετριασμού του κινδύνου και την κατανομή των πόρων.

Ανάλυση Σεναρίου

Η ανάλυση σεναρίων είναι μια πολύτιμη τεχνική που χρησιμοποιείται στην αξιολόγηση κινδύνου για τη διερεύνηση και την κατανόηση των πιθανών συνεπειών διαφορετικών κινδύνων.

- Δημιουργία υποθετικών σεναρίων: Η ανάλυση σεναρίων περιλαμβάνει τη δημιουργία υποθετικών σεναρίων που αντιπροσωπεύουν διάφορα συμβάντα κινδύνου. Αυτά τα σενάρια λαμβάνουν υπόψη παράγοντες όπως ο τύπος της

απειλής [57], ο φορέας επίθεσης, ο πιθανός αντίκτυπος και η απόκριση του οργανισμού.

- Αξιολόγηση Συνεπειών: Αξιολογώντας αυτά τα σενάρια, οι οργανισμοί μπορούν να εκτιμήσουν τις πιθανές συνέπειες διαφορετικών κινδύνων. Αυτό περιλαμβάνει την κατανόηση των οικονομικών, λειτουργικών και επιπτώσεων στη φήμη που θα μπορούσαν να προκύψουν από ένα συγκεκριμένο γεγονός κινδύνου.
- Ενημέρωση για τη λήψη αποφάσεων: Η ανάλυση σεναρίων ενημερώνει τη λήψη αποφάσεων παρέχοντας έναν δομημένο τρόπο διερεύνησης του φάσματος των δυνατοτήτων και των σχετικών κινδύνων τους. Βοηθά τους οργανισμούς να προσδιορίσουν ποιοι κίνδυνοι απαιτούν άμεση προσοχή και ποιοι μπορούν να αντιμετωπιστούν με τους υπάρχοντες ελέγχους.

Η ανάλυση σεναρίων είναι ιδιαίτερα χρήσιμη για πολύπλοκους ή αβέβαιους κινδύνους, επιτρέποντας στους οργανισμούς να προετοιμαστούν και να προγραμματίσουν για μια ποικιλία πιθανών αποτελεσμάτων [58]. Ενισχύει την επίγνωση των κινδύνων και βοηθά στην ανάπτυξη αποτελεσματικών στρατηγικών μετριασμού του κινδύνου.

5.3 Αξιολόγηση Κινδύνου

Μοντέλα πίνακα κινδύνου

Τα μοντέλα μήτρας κινδύνου χρησιμοποιούνται ευρέως στην αξιολόγηση κινδύνου για την κατηγοριοποίηση και την ιεράρχηση των κινδύνων με βάση τον αντίκτυπο και την πιθανότητα τους. Αυτά τα μοντέλα παρέχουν μια οπτική αναπαράσταση των κινδύνων, επιτρέποντας στους οργανισμούς να εστιάσουν τους πόρους τους στην αντιμετώπιση των πιο κρίσιμων απειλών.

Εικόνα 10: Αξιολόγηση Κινδύνου

- Στοιχεία ενός πίνακα κινδύνου: Ένας τυπικός πίνακας κινδύνου αποτελείται από δύο κύρια στοιχεία: αντίκτυπο και πιθανότητα. Ο αντίκτυπος αναφέρεται στις πιθανές συνέπειες ή τη ζημιά που θα μπορούσε να προκαλέσει ένα συμβάν κινδύνου, ενώ η πιθανότητα αντιπροσωπεύει την πιθανότητα εμφάνισης του γεγονότος κινδύνου. Αυτά τα στοιχεία συχνά χωρίζονται σε διακριτά επίπεδα ή κλίμακες, όπως χαμηλό, μεσαίο και υψηλό.
- Κατηγοριοποίηση κινδύνων: Οι κίνδυνοι απεικονίζονται στον πίνακα κινδύνου με βάση τον εκτιμώμενο αντίκτυπο και την πιθανότητά τους. Ο προκύπτων πίνακας χωρίζεται σε διαφορετικές ζώνες ή κατηγορίες κινδύνου, όπως χαμηλού κινδύνου, μέτριου κινδύνου και υψηλού κινδύνου. Αυτή η κατηγοριοποίηση βοηθά τους οργανισμούς να ιεραρχήσουν τους κινδύνους για περαιτέρω αξιολόγηση και προσπάθειες μετριασμού.
- Πλεονεκτήματα των μοντέλων πίνακα κινδύνου: Τα μοντέλα μήτρας κινδύνου προσφέρουν πολλά πλεονεκτήματα. Παρέχουν έναν σαφή και διαισθητικό τρόπο οπτικοποίησης των κινδύνων, καθιστώντας ευκολότερο για τους ενδιαφερόμενους να κατανοήσουν τη σημασία τους [59]. Επιπλέον, διευκολύνουν την επικοινωνία κινδύνου κατηγοριοποιώντας τους κινδύνους σε σημαντικές ομάδες. Οι οργανισμοί μπορούν να χρησιμοποιήσουν μοντέλα μήτρας κινδύνου για να εντοπίσουν κρίσιμους κινδύνους που απαιτούν άμεση προσοχή και να κατανείμουν τους πόρους ανάλογα.

Εκτίμηση δυναμικού κινδύνου

Η δυναμική αξιολόγηση κινδύνου είναι μια προσέγγιση που αναγνωρίζει τη διαρκώς μεταβαλλόμενη φύση του τοπίου της απειλής και του οργανωτικού πλαισίου. Σε αντίθεση με τις στατικές αξιολογήσεις, η δυναμική αξιολόγηση κινδύνου περιλαμβάνει συνεχή παρακολούθηση και επαναξιολόγηση των κινδύνων για προσαρμογή στις εξελισσόμενες συνθήκες.

- Συνεχής παρακολούθηση: Στη δυναμική αξιολόγηση κινδύνου, οι οργανισμοί παρακολουθούν συνεχώς το περιβάλλον τους για αλλαγές στο τοπίο απειλών, την τεχνολογία, τους κανονισμούς και τις επιχειρηματικές λειτουργίες. Αυτή η συνεχής παρακολούθηση διασφαλίζει ότι οι αξιολογήσεις κινδύνου παραμένουν ενημερωμένες και αντικατοπτρίζουν τις τρέχουσες συνθήκες [60].
- Απόκριση στην αλλαγή: Όταν εντοπίζονται αλλαγές στο τοπίο κινδύνου ή στο οργανωτικό πλαίσιο, η δυναμική αξιολόγηση κινδύνου ωθεί τους οργανισμούς να επαναξιολογήσουν τους κινδύνους και να προσαρμόσουν ανάλογα τις στρατηγικές μετριασμού του κινδύνου. Αυτή η προσαρμοστικότητα είναι ζωτικής σημασίας για την αντιμετώπιση αναδυόμενων απειλών και τρωτών σημείων.
- Ενσωμάτωση με την απόκριση σε περιστατικά: Η δυναμική αξιολόγηση κινδύνου συνδέεται στενά με τις πρακτικές αντιμετώπισης περιστατικών. Οι οργανισμοί που χρησιμοποιούν δυναμική αξιολόγηση είναι καλύτερα προετοιμασμένοι να ανταποκριθούν γρήγορα σε συμβάντα ασφαλείας, καθώς έχουν ήδη εξετάσει διάφορα σενάρια κινδύνου και επιλογές μετριασμού [61].
- Η δυναμική αξιολόγηση κινδύνου είναι απαραίτητη για οργανισμούς που δραστηριοποιούνται σε δυναμικά και ταχέως εξελισσόμενα περιβάλλοντα, όπως ο τομέας της κυβερνοασφάλειας. Προωθεί την προληπτική διαχείριση κινδύνων και επιτρέπει στους οργανισμούς να βρίσκονται μπροστά από τις αναδυόμενες απειλές.

Ενοποίηση με Επιχειρηματικούς Στόχους

Η αποτελεσματική αξιολόγηση κινδύνου ευθυγραμμίζεται με τους ευρύτερους επιχειρηματικούς στόχους και τους οργανισμούς. Διασφαλίζει ότι οι προσπάθειες διαχείρισης κινδύνου υποστηρίζουν τη συνολική αποστολή και τις διαδικασίες λήψης αποφάσεων.

- Στρατηγική ευθυγράμμιση: Οι εκτιμήσεις κινδύνου πρέπει να διεξάγονται με σαφή κατανόηση των στρατηγικών στόχων του οργανισμού. Αυτή η ευθυγράμμιση

διασφαλίζει ότι οι εντοπισμένοι κίνδυνοι σχετίζονται με την αποστολή και το όραμα του οργανισμού.

- Κατανομή πόρων: Οι αξιολογήσεις κινδύνου βοηθούν τους οργανισμούς να κατανέμουν αποτελεσματικά τους πόρους. Εντοπίζοντας κινδύνους υψηλής προτεραιότητας που ευθυγραμμίζονται με τους επιχειρηματικούς στόχους [62], οι οργανισμοί μπορούν να διαθέσουν πόρους για την αντιμετώπιση των πιο κρίσιμων απειλών.
- Ενημερωμένη Λήψη Αποφάσεων: Οι εκτιμήσεις κινδύνου παρέχουν στους λήπτες αποφάσεων πολύτιμες γνώσεις σχετικά με τον πιθανό αντίκτυπο των κινδύνων στους στόχους του οργανισμού. Αυτές οι πληροφορίες επιτρέπουν την τεκμηριωμένη λήψη αποφάσεων, συμπεριλαμβανομένων αποφάσεων που σχετίζονται με την αποδοχή κινδύνου, τον μετριασμό του κινδύνου και τη μεταφορά κινδύνου.
- Συμμόρφωση και Κανονισμοί: Πολλές βιομηχανίες υπόκεινται σε ρυθμιστικές απαιτήσεις που επιβάλλουν αξιολογήσεις κινδύνου. Η ενσωμάτωση της αξιολόγησης κινδύνου με τις προσπάθειες συμμόρφωσης διασφαλίζει ότι ο οργανισμός πληροί τις νομικές υποχρεώσεις ενώ παράλληλα ευθυγραμμίζεται με τους επιχειρηματικούς στόχους.
- Η ευθυγράμμιση με τους επιχειρηματικούς στόχους διασφαλίζει ότι οι εκτιμήσεις κινδύνου δεν εκτελούνται μεμονωμένα, αλλά αποτελούν αναπόσπαστο κομμάτι της συνολικής στρατηγικής και των λειτουργιών του οργανισμού.

Κοινοποίηση ευρημάτων κινδύνου

Η αποτελεσματική επικοινωνία των ευρημάτων κινδύνου είναι ζωτικής σημασίας για να διασφαλιστεί ότι τα ενδιαφερόμενα μέρη έχουν σαφή κατανόηση των εντοπισμένων κινδύνων και των συνεπειών τους [63].

- Συμμετοχή ενδιαφερομένων: Οι αξιολογήσεις κινδύνου περιλαμβάνουν πολλούς ενδιαφερόμενους, συμπεριλαμβανομένων στελεχών, διευθυντών, τεχνικών εμπειρογνωμόνων και νομικών ομάδων και ομάδων συμμόρφωσης. Η αποτελεσματική επικοινωνία διασφαλίζει ότι όλοι οι ενδιαφερόμενοι συμμετέχουν και ενημερώνονται σε όλη τη διαδικασία.
- Σαφής αναφορά: Τα ευρήματα κινδύνου πρέπει να αναφέρονται με σαφή και συνοπτικό τρόπο. Αυτό περιλαμβάνει την παροχή λεπτομερειών σχετικά με τους

εντοπισμένους κινδύνους, τον πιθανό αντίκτυπό τους, την πιθανότητα και τις προτεινόμενες στρατηγικές μετριασμού. Τα οπτικά βοηθήματα, όπως διαγράμματα και γραφήματα, μπορούν να ενισχύσουν την κατανόηση [64].

- Προσαρμοσμένα μηνύματα: Διαφορετικοί ενδιαφερόμενοι μπορεί να έχουν διαφορετικά επίπεδα τεχνικής εξειδίκευσης και ενδιαφερόντων. Η προσαρμογή της επικοινωνίας των ευρημάτων κινδύνου στις συγκεκριμένες ανάγκες και ανησυχίες κάθε κοινού διασφαλίζει ότι το μήνυμα είναι σχετικό και εφαρμόσιμο.
- Συστάσεις για τον μετριασμό του κινδύνου: Μαζί με τον εντοπισμό των κινδύνων, οι αξιολογήσεις κινδύνου θα πρέπει να προσφέρουν συστάσεις για τον μετριασμό του κινδύνου. Η κοινοποίηση αυτών των συστάσεων βοηθά τους ενδιαφερόμενους να κατανοήσουν τα βήματα που απαιτούνται για την αποτελεσματική αντιμετώπιση των εντοπισθέντων κινδύνων [65].
- Η αποτελεσματική επικοινωνία κινδύνου προάγει τη συνεργασία και τη λήψη τεκμηριωμένων αποφάσεων. Εξουσιοδοτεί τους οργανισμούς να λαμβάνουν προληπτικά μέτρα για τη διαχείριση και τον μετριασμό των κινδύνων, ενισχύοντας τελικά την ανθεκτικότητα και τη στάση ασφαλείας τους.

5.4 Στρατηγικές μετριασμού του κινδύνου

Εφαρμογή ελέγχου

Η εφαρμογή του ελέγχου είναι ένα κρίσιμο βήμα για τον μετριασμό των κινδύνων που εντοπίζονται κατά τη διαδικασία αξιολόγησης κινδύνου. Οι οργανισμοί χρησιμοποιούν μια ποικιλία τύπων ελέγχου για την αποτελεσματική διαχείριση των κινδύνων και αυτοί οι έλεγχοι μπορούν να κατηγοριοποιηθούν ευρέως σε τεχνικούς, διαδικαστικούς και ελέγχους που βασίζονται σε πολιτικές.

- Τεχνικοί έλεγχοι: Οι τεχνικοί έλεγχοι περιλαμβάνουν τη χρήση τεχνολογίας για τη διαφύλαξη συστημάτων πληροφοριών και δεδομένων. Παραδείγματα περιλαμβάνουν τείχη προστασίας, συστήματα ανίχνευσης εισβολής (IDS), λογισμικό προστασίας από ιούς, κρυπτογράφηση, στοιχεία ελέγχου πρόσβασης και μηχανισμούς ελέγχου ταυτότητας. Αυτοί οι έλεγχοι επικεντρώνονται στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των στοιχείων ενεργητικού των πληροφοριών [66]. Η επιλογή και η ανάπτυξη τεχνικών

ελέγχων εξαρτάται από τους συγκεκριμένους κινδύνους και τα τρωτά σημεία που έχουν εντοπιστεί.

- Διαδικαστικοί έλεγχοι: Οι διαδικαστικοί έλεγχοι περιλαμβάνουν πολιτικές, διαδικασίες και κατευθυντήριες γραμμές που υπαγορεύουν πώς οι εργαζόμενοι και οι χρήστες πρέπει να συμπεριφέρονται και να αλληλεπιδρούν με τα πληροφοριακά συστήματα. Συχνά περιλαμβάνουν προγράμματα εκπαίδευσης και ευαισθητοποίησης, σχέδια αντιμετώπισης περιστατικών, διαδικασίες διαχείρισης αλλαγών και εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια. Οι διαδικαστικοί έλεγχοι είναι απαραίτητοι για τη διασφάλιση της τήρησης των πολιτικών ασφαλείας και την εκπαίδευση των εργαζομένων σχετικά με τις βέλτιστες πρακτικές ασφάλειας.
- Έλεγχοι που βασίζονται σε πολιτικές: Οι έλεγχοι που βασίζονται σε πολιτικές προέρχονται από πολιτικές και οδηγίες ασφάλειας του οργανισμού. Αυτοί οι έλεγχοι θεσπίζουν το γενικό πλαίσιο ασφαλείας εντός του οποίου λειτουργούν οι τεχνικοί και διαδικαστικοί έλεγχοι. Οι πολιτικές ασφαλείας καθορίζουν τους στόχους ασφαλείας, τις ευθύνες και τις απαιτήσεις συμμόρφωσης του οργανισμού. Καθοδηγούν την ανάπτυξη και την εφαρμογή ειδικών ελέγχων και χρησιμεύουν ως βάση για τις προσπάθειες διαχείρισης κινδύνου.

Η αποτελεσματική εφαρμογή ελέγχου περιλαμβάνει μια ισορροπημένη προσέγγιση που λαμβάνει υπόψη το συγκεκριμένο τοπίο κινδύνου του οργανισμού, τις κανονιστικές απαιτήσεις και τους διαθέσιμους πόρους. Οι έλεγχοι θα πρέπει να επανεξετάζονται και να ενημερώνονται τακτικά για την αντιμετώπιση εξελισσόμενων απειλών και τρωτών σημείων [67].

Διαχείριση υπολειπόμενου κινδύνου

Ο υπολειπόμενος κίνδυνος αναφέρεται στο επίπεδο κινδύνου που παραμένει μετά την εφαρμογή των μέτρων ελέγχου. Είναι σημαντικό για τους οργανισμούς να διαχειρίζονται τους υπολειπόμενους κινδύνους για να διασφαλίσουν ότι ευθυγραμμίζονται με την ανοχή κινδύνου και την όρεξη του οργανισμού για κινδύνους.

- Αποδοχή Υπολειπόμενου Κινδύνου: Σε ορισμένες περιπτώσεις, οι οργανισμοί μπορεί να επιλέξουν να αποδεχτούν τους υπολειπόμενους κινδύνους. Αυτή η απόφαση λαμβάνεται συνήθως όταν το υπόλοιπο επίπεδο κινδύνου θεωρείται αποδεκτό και εντός της ανοχής κινδύνου του οργανισμού. Η αποδοχή μπορεί να βασίζεται σε ανάλυση κόστους-οφέλους ή σε προσδιορισμό ότι ο περαιτέρω μετριασμός δεν είναι εφικτός ή πρακτικός.

- Μεταφορά κινδύνων: Οι οργανισμοί μπορούν να μεταφέρουν υπολειπόμενους κινδύνους σε τρίτους, όπως ασφαλιστικούς φορείς ή παρόχους υπηρεσιών, μέσω συμβατικών συμφωνιών. Οι μηχανισμοί μεταφοράς κινδύνου, όπως τα ασφαλιστήρια συμβόλαια, μπορούν να συμβάλουν στον μετριασμό των οικονομικών ζημιών που σχετίζονται με συγκεκριμένους κινδύνους, παρέχοντας ένα επίπεδο προστασίας από ανεπιθύμητα συμβάντα [68].
- Περαιτέρω μετριασμός: Όταν οι υπολειπόμενοι κίνδυνοι υπερβαίνουν τα αποδεκτά επίπεδα ή κρίνονται μη αποδεκτοί, οι οργανισμοί μπορούν να επιλέξουν περαιτέρω μέτρα μετριασμού του κινδύνου. Αυτό θα μπορούσε να περιλαμβάνει την ενίσχυση των υφιστάμενων ελέγχων, την εφαρμογή πρόσθετων διασφαλίσεων ή την αναθεώρηση των πολιτικών και διαδικασιών ασφαλείας. Ο στόχος είναι να μειωθεί ο υπολειπόμενος κίνδυνος σε αποδεκτό επίπεδο.
- Η αποτελεσματική διαχείριση υπολειπόμενου κινδύνου διασφαλίζει ότι οι οργανισμοί λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τον τρόπο αντιμετώπισης των υπολειπόμενων κινδύνων, λαμβάνοντας υπόψη τον πιθανό αντίκτυπό τους και την ανοχή του οργανισμού σε κινδύνους.

Ενσωμάτωση με την απόκριση περιστατικού

Οι στρατηγικές μετριασμού του κινδύνου και τα σχέδια αντιμετώπισης συμβάντων συνδέονται στενά, με τη διαχείριση κινδύνου να διαδραματίζει προληπτικό ρόλο στην πρόληψη συμβάντων και η απόκριση σε περιστατικά να χρησιμεύει ως αντιδραστικό μέτρο όταν συμβαίνουν συμβάντα.

- Προληπτικά μέτρα: Οι στρατηγικές μετριασμού του κινδύνου περιλαμβάνουν προληπτικά μέτρα που στοχεύουν στην πρόληψη συμβάντων ασφαλείας. Αυτά τα μέτρα μπορεί να περιλαμβάνουν αξιολογήσεις ευπάθειας, διαχείριση ενημερώσεων κώδικα, έλεγχο πρόσβασης, εκπαίδευση εργαζομένων και μηχανισμούς ανίχνευσης απειλών [69]. Εντοπίζοντας και αντιμετωπίζοντας τα τρωτά σημεία και τις απειλές προτού μπορέσουν να γίνουν αντικείμενο εκμετάλλευσης, οι οργανισμοί μειώνουν την πιθανότητα συμβάντων ασφαλείας.
- Αντιδραστικά μέτρα: Τα σχέδια αντιμετώπισης περιστατικών περιγράφουν τις διαδικασίες που πρέπει να ακολουθούνται όταν συμβαίνουν περιστατικά ασφαλείας. Αυτά τα σχέδια περιγράφουν λεπτομερώς τον τρόπο με τον οποίο οι οργανισμοί θα εντοπίσουν, θα ανταποκριθούν και θα ανακτήσουν από περιστατικά

όπως παραβιάσεις δεδομένων, μολύνσεις από κακόβουλο λογισμικό ή παραβιάσεις του συστήματος. Η αποτελεσματική απόκριση συμβάντων ελαχιστοποιεί τον αντίκτυπο των συμβάντων και διευκολύνει την ταχεία επιστροφή στις κανονικές λειτουργίες.

- Συνεχής βελτίωση: Η ενσωμάτωση του μετριασμού του κινδύνου και της αντιμετώπισης περιστατικών συνεπάγεται συνεχείς προσπάθειες βελτίωσης. Οι οργανισμοί αξιολογούν τακτικά την αποτελεσματικότητα των ελέγχων τους και των διαδικασιών αντιμετώπισης περιστατικών [70]. Τα διδάγματα από προηγούμενα συμβάντα χρησιμοποιούνται για τη βελτίωση τόσο των στρατηγικών διαχείρισης κινδύνου όσο και των σχεδίων αντιμετώπισης περιστατικών, ενισχύοντας τη συνολική στάση ασφαλείας.

Η στενή ευθυγράμμιση της διαχείρισης κινδύνου και της αντιμετώπισης συμβάντων διασφαλίζει μια ολιστική προσέγγιση στην ασφάλεια στον κυβερνοχώρο. Επιτρέπει στους οργανισμούς να μειώνουν προληπτικά τους κινδύνους και να ανταποκρίνονται αποτελεσματικά σε συμβάντα ασφαλείας όταν συμβαίνουν.

Συνεχής παρακολούθηση και βελτίωση

Η συνεχής παρακολούθηση και η βελτίωση είναι θεμελιώδεις για την αποτελεσματική διαχείριση κινδύνων. Τα τοπία κινδύνου εξελίσσονται και οι οργανισμοί πρέπει να προσαρμόσουν ανάλογα τις στρατηγικές μετριασμού του κινδύνου.

- Τακτική επανεκτίμηση: Οι οργανισμοί θα πρέπει να επανεκτιμούν τακτικά το τοπίο κινδύνου για να εντοπίζουν αλλαγές σε απειλές, ευπάθειες και επιχειρηματικές λειτουργίες. Αυτό περιλαμβάνει τη διεξαγωγή περιοδικών αξιολογήσεων κινδύνου για την αξιολόγηση της αποτελεσματικότητας των υφιστάμενων ελέγχων και τον εντοπισμό νέων κινδύνων.
- Προσαρμογή των προσπαθειών μετριασμού: Με βάση τα αποτελέσματα των συνεχιζόμενων αξιολογήσεων κινδύνου, οι οργανισμοί μπορούν να προσαρμόσουν τις προσπάθειές τους για τον μετριασμό του κινδύνου. Αυτό μπορεί να περιλαμβάνει ενίσχυση ή τροποποίηση υφιστάμενων ελέγχων, εφαρμογή νέων τεχνολογιών ή αναθεώρηση πολιτικών και διαδικασιών ασφαλείας για την αντιμετώπιση αναδυόμενων κινδύνων [71].
- Βρόχος ανατροφοδότησης: Η συνεχής παρακολούθηση και η βελτίωση δημιουργούν έναν βρόχο ανατροφοδότησης που ενημερώνει τη λήψη αποφάσεων. Τα διδάγματα από προηγούμενα συμβάντα, οι έλεγχοι ασφάλειας και οι

αξιολογήσεις συμβάλλουν στη βελτίωση των στρατηγικών διαχείρισης κινδύνου. Αυτή η επαναληπτική διαδικασία ενισχύει την ικανότητα ενός οργανισμού να προσαρμόζεται στις εξελισσόμενες απειλές και να διατηρεί μια ισχυρή στάση ασφαλείας.

Η συνεχής παρακολούθηση και η βελτίωση αποτελούν βασικά στοιχεία ενός ώριμου προγράμματος διαχείρισης κινδύνου. Διασφαλίζουν ότι οι οργανισμοί παραμένουν σε επαγρύπνηση στον εντοπισμό και τον μετριασμό των κινδύνων, συμβάλλοντας στη μακροπρόθεσμη ασφάλεια και ανθεκτικότητα.

6. Μηχανική Μάθηση στην Εκτίμηση Κινδύνων

6.1 Προεπεξεργασία δεδομένων

Η προεπεξεργασία δεδομένων είναι ένα κομβικό στάδιο στην εφαρμογή των τεχνικών μηχανικής μάθησης για την αξιολόγηση κινδύνων στην ασφάλεια των συστημάτων πληροφοριών. Χρησιμεύει ως το θεμέλιο πάνω στο οποίο χτίζονται ακριβείς και αξιόπιστες προβλέψεις κινδύνου. Αυτή η ενότητα εμβαθύνει στις κρίσιμες πτυχές της προεπεξεργασίας δεδομένων, τονίζοντας τη σημασία της για τη διασφάλιση της ποιότητας και της χρηστικότητας των δεδομένων που χρησιμοποιούνται για την αξιολόγηση κινδύνου βάσει μηχανικής μάθησης.

Σημασία της προεπεξεργασίας δεδομένων

Πριν ξεκινήσετε την ανάπτυξη μοντέλων μηχανικής μάθησης για την αξιολόγηση κινδύνου, είναι επιτακτική ανάγκη να αντιμετωπιστούν διάφορες προκλήσεις που σχετίζονται με δεδομένα που μπορούν να επηρεάσουν σημαντικά την ακρίβεια και την αποτελεσματικότητα των μοντέλων. Η προεπεξεργασία δεδομένων είναι η διαδικασία καθαρισμού, μετατροπής και οργάνωσης ακατέργαστων δεδομένων σε μορφή κατάλληλη για ανάλυση [60]. Η σημασία του δεν μπορεί να υπερεκτιμηθεί, καθώς η ποιότητα των δεδομένων εισόδου επηρεάζει άμεσα την ποιότητα των προβλέψεων του μοντέλου.

Καθαρισμός δεδομένων

Τα δεδομένα που συλλέγονται για την αξιολόγηση κινδύνου συχνά περιέχουν τιμές που λείπουν, ακραίες τιμές, ασυνέπειες και σφάλματα. Ο καθαρισμός δεδομένων περιλαμβάνει τον εντοπισμό και τη διόρθωση αυτών των ζητημάτων για να διασφαλιστεί ότι το σύνολο δεδομένων είναι αξιόπιστο και συνεπές [61]. Κατά τη διάρκεια αυτής της φάσης εφαρμόζονται στρατηγικές όπως ο καταλογισμός (αντικατάσταση τιμών που λείπουν), ο εντοπισμός και ο χειρισμός ακραίων τιμών και η διόρθωση σφαλμάτων.

Επιλογή χαρακτηριστικών και μηχανική

Τα αποτελεσματικά μοντέλα αξιολόγησης κινδύνου βασίζονται σε σχετικά και ενημερωτικά χαρακτηριστικά. Η επιλογή χαρακτηριστικών είναι η διαδικασία αναγνώρισης και διατήρησης των πιο σχετικών χαρακτηριστικών από το σύνολο δεδομένων, απορρίπτοντας εκείνα που δεν συμβάλλουν στην εργασία πρόβλεψης [62]. Η μηχανική χαρακτηριστικών περιλαμβάνει τη δημιουργία νέων χαρακτηριστικών ή τη μετατροπή υπαρχόντων για να ενισχύσει την

ικανότητα του μοντέλου να καταγράφει πρότυπα κινδύνου. Στο πλαίσιο της ασφάλειας συστημάτων πληροφοριών, οι σχετικές δυνατότητες μπορεί να περιλαμβάνουν διαμορφώσεις διακομιστή, ρυθμίσεις ασφάλειας δικτύου και δεδομένα ιστορικού περιστατικού [63].

Κανονικοποίηση και κλιμάκωση δεδομένων

Η κανονικοποίηση και η κλιμάκωση είναι τεχνικές που χρησιμοποιούνται για να φέρουν τα χαρακτηριστικά δεδομένων σε μια συνεπή κλίμακα. Αυτό είναι ιδιαίτερα σημαντικό όταν έχουμε να κάνουμε με χαρακτηριστικά που έχουν διαφορετικές μονάδες ή μεγέθη [64]. Η κανονικοποίηση διασφαλίζει ότι κάθε χαρακτηριστικό συμβάλλει αναλογικά στη διαδικασία εκμάθησης του μοντέλου, αποτρέποντας ορισμένα χαρακτηριστικά από το να κυριαρχούν σε άλλα λόγω της εγγενούς τους κλίμακας.

Χειρισμός μη ισορροπημένων δεδομένων

Στην ασφάλεια συστημάτων πληροφοριών, τα μη ισορροπημένα σύνολα δεδομένων είναι κοινά, όπου μια κατηγορία (π.χ. "Χωρίς κίνδυνος") υπερτερεί σημαντικά της άλλης κατηγορίας (π.χ. "Κίνδυνος"). Η αντιμετώπιση της ανισορροπίας της τάξης είναι ζωτικής σημασίας για να αποτραπεί η προκατάληψη του μοντέλου προς την πλειοψηφική τάξη [65]. Τεχνικές όπως η υπερδειγματοληψία της κλάσης μειοψηφίας, η υποδειγματοληψία της κλάσης πλειοψηφίας ή η χρήση μεθόδων παραγωγής συνθετικών δεδομένων μπορούν να εφαρμοστούν για την εξισορρόπηση του συνόλου δεδομένων.

Διαχωρισμός δεδομένων

Μόλις ολοκληρωθεί η προεπεξεργασία δεδομένων, το σύνολο δεδομένων χωρίζεται συνήθως σε σύνολα εκπαίδευσης, επικύρωσης και δοκιμών. Το σετ εκπαίδευσης χρησιμοποιείται για την εκπαίδευση του μοντέλου μηχανικής εκμάθησης, το σύνολο επικύρωσης βοηθά στον συντονισμό των υπερπαραμέτρων και στην αξιολόγηση της απόδοσης του μοντέλου κατά την ανάπτυξη και το σύνολο δοκιμών αξιολογεί την ικανότητα γενίκευσης του τελικού μοντέλου [66].

Συνοπτικά, η Ενότητα 6.1 τονίζει ότι η προεπεξεργασία δεδομένων είναι ένας κρίσιμος πρόδρομος για την ανάπτυξη μοντέλων μηχανικής μάθησης για την αξιολόγηση κινδύνου στην ασφάλεια συστημάτων πληροφοριών. Περιλαμβάνει καθαρισμό δεδομένων, επιλογή χαρακτηριστικών και μηχανική, κανονικοποίηση, χειρισμό μη ισορροπημένων δεδομένων και κατάλληλο διαχωρισμό δεδομένων [67]. Διασφαλίζοντας ότι τα δεδομένα που χρησιμοποιούνται για τη μοντελοποίηση είναι υψηλής ποιότητας και κατάλληλα προετοιμασμένα, οι οργανισμοί μπορούν να βελτιώσουν την ακρίβεια και την αξιοπιστία των

μοντέλων αξιολόγησης κινδύνου, συμβάλλοντας τελικά στη βελτίωση των μέτρων ασφαλείας και στην πρόληψη συμβάντων.

6.2 Μηχανική Χαρακτηριστικών

Στην επιδίωξη της ενίσχυσης της ασφάλειας των συστημάτων πληροφοριών μέσω της αξιολόγησης κινδύνου βάσει μηχανικής μάθησης, η Ενότητα 6.2 εμβαθύνει στην κρίσιμη πτυχή των μηχανικών χαρακτηριστικών από δεδομένα. Αυτή η διαδικασία περιλαμβάνει τη μετατροπή ακατέργαστων δεδομένων σε σημαντικά χαρακτηριστικά που μπορούν να χρησιμοποιηθούν αποτελεσματικά από μοντέλα μηχανικής μάθησης για να διακρίνουν μοτίβα, να αξιολογήσουν τους κινδύνους και να κάνουν προβλέψεις.

Τεχνικά χαρακτηριστικά για την αξιολόγηση κινδύνου [68]

Τα αποτελεσματικά μοντέλα αξιολόγησης κινδύνου βασίζονται σε μεγάλο βαθμό στην επιλογή και τη μηχανική των χαρακτηριστικών που ενσωματώνουν τις βασικές πτυχές της ασφάλειας συστημάτων πληροφοριών. Αυτά τα χαρακτηριστικά χρησιμεύουν ως δομικά στοιχεία για αλγόριθμους μηχανικής μάθησης, επιτρέποντάς τους να καταγράφουν περίπλοκες σχέσεις και αποχρώσεις μέσα στα δεδομένα.

Εξαγωγή χαρακτηριστικών

Η εξαγωγή χαρακτηριστικών είναι ένα θεμελιώδες συστατικό των τεχνικών χαρακτηριστικών. Περιλαμβάνει τον εντοπισμό σχετικών πληροφοριών από ακατέργαστα δεδομένα και τη μετατροπή τους σε μορφή που μπορεί να χρησιμοποιηθεί για ανάλυση [69]. Στο πλαίσιο της ασφάλειας συστημάτων πληροφοριών, αυτό μπορεί να περιλαμβάνει την εξαγωγή λεπτομερειών διαμόρφωσης διακομιστή, μοτίβων κίνησης δικτύου ή στατιστικών στοιχείων ιστορικού συμβάντων.

Μετασχηματισμός χαρακτηριστικών

Ο μετασχηματισμός χαρακτηριστικών περιλαμβάνει διάφορες τεχνικές για την αλλαγή της αναπαράστασης των δεδομένων. Αυτό μπορεί να περιλαμβάνει κλιμάκωση, κωδικοποίηση κατηγορικών μεταβλητών ή εφαρμογή μαθηματικών μετασχηματισμών για να γίνουν τα δεδομένα πιο κατάλληλα για αλγόριθμους μηχανικής μάθησης [70]. Για παράδειγμα, η μετατροπή κατηγορικών χαρακτηριστικών όπως το "Λειτουργικό Σύστημα" σε αριθμητικές

τιμές ή η εφαρμογή λογαριθμικών μετασχηματισμών σε λοξές κατανομές μπορεί να βελτιώσει την απόδοση του μοντέλου.

Μείωση διαστάσεων

Τα σύνολα δεδομένων ασφαλείας συστημάτων πληροφοριών περιέχουν συχνά μια πληθώρα χαρακτηριστικών, μερικά από τα οποία μπορεί να είναι περιττά ή λιγότερο ενημερωτικά. Οι τεχνικές μείωσης διαστάσεων, όπως η ανάλυση κύριου στοιχείου (PCA) ή οι αλγόριθμοι επιλογής χαρακτηριστικών, στοχεύουν στη μείωση του αριθμού των χαρακτηριστικών διατηρώντας παράλληλα τις σχετικές πληροφορίες. Αυτό όχι μόνο βελτιώνει την απόδοση του μοντέλου, αλλά βοηθά επίσης στον μετριασμό του κινδύνου υπερβολικής τοποθέτησης [71].

Χρονικά και συμφραζόμενα χαρακτηριστικά

Στο πλαίσιο της ασφάλειας των πληροφοριακών συστημάτων, τα χρονικά και συμφραζόμενα χαρακτηριστικά διαδραματίζουν κρίσιμο ρόλο. Αυτά τα χαρακτηριστικά καταγράφουν μοτίβα που εξαρτώνται από το χρόνο και πληροφορίες που είναι ζωτικής σημασίας για την αξιολόγηση κινδύνου. Για παράδειγμα, η παρακολούθηση της συχνότητας των προσπαθειών σύνδεσης με την πάροδο του χρόνου ή η εξέταση της αλληλουχίας των γεγονότων δικτύου μπορεί να παρέχει πολύτιμες πληροφορίες σχετικά με τους κινδύνους ασφαλείας.

Ενοποίηση τεχνογνωσίας τομέα

Η ενσωμάτωση της τεχνογνωσίας στον τομέα είναι μια βασική πτυχή της μηχανικής χαρακτηριστικών. Οι ειδικοί και οι επαγγελματίες σε θέματα ασφάλειας διαθέτουν πολύτιμες γνώσεις σχετικά με τις αποχρώσεις και τους κρίσιμους δείκτες ασφάλειας συστημάτων πληροφοριών. Η συμβολή τους μπορεί να καθοδηγήσει την επιλογή και τη μηχανική των χαρακτηριστικών που σχετίζονται περισσότερο με το συγκεκριμένο πλαίσιο ασφάλειας.

Προσαρμοστικότητα σε μεταβαλλόμενες απειλές

Ένα δυναμικό τοπίο ασφαλείας απαιτεί η μηχανική χαρακτηριστικών να παραμένει προσαρμόσιμη στις εξελισσόμενες απειλές. Νέες απειλές και τρωτά σημεία εμφανίζονται συνεχώς και οι διαδικασίες μηχανικής των χαρακτηριστικών θα πρέπει να σχεδιάζονται για να ενσωματώνουν αυτές τις αλλαγές απρόσκοπτα [72]. Αυτή η προσαρμοστικότητα διασφαλίζει ότι τα μοντέλα αξιολόγησης κινδύνου παραμένουν αποτελεσματικά ενόψει των αναδυόμενων προκλήσεων ασφάλειας.

Συμπερασματικά, η Ενότητα 6.2 υπογραμμίζει τον κεντρικό ρόλο των μηχανικών χαρακτηριστικών από δεδομένα στην ανάπτυξη μοντέλων μηχανικής μάθησης για την αξιολόγηση κινδύνου στην ασφάλεια συστημάτων πληροφοριών. Περιλαμβάνει εξαγωγή χαρακτηριστικών, μετασχηματισμό, μείωση διαστάσεων, εξέταση χρονικών και συμφραζόμενων παραγόντων, ενσωμάτωση της τεχνογνωσίας του τομέα και προσαρμοστικότητα σε μεταβαλλόμενες απειλές. Η αποτελεσματική μηχανική χαρακτηριστικών δίνει τη δυνατότητα στα μοντέλα μηχανικής μάθησης να διακρίνουν ουσιαστικά μοτίβα και να συμβάλλουν σημαντικά στην ενίσχυση της ασφάλειας των συστημάτων πληροφοριών

6.3 Εκπαίδευση και επικύρωση μοντέλου

Στον τομέα της ενίσχυσης της ασφάλειας των συστημάτων πληροφοριών μέσω της αξιολόγησης κινδύνου βάσει μηχανικής μάθησης, η Ενότητα 6.3 εστιάζει στις κρίσιμες φάσεις της εκπαίδευσης και της επικύρωσης του μοντέλου. Αυτές οι φάσεις είναι ζωτικής σημασίας για την ανάπτυξη ακριβών και ισχυρών μοντέλων αξιολόγησης κινδύνου που μπορούν να εντοπίσουν και να κατηγοριοποιήσουν αποτελεσματικά τους κινδύνους ασφαλείας.

Εικόνα 11: Εκπαίδευση και επικύρωση μοντέλου

Εκπαίδευση μοντέλου

Η εκπαίδευση μοντέλων είναι η διαδικασία με την οποία ένας αλγόριθμος μηχανικής μάθησης μαθαίνει μοτίβα και σχέσεις μέσα στα δεδομένα για να κάνει προβλέψεις. Στο πλαίσιο της αξιολόγησης κινδύνου, το μοντέλο μηχανικής εκμάθησης εκτίθεται σε ένα επισημασμένο σύνολο δεδομένων, όπου κάθε σημείο δεδομένων σχετίζεται με ένα γνωστό επίπεδο κινδύνου (π.χ. "Χωρίς κίνδυνος" ή "Κίνδυνος") [73]. Ο στόχος του μοντέλου είναι να μάθει από αυτά τα δεδομένα και να γενικεύσει τα ευρήματά του για να κάνει προβλέψεις για αόρατα δεδομένα.

Εποπτευόμενη μάθηση

Η εποπτευόμενη μάθηση είναι η διαδεδομένη προσέγγιση στην αξιολόγηση κινδύνου. Κατά τη διάρκεια της εκπαίδευσης του μοντέλου, ο αλγόριθμος μαθαίνει να αντιστοιχίζει χαρακτηριστικά εισόδου (όπως διαμορφώσεις διακομιστή, ρυθμίσεις ασφάλειας δικτύου και δεδομένα ιστορικού περιστατικού) στα αντίστοιχα επίπεδα κινδύνου. Οι κοινοί αλγόριθμοι εποπτευόμενης μάθησης που χρησιμοποιούνται στην αξιολόγηση κινδύνου περιλαμβάνουν λογιστική παλινδρόμηση, δέντρα αποφάσεων, τυχαία δάση και μηχανές υποστήριξης διανυσμάτων.

Διασταυρωμένη επικύρωση

Για να αξιολογηθεί η ικανότητα γενίκευσης ενός μοντέλου και να διασφαλιστεί ότι αποδίδει καλά σε μη ορατά δεδομένα, χρησιμοποιείται συχνά η διασταυρούμενη επικύρωση. Η διασταυρούμενη επικύρωση περιλαμβάνει τη διαίρεση του συνόλου δεδομένων σε πολλαπλά υποσύνολα, που συνήθως αναφέρονται ως folds [73]. Το μοντέλο εκπαιδεύεται σε ένα υποσύνολο δεδομένων και επικυρώνεται σε ένα άλλο, με αυτή τη διαδικασία να επαναλαμβάνεται για κάθε πτυχή. Τα αποτελέσματα υπολογίζονται κατά μέσο όρο, παρέχοντας μια πιο ισχυρή αξιολόγηση της απόδοσης του μοντέλου.

Ρύθμιση υπερπαραμέτρων

Τα μοντέλα μηχανικής μάθησης έχουν συχνά υπερπαραμέτρους που απαιτούν συντονισμό για τη βελτιστοποίηση της απόδοσής τους. Οι υπερπαράμετροι είναι ρυθμίσεις διαμόρφωσης που δεν μαθαίνονται από τα δεδομένα αλλά επηρεάζουν τη συμπεριφορά του μοντέλου. Τεχνικές όπως η αναζήτηση πλέγματος ή η τυχαία αναζήτηση χρησιμοποιούνται για τη συστηματική διερεύνηση διαφορετικών συνδυασμών υπερπαραμέτρων για την εύρεση του μοντέλου με την καλύτερη απόδοση [73].

Αξιολόγηση μοντέλου

Η αξιολόγηση του μοντέλου είναι ένα κρίσιμο βήμα για την αξιολόγηση της απόδοσης του εκπαιδευμένου μοντέλου αξιολόγησης κινδύνου. Αυτή η φάση περιλαμβάνει τη χρήση διαφόρων μετρήσεων και τεχνικών για να μετρηθεί πόσο καλά το μοντέλο μπορεί να προβλέψει με ακρίβεια τα επίπεδα κινδύνου.

Κοινές μετρήσεις αξιολόγησης

Οι μετρήσεις αξιολόγησης που χρησιμοποιούνται συνήθως στην αξιολόγηση κινδύνου περιλαμβάνουν την ακρίβεια, την ανάκληση, τη βαθμολογία F1 και την περιοχή κάτω από τη χαρακτηριστική καμπύλη λειτουργίας του δέκτη (AUC-ROC) [74]. Αυτές οι μετρήσεις παρέχουν πληροφορίες για την ικανότητα του μοντέλου να ταξινομεί σωστά τους κινδύνους, να εντοπίζει ψευδώς θετικά και ψευδώς αρνητικά και τη συνολική απόδοση.

Αντιμετώπιση ανισορροπίας τάξης

Η αντιμετώπιση της ανισορροπίας της τάξης είναι υψίστης σημασίας στην αξιολόγηση κινδύνου, καθώς η κατηγορία "Χωρίς Κίνδυνο" συχνά υπερτερεί σημαντικά της κατηγορίας "Κινδύνου". Οι μετρήσεις αξιολόγησης θα πρέπει να επιλέγονται προσεκτικά για να λαμβάνεται υπόψη αυτή η ανισορροπία και θα πρέπει να λαμβάνονται υπόψη τεχνικές όπως η επαναδειγματοληψία, η μάθηση με ευαισθησία στο κόστος ή η χρήση διαφορετικών τιμών κατωφλίου.

Επικύρωση σε μη ορατά δεδομένα:

Για να αξιολογηθεί πραγματικά η αποτελεσματικότητα ενός μοντέλου, πρέπει να επικυρωθεί σε μη εμφανή δεδομένα ή σε ένα σύνολο δεδομένων δοκιμής που δεν χρησιμοποιήθηκε κατά τη διάρκεια της εκπαίδευσης. Αυτό το βήμα προσομοιώνει την απόδοση του μοντέλου σε ένα πραγματικό σενάριο όταν αντιμετωπίζει προηγουμένως απαρατήρητα περιστατικά ασφαλείας.

Επαναληπτική βελτίωση μοντέλου:

Η εκπαίδευση και η επικύρωση του μοντέλου είναι επαναληπτικές διαδικασίες. Με βάση τα αποτελέσματα της αξιολόγησης, τα μοντέλα μπορούν να βελτιωθούν με την προσαρμογή των υπερπαραμέτρων, την προσθήκη νέων χαρακτηριστικών ή την ενσωμάτωση πρόσθετων πηγών δεδομένων [75]. Αυτή η επαναληπτική προσέγγιση στοχεύει στη συνεχή

βελτίωση της απόδοσης του μοντέλου και στην προσαρμογή στις εξελισσόμενες απειλές ασφαλείας.

Συνοπτικά, η Ενότητα 6.3 υπογραμμίζει τη σημασία της εκπαίδευσης και της επικύρωσης μοντέλων για την ανάπτυξη μοντέλων αξιολόγησης κινδύνου που βασίζονται στη μηχανική μάθηση για την ασφάλεια συστημάτων πληροφοριών. Περιλαμβάνει εποπτευόμενη μάθηση, διασταυρούμενη επικύρωση, συντονισμό υπερπαραμέτρων, μετρήσεις αξιολόγησης μοντέλων, χειρισμό ανισορροπίας κλάσης, επικύρωση σε μη ορατά δεδομένα και επαναληπτική βελτίωση του μοντέλου. Με την προσεκτική πλοήγηση σε αυτές τις φάσεις, οι οργανισμοί μπορούν να αξιοποιήσουν τη δύναμη της μηχανικής μάθησης για να βελτιώσουν τη στάση ασφαλείας τους και να μετριάσουν αποτελεσματικά τους κινδύνους.

6.4. Ενοποίηση με Πληροφοριακά Συστήματα

Η ενότητα 6.4 διερευνά μια κρίσιμη πτυχή της ενίσχυσης της ασφάλειας των πληροφοριακών συστημάτων μέσω της αξιολόγησης κινδύνου που βασίζεται στη μηχανική μάθηση: την ενοποίηση μοντέλων αξιολόγησης κινδύνου με τα υπάρχοντα συστήματα πληροφοριών. Αυτή η ενοποίηση είναι απαραίτητη για τη δημιουργία ενός απρόσκοπτου και αποτελεσματικού οικοσυστήματος ασφάλειας που μπορεί να εντοπίσει και να ανταποκριθεί σε κινδύνους ασφάλειας σε πραγματικό χρόνο.

Εκτίμηση κινδύνου σε πραγματικό χρόνο

Ένας από τους πρωταρχικούς στόχους της ενσωμάτωσης της αξιολόγησης κινδύνου βάσει μηχανικής μάθησης είναι να καταστεί δυνατή η αξιολόγηση κινδύνου σε πραγματικό χρόνο στα συστήματα πληροφοριών. Αυτό σημαίνει ότι καθώς δημιουργούνται δεδομένα και συμβαίνουν γεγονότα μέσα στο σύστημα, το μοντέλο αξιολόγησης κινδύνου μπορεί να αναλύει συνεχώς αυτά τα δεδομένα και να παρέχει άμεσες πληροφορίες για πιθανούς κινδύνους ασφαλείας.

Συλλογή και τροφοδοσία δεδομένων

Για να καταστεί δυνατή η αξιολόγηση κινδύνου σε πραγματικό χρόνο, συλλέγονται δεδομένα από διάφορες πηγές εντός του συστήματος πληροφοριών και τροφοδοτούνται στο μοντέλο αξιολόγησης κινδύνου. Αυτά τα δεδομένα μπορεί να περιλαμβάνουν αρχεία καταγραφής διακομιστή, δεδομένα κίνησης δικτύου, μοτίβα πρόσβασης χρηστών και άλλα. Το

μοντέλο επεξεργάζεται αυτά τα εισερχόμενα δεδομένα για να εντοπίσει πιθανές απειλές ασφαλείας.

Συμπεράσματα μηχανικής μάθησης

Το μοντέλο αξιολόγησης κινδύνου, που εκπαιδεύτηκε κατά τη φάση εκπαίδευσης και επικύρωσης του μοντέλου, λειτουργεί ως ο βασικός κινητήρας για την ανάλυση των εισερχόμενων δεδομένων. Οι αλγόριθμοι μηχανικής μάθησης εντός του μοντέλου κατηγοριοποιούν και ιεραρχούν τους κινδύνους με βάση τα χαρακτηριστικά που εξάγονται από τα εισερχόμενα δεδομένα.

Δημιουργία ειδοποιήσεων

Όταν το μοντέλο αξιολόγησης κινδύνου εντοπίζει έναν κίνδυνο ασφάλειας που υπερβαίνει ένα προκαθορισμένο όριο, δημιουργεί ειδοποιήσεις ή ειδοποιήσεις. Αυτές οι ειδοποιήσεις μπορούν να λάβουν διάφορες μορφές, όπως ειδοποιήσεις μέσω email προς το προσωπικό ασφαλείας, αναδυόμενα μηνύματα στους πίνακες εργαλείων του συστήματος ή αυτοματοποιημένες ενέργειες για τον μετριασμό του εντοπισθέντος κινδύνου.

Ενοποίηση με Συστήματα Ασφαλείας Πληροφοριών και Διαχείρισης Συμβάντων (SIEM):

Τα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) διαδραματίζουν κρίσιμο ρόλο στη συγκέντρωση και ανάλυση δεδομένων που σχετίζονται με την ασφάλεια. Η ενσωμάτωση μοντέλων αξιολόγησης κινδύνου που βασίζονται σε μηχανική μάθηση με συστήματα SIEM ενισχύει τις δυνατότητες αυτών των συστημάτων. Επιτρέπει πιο προηγμένη ανάλυση γεγονότων και συμβάντων ασφάλειας με επίγνωση του πλαισίου.

Προσαρμοστικές απαντήσεις:

Η ενσωμάτωση μοντέλων αξιολόγησης κινδύνου με συστήματα πληροφοριών επιτρέπει προσαρμοστικές απαντήσεις σε απειλές ασφαλείας. Όταν ανιχνεύεται ένας κίνδυνος, μπορούν να ενεργοποιηθούν αυτοματοποιημένες αποκρίσεις, όπως η απομόνωση επηρεαζόμενων συστημάτων, ο αποκλεισμός ύποπτων διευθύνσεων IP ή η κλιμάκωση περιστατικών σε ομάδες αντιμετώπισης περιστατικών.

Συνεχής Μάθηση και Προσαρμογή:

Η ενσωμάτωση υποστηρίζει επίσης τη συνεχή μάθηση και την προσαρμογή. Καθώς το μοντέλο αξιολόγησης κινδύνου λειτουργεί εντός του πληροφοριακού συστήματος, μπορεί να μάθει από τις επιδόσεις του και να προσαρμοστεί στις εξελισσόμενες απειλές. Αυτή η προσαρμοστικότητα είναι κρίσιμη σε ένα διαρκώς μεταβαλλόμενο τοπίο κυβερνοασφάλειας.

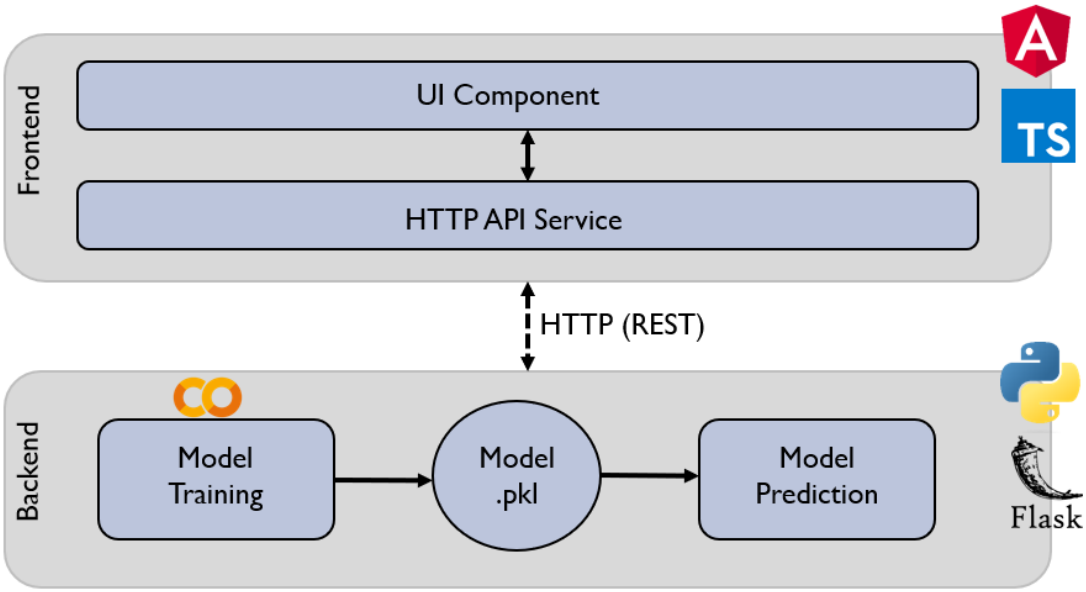
Βρόχος ανατροφοδότησης

Δημιουργείται ένας βρόχος ανάδρασης για να διασφαλιστεί ότι οι πληροφορίες από το μοντέλο αξιολόγησης κινδύνου χρησιμοποιούνται για τη βελτίωση της συνολικής θέσης ασφαλείας του συστήματος πληροφοριών. Αυτό περιλαμβάνει τη βελτίωση των πολιτικών ασφαλείας, την προσαρμογή των ελέγχων πρόσβασης και την εφαρμογή προληπτικών μέτρων για την αντιμετώπιση των εντοπισμένων κινδύνων.

Συμπερασματικά, η Ενότητα 6.4 υπογραμμίζει τη σημασία της ενσωμάτωσης μοντέλων αξιολόγησης κινδύνου που βασίζονται στη μηχανική μάθηση με συστήματα πληροφοριών για την επίτευξη ικανοτήτων αξιολόγησης κινδύνου και αντίδρασης σε πραγματικό χρόνο. Αυτή η ενοποίηση δίνει τη δυνατότητα στους οργανισμούς να βελτιώνουν την ασφάλεια των πληροφοριακών συστημάτων τους παρακολουθώντας, αναλύοντας και μετριάζοντας συνεχώς τους κινδύνους ασφαλείας, συμβάλλοντας τελικά σε ένα πιο ανθεκτικό και ασφαλές ψηφιακό περιβάλλον.

7. Αρχιτεκτονική Εφαρμογής

Το διάγραμμα της παρακάτω εικόνας απεικονίζει την αρχιτεκτονική ενός συστήματος πληροφοριών εργαλείου αξιολόγησης κινδύνου (Risk assessment tool), χωρισμένο σε δύο κύριες ενότητες: Frontend και Backend.



Εικόνα 12: Αρχιτεκτονική Risk assessment tool

Frontend

Στοιχείο διεπαφής χρήστη: Αντιπροσωπεύει τη διεπαφή χρήστη του συστήματος όπου οι χρήστες αλληλεπιδρούν με το εργαλείο. Αναπτύχθηκε χρησιμοποιώντας Angular σε TypeScript (όπως υποδεικνύεται από το λογότυπο "TS"). Εδώ οι χρήστες εισάγουν δεδομένα και βλέπουν τα αποτελέσματα της αξιολόγησης κινδύνου.

Backend

Εκπαίδευση μοντέλου: Αυτή είναι η διαδικασία κατά την οποία ένα μοντέλο μηχανικής μάθησης εκπαιδεύεται χρησιμοποιώντας ιστορικά δεδομένα. Κατά τη διάρκεια αυτής της φάσης, το μοντέλο μαθαίνει να εντοπίζει πρότυπα που είναι ενδεικτικά του κινδύνου.

Model .pkl

Μετά την εκπαίδευση, το μοντέλο αποθηκεύεται σε σειριακή μορφή με επέκταση .pkl, που σημαίνει "pickle". Το Pickle είναι μια λειτουργική μονάδα Python που σειριοποιεί

αντικείμενα Python στο δίσκο, ώστε να μπορούν να φορτωθούν ξανά σε άλλες διεργασίες Python. Η προαναφερθείσα εργασία γίνεται με την χρήση του google cloud service του Colab. Πρόβλεψη μοντέλου: Αυτό είναι το στάδιο όπου το εκπαιδευμένο μοντέλο χρησιμοποιείται για να κάνει προβλέψεις. Νέα δεδομένα τροφοδοτούνται στο μοντέλο και εκδίδει την αξιολόγησή του για τον κίνδυνο με βάση τα όσα έχει μάθει κατά τη διάρκεια της εκπαίδευσης.

Υπηρεσία HTTP API:

Αυτό είναι ένα επίπεδο υπηρεσίας που λειτουργεί ως ενδιάμεσος μεταξύ του frontend και του backend. Πιθανότατα υλοποιείται χρησιμοποιώντας το Flask (όπως υποδεικνύεται από το λογότυπο του Flask), ένα micro-web framework στην Python. Η υπηρεσία εκθέτει τελικά endpoints HTTP RESTful που μπορεί να καταναλώσει η διεπαφή για την αποστολή δεδομένων στο backend και την ανάκτηση προβλέψεων.

Ροή δεδομένων/Ανάλυση:

- Ένας χρήστης εισάγει δεδομένα στο στοιχείο διεπαφής χρήστη στη διεπαφή.
- Το στοιχείο διεπαφής χρήστη στέλνει τα δεδομένα στην υπηρεσία HTTP API χρησιμοποιώντας ένα πρωτόκολλο HTTP (REST).
- Η υπηρεσία HTTP API λαμβάνει τα δεδομένα και τα μεταβιβάζει στη διαδικασία πρόβλεψης μοντέλου στο backend.
- Η διαδικασία Πρόβλεψης Μοντέλου χρησιμοποιεί το εκπαιδευμένο μοντέλο μηχανικής εκμάθησης (σε σειρά ως .pkl) για την αξιολόγηση του κινδύνου με βάση τα δεδομένα εισόδου.
- Τα αποτελέσματα πρόβλεψης αποστέλλονται πίσω στο frontend μέσω της υπηρεσίας HTTP API.
- Στη συνέχεια, το στοιχείο διεπαφής χρήστη εμφανίζει τα αποτελέσματα στον χρήστη.

Το διακεκομμένο βέλος υποδεικνύει ότι η επικοινωνία μεταξύ της Υπηρεσίας API HTTP και της διαδικασίας πρόβλεψης μοντέλου ενδέχεται να μην είναι απευθείας κλήση. θα μπορούσε να είναι μια εσωτερική κλήση διαδικασίας μέσα στο σύστημα υποστήριξης. Η συνολική αρχιτεκτονική είναι ένα κοινό μοτίβο για εφαρμογές μηχανικής εκμάθησης που βασίζονται στο web, διευκολύνοντας τον διαχωρισμό των ανησυχιών και την επεκτασιμότητα.

8. Οδηγός Χρήσης Εφαρμογής

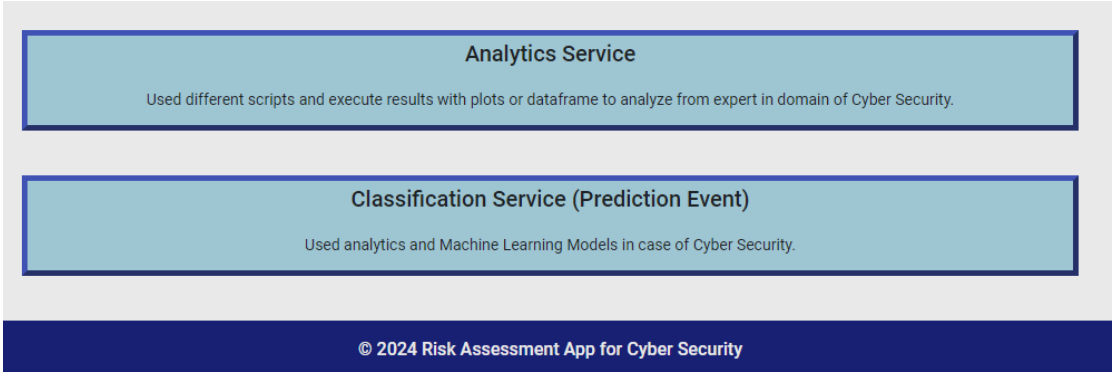
Στο συγκεκριμένο κεφάλαιο θα παρουσιαστεί η εφαρμογή του risk assessment εργαλείου προκειμένου να ανιχνευτεί αν υπάρχει κίνδυνος ή όχι ευπάθειας ή ακόμα καλύτερα επίθεσης στο εν λόγω σύστημα που ελέγχεται.

Εικόνα 13: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (1)

Αρχικά στην παρακάτω εικόνα μπορούμε να δούμε την κύρια οθόνη του πληροφοριακού συστήματος.

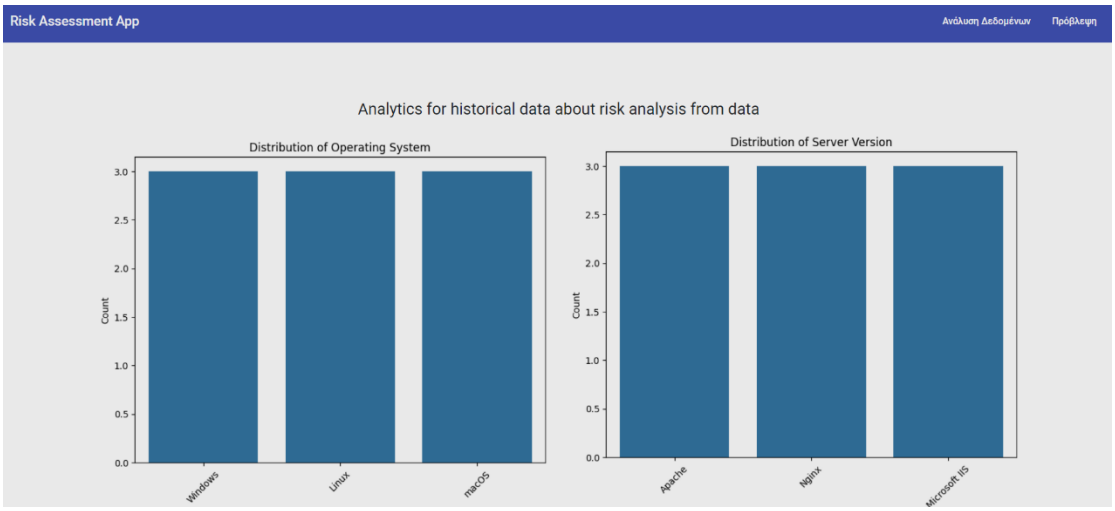
Εικόνα 14: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (2)

Στην επόμενη αμέσως εικόνα μπορούμε να δούμε την κύρια σελίδα του συστήματος και την παροχή υπηρεσιών προς τον χρήστη του συγκεκριμένου συστήματος, όπου είναι η ανάλυση δεδομένων και επίσης η πρόβλεψη για πιθανή ευπάθεια ή όχι για το σύστημα το οποίο ελέγχεται μέσω κατάλληλης φόρμας και με τη χρήση των αλγορίθμων μηχανικής μάθησης.



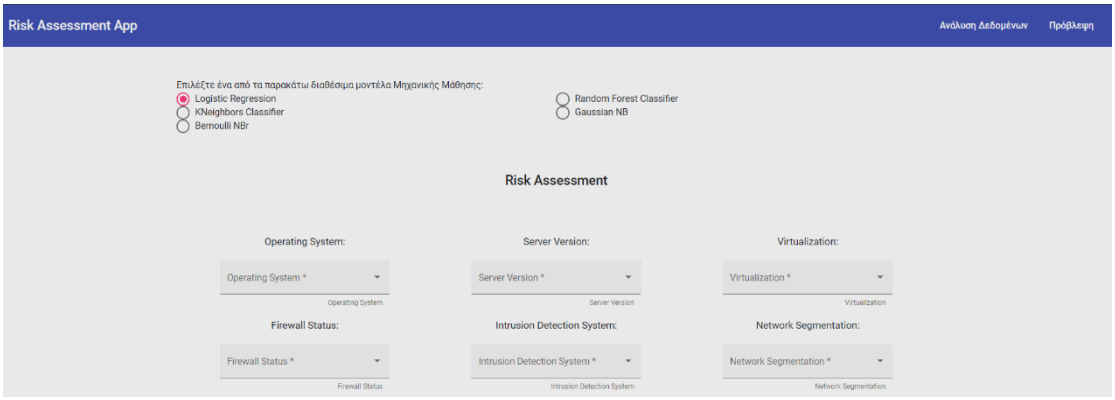
Εικόνα 15: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (3)

Στην παρακάτω εικόνα γίνονται καλύτερα ευκρινή οι υπηρεσίες που παρέχονται στο συγκεκριμένο σύστημα.

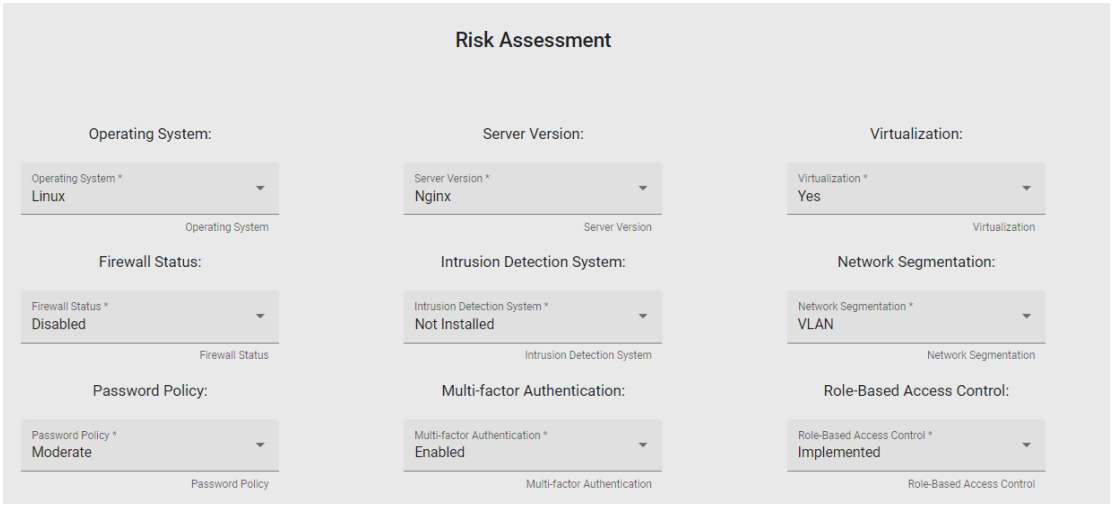


Εικόνα 16: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (4)

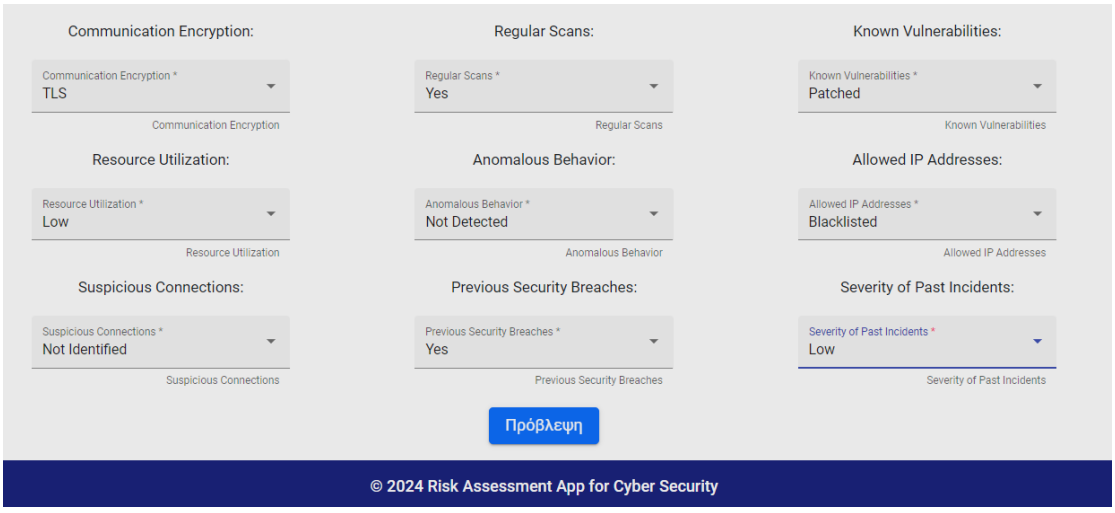
Στις επόμενες εικόνες βλέπουμε την παρουσίαση της φόρμας με τα πεδία που συνίσταται. Στη συνέχεια φαίνονται συμπληρωμένα τα πεδία της φόρμας και εν τέλει παρατηρείται το τελικό αποτέλεσμα που βασίζεται στις παραμέτρους που τίθενται στη συγκεκριμένη φόρμα. Τέλος πραγματοποιείται η πρόβλεψη για το κίνδυνο επίθεσης ή όχι του συστήματος του οποίου ελέγχουμε μέσω συγκεκριμένων αλγορίθμων μηχανικής μάθησης.



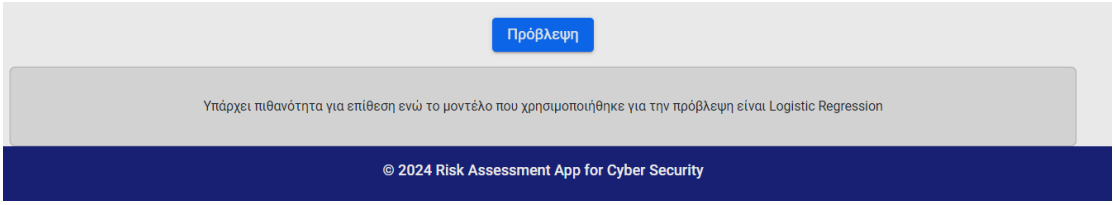
Εικόνα 17: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (5)



Εικόνα 18: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (6)



Εικόνα 19: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (7)



Εικόνα 20: Στιγμιότυπο Οθόνης εφαρμογής Risk Assessment Tool (8)

Συμπέρασμα

Στο ταχέως εξελισσόμενο τοπίο της ασφάλειας των πληροφοριακών συστημάτων, η ενσωμάτωση εργαλείων αξιολόγησης κινδύνου και συστημάτων προειδοποίησης που βασίζονται στη μηχανική μάθηση διαδραματίζει κεντρικό ρόλο στη διαφύλαξη ευαίσθητων δεδομένων και στη διασφάλιση της επιχειρηματικής συνέχειας. Αυτή η ολοκληρωμένη προσέγγιση είναι απαραίτητη για την αντιμετώπιση των ολοένα αυξανόμενων απειλών στον κυβερνοχώρο που αντιμετωπίζουν άτομα και οργανισμοί.

Η ιστορική προοπτική αποκαλύπτει ότι η έννοια της ασφάλειας μηχανικής μάθησης και η συνάφειά της με τα συστήματα πληροφοριών προηγείται της πρόσφατης προσοχής. Οι πρώτες εργασίες για την αντίθετη μηχανική μάθηση και η μελέτη των απειλών σε αλγόριθμους μη βαθιάς μηχανικής μάθησης άνοιξαν το δρόμο για την κατανόηση και την αντιμετώπιση των προκλήσεων ασφάλειας στο πεδίο.

Η σημασία της ασφάλειας των συστημάτων πληροφοριών δεν μπορεί να υπερεκτιμηθεί. Με την ψηφιοποίηση των λειτουργιών σε όλους τους κλάδους, η διασφάλιση κρίσιμων δεδομένων και υποδομών έχει καταστεί πρωταρχικής σημασίας. Τα συστήματα πληροφοριών φιλοξενούν πολύτιμα περιουσιακά στοιχεία και οι συνέπειες των παραβιάσεων της ασφάλειας μπορεί να είναι σοβαρές. Ως εκ τούτου, είναι απαραίτητη μια προληπτική προσέγγιση για την εκτίμηση του κινδύνου και τον μετριασμό της απειλής.

Ο σκοπός και το εύρος της έρευνας που περιγράφεται σε αυτό το έργο είναι η ανάπτυξη ενός έξυπνου συστήματος προειδοποίησης που αξιοποιεί αλγόριθμους μηχανικής μάθησης για την κατηγοριοποίηση και την ιεράρχηση των εντοπισμένων κινδύνων. Αυτό το σύστημα στοχεύει να παρέχει στους χρήστες πολύτιμες γνώσεις σχετικά με τη σημασία των εντοπισμένων κινδύνων, επιτρέποντας πιο αποτελεσματική λήψη αποφάσεων και αντιμετώπιση περιστατικών. Η έρευνα περιλαμβάνει μια διεξοδική ανασκόπηση της υπάρχουσας βιβλιογραφίας, την ανάπτυξη πρωτοτύπων συστημάτων ειδοποίησης και την αξιολόγηση αλγορίθμων μηχανικής μάθησης για την κατηγοριοποίηση κινδύνου.
Οι ερευνητικοί στόχοι περιλαμβάνουν:

- Διεξαγωγή μιας περιεκτικής βιβλιογραφικής ανασκόπησης σχετικά με την ασφάλεια συστημάτων πληροφοριών, τις μεθοδολογίες αξιολόγησης κινδύνου και τις εφαρμογές μηχανικής μάθησης στο πεδίο.
- Ανάπτυξη ενός πρωτότυπου συστήματος ειδοποιήσεων που ενσωματώνεται απρόσκοπτα με τα υπάρχοντα συστήματα πληροφοριών.
- Διερεύνηση αλγορίθμων μηχανικής μάθησης για την αυτόματη κατηγοριοποίηση των κινδύνων με βάση τον αντίκτυπο, την πιθανότητα και τη συνάφεια.

- Αξιολόγηση της πρακτικότητας της ενίσχυσης της ασφάλειας των πληροφοριακών συστημάτων μέσω έξυπνης αξιολόγησης κινδύνου και συστημάτων ειδοποίησης σε πραγματικό χρόνο.

Συνοπτικά, η σύνθεση της μηχανικής μάθησης, των μεθοδολογιών αξιολόγησης κινδύνου και της ασφάλειας των συστημάτων πληροφοριών αποτελεί μια πολλά υποσχόμενη οδό για τη βελτίωση της στάσης ασφαλείας των οργανισμών. Καθώς οι απειλές συνεχίζουν να εξελίσσονται, αυτό το ερευνητικό έργο επιδιώκει να συνεισφέρει πολύτιμα εργαλεία και πλαίσια στον τομέα της κυβερνοασφάλειας, ενισχύοντας τελικά την άμυνα κατά των κυβερνοεπιθέσεων και διασφαλίζοντας τη συνεχή ακεραιότητα των κρίσιμων πληροφοριακών συστημάτων.

Το ταξίδι προς έναν πιο ασφαλή ψηφιακό κόσμο είναι μια συνεχής προσπάθεια και τα αποτελέσματα αυτής της ερευνητικής προσπάθειας αναμένεται να συμβάλουν σημαντικά στην ευρύτερη αποστολή της προστασίας των πληροφοριακών συστημάτων και της προστασίας των ψηφιακών περιουσιακών στοιχείων ατόμων και οργανισμών.

Μελλοντικές εργασίες και συστάσεις

Καθώς ο τομέας της ασφάλειας των συστημάτων πληροφοριών και της αξιολόγησης κινδύνου με γνώμονα τη μηχανική μάθηση συνεχίζει να εξελίσσεται, υπάρχουν αρκετοί δρόμοι για μελλοντική έρευνα και συστάσεις για περαιτέρω βελτίωση του τοπίου της ασφάλειας:

1. Προηγμένες τεχνικές μηχανικής μάθησης: Εξερεύνηση και ανάπτυξη σε προηγμένους αλγόριθμους και τεχνικές μηχανικής μάθησης που μπορούν να προσαρμοστούν σε αναδυόμενες απειλές στον κυβερνοχώρο. Η έρευνα για τη βαθιά μάθηση, την ενισχυτική μάθηση και τις μεθόδους συνόλου μπορεί να παρέχει πιο ισχυρά μοντέλα για την αξιολόγηση κινδύνου και την ανίχνευση απειλών.
2. Ενσωμάτωση πληροφοριών απειλών σε πραγματικό χρόνο: Ενσωμάτωση πληροφοριών απειλών σε πραγματικό χρόνο στα συστήματα αξιολόγησης κινδύνου. Αυτό θα επιτρέψει στους οργανισμούς να παραμένουν ενημερωμένοι με τις τελευταίες τάσεις απειλών και να προσαρμόζουν ανάλογα τα μέτρα ασφαλείας τους.
3. Ανθρωποκεντρική ασφάλεια: Διερεύνηση περαιτέρω για το ανθρώπινο στοιχείο στα συστήματα ασφαλείας. Ανάπτυξη σε μέτρα ασφαλείας με επίκεντρο τον χρήστη, όπως καλύτερα προγράμματα εκπαίδευσης και ευαισθητοποίησης των χρηστών, για την ενίσχυση της πρώτης γραμμής άμυνας έναντι της κοινωνικής μηχανικής και των εσωτερικών απειλών.
4. Επεξηγήσιμη τεχνητή νοημοσύνη: Αντιμετώπιση για το ζήτημα της ερμηνευσιμότητας και της επεξήγησης σε μοντέλα μηχανικής μάθησης που χρησιμοποιούνται για την αξιολόγηση κινδύνου. Ενίσχυση για τη διαφάνεια και τη λογοδοσία αναπτύσσοντας μοντέλα που παρέχουν σαφείς εξηγήσεις για τις εκτιμήσεις κινδύνου τους.
5. Κανονιστική συμμόρφωση: Μείνετε ενήμεροι για τα εξελισσόμενα ρυθμιστικά τοπία και τις απαιτήσεις συμμόρφωσης, ειδικά στο πλαίσιο της νομοθεσίας περί προστασίας δεδομένων και απορρήτου. Βεβαίωση ότι τα εργαλεία και οι πρακτικές αξιολόγησης κινδύνου ευθυγραμμίζονται με αυτούς τους κανονισμούς.
6. Ενσωμάτωση με DevSecOps: Ενσωμάτωση σχετικά με τις πρακτικές ασφαλείας στον κύκλο ζωής ανάπτυξης λογισμικού ενσωματώνοντας την αξιολόγηση κινδύνου και την ειδοποίηση στις διαδικασίες DevSecOps. Αυτή η προληπτική προσέγγιση μπορεί να βοηθήσει στον εντοπισμό και τον μετριασμό των τρωτών σημείων νωρίς στον κύκλο ανάπτυξης.

7. Συνεχής Παρακολούθηση και Προσαρμογή: Έμφαση για τη σημασία της συνεχούς παρακολούθησης και προσαρμογής των μέτρων ασφαλείας. Τα τοπία απειλών αλλάζουν γρήγορα και οι οργανισμοί πρέπει να είναι ευέλικτοι στην προσαρμογή των στρατηγικών αξιολόγησης κινδύνου.

Συμπερασματικά, ο τομέας της ασφάλειας των πληροφοριακών συστημάτων και της αξιολόγησης κινδύνου είναι ένας δυναμικός και διαρκώς εξελισσόμενος τομέας. Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην παραμονή μπροστά από τις αναδυόμενες απειλές, στην ενίσχυση της επεξήγησης των μοντέλων μηχανικής μάθησης και στην προώθηση μιας κουλτούρας ευαισθητοποίησης σχετικά με την ασφάλεια. Υιοθετώντας αυτές τις συστάσεις, οι οργανισμοί μπορούν να προστατεύσουν καλύτερα τα πληροφοριακά τους συστήματα και να συμβάλουν σε ένα πιο ασφαλές ψηφιακό περιβάλλον.

Βιβλιογραφική Αναφορά

[1] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. J. Goodfellow, et al., "Intriguing properties of neural networks", Proc. 2nd Int. Conf. Learn. Represent., pp. 1-10, Apr. 2014.

[2] I. J. Goodfellow, J. Shlens and C. Szegedy, "Explaining and harnessing adversarial examples", Proc. Int. Conf. Learn. Representations, pp. 1-11, Mar. 2015.

[3] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning", Pattern Recognit., vol. 84, pp. 317-331, Dec. 2018.

[4] N. N. Dalvi, P. M. Domingos, Mausam, S. K. Sanghai and D. Verma, "Adversarial classification", Proc. 10th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., pp. 99-108, Aug. 2004.

[5] B. Nelson, M. Barreno, F. J. Chi, A. D. Joseph, B. I. P. Rubinstein, U. Saini, et al., "Exploiting machine learning to subvert your spam filter", Proc. USENIX Workshop Large-Scale Exploit. Emerg. Threat., pp. 1-9, Apr. 2008.

[6] M. Barreno, B. Nelson, A. D. Joseph and J. D. Tygar, "The security of machine learning", Mach. Learn., vol. 81, pp. 121-148, Nov. 2010.

[7] N. Akhtar and A. S. Mian, "Threat of adversarial attacks on deep learning in computer vision: A survey", IEEE Access, vol. 6, pp. 14410-14430, Jul. 2018.

[8] X. Yuan, P. He, Q. Zhu and X. Li, "Adversarial examples: Attacks and defenses for deep learning", IEEE Trans. Neural Netw. Learn. Syst., vol. 30, no. 9, pp. 2805-2824, Sep. 2019.

[9] M. S. Riazi and F. Koushanfar, "Privacy-preserving deep learning and inference", Proc. Int. Conf. Comput.-Aided Design ICCAD, pp. 1-4, Nov. 2018.

[10] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu and V. C. M. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view", IEEE Access, vol. 6, pp. 12103-12117, 2018.

[11] N. Papernot, P. D. McDaniel, A. Sinha and M. P. Wellman, "SoK: Security and privacy in machine learning", Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P), pp. 399-414, Apr. 2018.

[12] T. Gu, B. Dolan-Gavitt and S. Garg, "BadNets: Identifying vulnerabilities in the machine learning model supply chain" in arXiv:1708.06733, 2017, [online] Available: http://arxiv.org/abs/1708.06733.

[13] S. Yeom, I. Giacomelli, M. Fredrikson and S. Jha, "Privacy risk in machine learning: Analyzing the connection to overfitting", Proc. IEEE 31st Comput. Secur. Found. Symp. (CSF), pp. 268-282, Jul. 2018.

[14] Shon, T.; Moon, J. A hybrid machine learning approach to network anomaly detection. Inf. Sci. (NY) 2007, 177, 3799–3821.

[15] Bhoiwala, J.P.; Jhaveri, R.H. Cooperation Based Defense Mechanism against Selfish Nodes in DTNs. ACM Int. Conf. Proc. Ser. 2017.

[16] Jhaveri, R.H. Secure Routing in Mobile Ad-Hoc Networks: Attacks and Solutions; LAMBERT Academic Publishing: Saarbrücken, Germany, 2017.

[17] Vidal, J.M.; Orozco, A.L.S.; Villalba, L.J.G. Alert correlation framework for malware detection by anomaly-based packet payload analysis. J. Netw. Comput. Appl. 2017, 97, 11–22.

[18] Cohen, Y.; Hendler, D.; Rubin, A. Detection of malicious webmail attachments based on propagation patterns. Knowl. Based Syst. 2018, 141, 67–79.
[19] Paxson, V. Bro: A system for detecting network intruders in real-time. Comput. Netw. 1999, 31, 2435–2463.
[20] Jhaveri, R.H.; Patel, N.M. A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. Wirel. Netw. 2015, 21, 2781–2798.
[21] Jhaveri, R.H.; Patel, N.M. Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. Int. J. Commun. Syst. 2017, 30, e3148.
[22] Jhaveri, R.H. MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs. In Proceedings of the 2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT), Rohtak, India, 6–7 April 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 254–260.
[23] Jhaveri, R.H. Reliable Approach to Prevent Blackhole and Grayholes Attacks in Mobile ad-hoc Networks; IET Editorial Book; IET: London, UK, 2013; pp. 261–280.
[24] Jhaveri, R.H.; Patel, N.M.; Jinwala, D.C.; Ortiz, J.H.; de la Cruz, A.P. A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks; Ortiz, J.H., de la Cruz, A.P., Eds.; IntechOpen: London, UK, 2017; pp. 19–45.
[25] Overill, R.E. How Re (Pro) active Should an IDS be? In Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection (RAID), Louvain-la-Neuve, Belgium, 14–16 September 1998; pp. 1–6.
[26] Francisco, S.; Martin, D.; Schulman, A. Infranet: Circumventing web censorship and surveillance. In Proceedings of the 11 the USENIX Security Symposium, Berkeley, CA, USA, 5–9 August 2002.
[27] Rhodes, B.C.; Mahaffey, J.A.; Cannady, J.D. Multiple self-organizing maps for intrusion detection. In Proceedings of the 23rd National Information Systems Security Conference, Baltimore, MD, USA, 16–19 October 2000; pp. 16–19.
[28] Yamada, A.; Miyake, Y. Intrusion detection system to detect variant attacks using learning algorithms with automatic generation of training data. In Proceedings of the IEEE Coding and Computing, Las Vegas, NV, USA, 4–6 April 2005; IEEE: Piscataway, NJ, USA, 2005; pp. 1–6.
[29] Lippmann, R.P.; Cunningham, R.K. Improving intrusion detection performance using keyword selection and neural networks. Comput. Netw. 2000, 34, 597–603.
[30] Wong, W.T.; Hsu, S.H. Application of SVM and ANN for image retrieval. Eur. J. Oper. Res. 2006, 173, 938–950.
[31] Borges, P.; Sousa, B.; Ferreira, L.; Saghezchi, F.B.; Mantas, G.; Ribeiro, J.; Simoes, P. Towards a Hybrid Intrusion Detection System for Android-based PPDR terminals. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1034–1039.
[32] Karthick, R.R.; Hattiwale, V.P.; Ravindran, B. Adaptive network intrusion detection system using a hybrid approach. In Proceedings of the IEEE

Fourth International Conference on Communication Systems and Networks, Bangalore, India, 3–7 January 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1–7.

[33] Freund, Y.; Schapire, R.E. Experiments with a new boosting algorithm. In Proceedings of the ICML'96 Proceedings of the Thirteenth International Conference on International Conference on Machine Learning, Bari, Italy, 3–6 July 1996; pp. 148–156.

[34] Bauer, E.; Kohavi, R.; Chan, P.; Stolfo, S.; Wolpert, D. An Empirical Comparison of Voting Classification Algorithms: Bagging, Boosting, and Variants. Mach. Learn. 1999, 36, 105–139.

[35] Breiman, L. Random forests. Mach. Learn. 2001, 45, 5–32.

[36] Parmanto, B.; Munro, P.W.; Doyle, H.R. Improving committee diagnosis with resampling techniques. Adv. Neural Inf. Process. Syst. 1996, 8, 882–888.

[37] Ma, T.; Wang, F.; Cheng, J.; Yu, Y.; Chen, X. A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection. Sensors (Basel) 2016, 16, 1701.

[38] Viegas, E.K.; Santin, A.O.; Oliveira, L.S. Toward a reliable anomaly-based intrusion detection in real-world environments. Comput. Netw. 2017, 127, 200–216.

[39] Ghanem, K.; Aparicio-Navarro, F.J.; Kyriakopoulos, K.G.; Lambotharan, S.; Chambers, J.A. Support Vector Machine for Network Intrusion and Cyber-Attack Detection. In Proceedings of the 2017 Sensor Signal Processing for Defence Conference (SSPD), London, UK, 6–7 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.

[40] Al-Yaseen, W.L.; Othman, Z.A.; Nazri, M.Z.A. Hybrid Modified K -Means with C4.5 for Intrusion Detection Systems in Multiagent Systems. Sci. World J. 2015.

[41] Ross, J.; Morgan, Q.; Publishers, K. Book Review: C4. 5: Programs for Machine Learning. Mach. Learn. 1994, 16, 235.

[42] Abadeh, M.S.; Habibi, J.; Barzegar, Z.; Sergi, M. A parallel genetic local search algorithm for intrusion detection in computer networks. Elsevier Eng. Appl. Artif. Intell. 2007, 20, 1058–1069.

[43] Giacinto, G.; Perdisci, R.; del Rio, M.; Roli, F. Intrusion detection in computer networks by a modular ensemble of one-class classifiers. Inf. Fusion 2008, 9, 69–82.

[44] Gajin, V.T.S. Ensemble classifiers for supervised anomaly-based network intrusion detection. In Proceedings of the 2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 7–9 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 13–19.

[45] Hansen, J.V.; Lowry, P.B.; Meservy, R.D.; McDonald, D.M. Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decis. Support Syst. 2007, 43, 1362–1374.

[46] Jhaveri, R.H. DoS Attacks in Mobile Ad Hoc Networks: A Survey DoS Attacks in Mobile Ad-hoc Networks: A Survey. In Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, Rohtak, Haryana, India, 7–8 January 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 535–541.

[47] Prichard, J.J.; Macdonald, L.E. Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks. J. Inf. Technol. Educ. 2004, 3, 279–289.
[48] Gunawardena, S.H.; Kulkarni, D.; Gnanasekaraiyer, B. A Steganography-based framework to prevent active attacks during user authentication. In Proceedings of the 2013 8th International Conference on Computer Science & Education, Colombo, Sri Lanka, 26-28 April 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 383–388.
[49] Allen, J.; Gomez, L.; Green, M.; Ricciardi, P.; Sanabria, C.; Kim, S. Social Network Security Issues: Social Engineering and Phishing Attacks. In Proceedings of the Student-Faculty Research Day, CSIS, White Plains, NY, USA, 4 May 2012; pp. 1–7.
[50] Applegate, S.D. Social engineering: Hacking the wetware! Inf. Secur. J. 2009, 18, 40–46.
[51] Khonji, M.; Iraqi, Y.; Jones, A. Phishing detection: A literature survey. IEEE Commun. Surv. Tutor. 2013, 15, 2091–2121.
[52] Li, Y.; Xiao, R.; Feng, J.; Zhao, L. A semi-supervised learning approach for detection of phishing webpages. Optik 2013, 124, 6027–6033.
[53] Smadi, S.; Aslam, N.; Zhang, L. Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. Decis. Support Syst. 2018, 107, 88–102.
[54] Hamid, I.R.A.; Abawajy, J.H. An approach for profiling phishing activities. Comput. Secur. 2014, 45, 27–41.
[55] Basnet, R. Feature Selection for Improved Phishing Detection. In Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Dalian, China, 9–12 June 2012; Springer: Berlin/Heidelberg, Germany, 2012.
[56] Li, Y.; Wang, G.; Nie, L.; Wang, Q.; Tan, W. Distance Metric Optimization Driven Convolutional Neural Network for Age-Invariant Face Recognition. Pattern Recognit. 2018, 75, 51–62.
[57] Chatterjee, M.; Namin, A.S. Deep Reinforcement Learning for Detecting Malicious Websites. arXiv 2019, arXiv:1905.09207.
[58] Hamid, I.R.A.; Abawajy, J. Hybrid feature selection for phishing email detection. In Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing, Melbourne, Australia, 24–26 October 2011; Springer: Berlin/Heidelberg, Germany, 2011; Volume 7017, pp. 266–275.
[59] Li, T.; Li, J.; Liu, Z.; Li, P.; Jia, C. Differentially private Naive Bayes learning over multiple data sources. Inf. Sci. 2018, 444, 89–104.
[60] Martin, D.J.; Kifer, D.; Machanavajjhala, A.; Gehrke, J.; Halpern, J.Y. Worst-Case Background Knowledge for Privacy-Preserving Data Publishing. In Proceedings of the 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, Turkey, 15–20 April 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 126–135.
[61] Nazir, A.; Raza, S.; Chuah, C.N. Unveiling facebook: A measurement study of social network-based applications. In Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement, Vouliagmeni, Greece, 20–22 October 2008; ACM: New York, NY, USA, 2008; pp. 43–56.

[62] Liu, Z.; Wu, Z.; Li, T.; Li, J.; Shen, C. GMM and CNN Hybrid Method for Short Utterance Speaker Recognition. IEEE Trans. Ind. Inform. 2018, 14, 3244–3252.

[63] Ntoulas, A.; Najork, M.; Manasse, M.; Fetterly, D. Detecting spam web pages through content analysis. In Proceedings of the 15th International Conference on World Wide Web, Edinburgh, Scotland, 23–26 May 2006; ACM: New York, NY, USA, 2006; p. 83.

[64] Zhou, D.; Burges, C.J.C.; Tao, T. Transductive link spam detection. In Proceedings of the Adversarial Information Retrieval on the Web (AIRWeb), Banff, AB, Canada, 8 May 2007; p. 21.

[65] Wang, C.; Shen, J.; Liu, Q.; Ren, Y.; Li, T. A Novel Security Scheme based on Instant Encrypted Transmission for Internet-of-Things. Secur. Commun. Netw. 2018.

[66] Webb, S.; Caverlee, J.; Pu, C. Predicting Web Spam with HTTP Session Information. In Proceedings of the CIKM'08 17th ACM Conference on Information and Knowledge Management, Napa Valley, CA, USA, 26–30 October 2008; ACM: New York, NY, USA, 2008; pp. 339–348.

[67] Radlinski, F. Addressing malicious noise in clickthrough data. In Proceedings of the Learning to Rank for Information Retrieval Workshop at SIGIR, Ithaca, NY, USA, 2 December 2007.

[68] Huang, Z.; Liu, S.; Mao, X.; Chen, K.; Li, J. Insight of the protection for data security under selective opening attacks R. Inf. Sci. (NY) 2017, 412–413, 223–241.

[69] Munteanu, A.; Fotache, D.; Dospinescu, O. Information Systems Security Risk Assessment: Harmonization with International Accounting Standards. In Proceedings of the 2008 International Conference on Computational Intelligence for Modelling Control & Automation, Vienna, Austria, 10–12 December 2008; IEEE: Piscataway, NJ, USA, 2009; pp. 1111–1117.

[70] Asosheh, A.; Dehmoubed, B.; Khani, A. A new quantitative approach for information security risk assessment. In Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology, Dallas, TX, USA, 8–11 June 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 222–227.

[71] Guan, B.-C.; Lo, C.-C.; Wang, P.; Hwang, J.-S. Evaluation of information security related risks of an organization—The application of the multi-criteria decision-making method. In Proceedings of the IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, Taipei, Taiwan, 14–16 October 2003; IEEE: Piscataway, NJ, USA; 2003; pp. 168–175.

[72] Munir, R.; Mufti, M.R.; Awan, I.; Hu, Y.F.; Disso, J.P. Detection, mitigation and quantitative security risk assessment of invisible attacks at enterprise network. In Proceedings of the 2015 3rd International Conference on Future Internet of Things and Cloud, Rome, Italy, 24–26 August 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 256–263.

[73] Saripalli, P.; Walters, B. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5–10 July 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 280–288.

[74] Patel, N.J.; Jhaveri, R.H. Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A survey. In Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, 2–3 January 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 468–472.

[75] Thompson, H.H. Why security testing is hard. IEEE Secur. Priv. 2003, 1, 83–86.