Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μεθοδολογίες Διαχείρισης και Αποτίμησης Ευπαθειών «Vulnerability Assessment and Management Methodologies»**
Ονοματεπώνυμο Φοιτητή	**Καλογερόπουλος Γεώργιος**
Πατρώνυμο	**Ηλίας**
Αριθμός Μητρώου	**ΜΠΣΠ17027**
Επιβλέπων	**Παναγιώτης Κοντζανικολάου**

Ημερομηνία Παράδοσης: **Σεπτέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

Παναγιώτης Κοτζανικολάου Αναπληρωτής Καθηγητής	Δέσποινα Πολέμη Καθηγήτρια	Κωνσταντίνος Πατσάκης Αναπληρωτής Καθηγητής

ΠΕΡΙΛΗΨΗ

Η ευπάθεια, στην επιστήμη της Πληροφορικής, ορίζεται ως μια κατάσταση έκθεσης σε ενδεχόμενη επίθεση, υποβάθμιση ή βλάβη, φυσικά, ηλεκτρονικά ή συναισθηματικά. Ενώ οι δυο πρώτες περιπτώσεις εντάσσονται στο πλαίσιο της κυβερνοασφάλειας, οι ευπάθειες συναισθηματικής φύσεως εκδηλώνονται σε φαινόμενα χακτιβισμού, εθνοκρατικών επιθέσεων ή ακόμη και διαδικτυακού εκφοβισμού. Η κατανόηση αυτού του τοπίου ευπάθειας αποτελεί σημαντικό βήμα προς τον σχεδιασμό μιας κατάλληλης θέσης άμυνας και προστασίας, και σε πολλές περιπτώσεις, κατά την εξέταση πιθανών απειλών, τα όρια του φυσικού και ηλεκτρονικού κόσμου συγχέονται. Η παρούσα μεταπτυχιακή διατριβή μελετά το ζήτημα της ευπάθειας, κυρίως, ως προς τις πτυχές της διαχείρισης και της αποτίμησης. Πιο αναλυτικά, ενώ αναφέρονται τα βασικά χαρακτηριστικά της ευπάθειας, σχολιάζονται περαιτέρω οι μορφές που αυτή μπορεί να λαμβάνει, οι τρόποι εντοπισμού τούς, καθώς και οι διαδικασίες προφύλαξης από πιθανές επιθέσεις. Για πληρέστερη

κατανόηση των ζητημάτων αυτών, στο τέλος της εργασίας, αναφέρονται συγκεκριμένα παραδείγματα εντοπισμού και διαχείρισης ευπαθειών.

Λέξεις Κλειδιά: Ευπάθειες, Μεθοδολογίες Διαχείρισης, Αποτίμηση.

ABSTRACT

Vulnerability, in IT science, is defined as a state of exposure to possible attack, degradation or damage, physically, electronically or emotionally. While the first two cases are part of cybersecurity, vulnerabilities of an emotional nature are manifested in phenomena of hacking, ethnocentric attacks or even cyberbullying. Understanding this vulnerability landscape is an important step in designing an appropriate defense and protection position, and in many cases, when considering potential threats, the boundaries of physical and electronic worlds are confused. This master's thesis studies the issue of vulnerability, mainly in terms of management and valuation aspects. In more detail, while the main characteristics of the vulnerability are mentioned, the forms that it can take, the ways of their detection, as well as the procedures for

protection from possible attacks are further commented. For a more complete understanding of these issues, specific examples of vulnerability detection and management are provided at the end of the paper.

Keywords: Vulnerabilities, Management Methodologies, Valuation.

Περιεχόμενα

Περιεχόμενα Πινάκων

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

1.1 Η έννοια της ευπάθειας

Η ευπάθεια από μόνη της δεν καθιστά ένα μέσο επίθεσης (attack vector) αποτελεσματικό. Στην πραγματικότητα, η ύπαρξη ευπάθειας σημαίνει ότι υπάρχει κίνδυνος επικείμενης επίθεσης. Οι ευπάθειες δεν είναι τίποτα παραπάνω από ένα σφάλμα. Ένα σφάλμα στον κώδικα, στον σχεδιασμό, στην εφαρμογή ή στις ρυθμιστικές παραμέτρους, το οποίο είναι εκμεταλλεύσιμο και μπορεί να επιτρέψει τυχών κακόβουλη δραστηριότητα. Έτσι λοιπόν, χωρίς την ύπαρξη κάποιας κακόβουλης εκμετάλλευσης, μια ευπάθεια αποτελεί ένα δυνητικό πρόβλημα και χρησιμοποιείται για την εκτίμηση της επικινδυνότητας, προκειμένου να υπολογίσουμε τι θα μπορούσε να συμβεί.

Ανάλογα με το είδος της ευπάθειας, τη δυνατότητα εκμετάλλευσης της και την αξιολόγηση των πόρων του συστήματος, με βάση το σφάλμα, ο πραγματικός κίνδυνος θα μπορούσε είτε να περιοριστεί είτε να προκληθεί μια καταστροφή που εκκρεμεί. Παρ'όλο που αυτή είναι μια απλούστευση της διαδικασίας αξιολόγησης ενός πραγματικού κινδύνου, θέτει τη βάση των προνομιούχων δικαιωμάτων που αποκτά ένα μέσο επίθεσης (attack vector).

Οι ευπάθειες και η κακόβουλη εκμετάλλευση τους δεν είναι πάντα ίσης δυναμικής και ανάλογα με τα δικαιώματα του χρήστη ή της εφαρμογής, που βρίσκεται σε εκτέλεση, σε συνδυασμό και με την ευπάθεια, η ισχύς της εκμετάλλευσης και η αποτελεσματικότητα του μέσου της επίθεσης, μπορεί να αλλάζει. Για παράδειγμα, μια ευπάθεια σε έναν επεξεργαστή κειμένου, που χρησιμοποιείται από έναν απλό χρήστη μπορεί να έχει τελείως διαφορετικούς εκμεταλλεύσιμους κινδύνους σε σχέση με έναν που χρησιμοποιείται από έναν χρήστη-διαχειριστή. Ο ένας θα μπορούσε να είναι περιορισμένος στα προνόμια, που έχει ένας απλός χρήστης και ο άλλος θα μπορούσε να έχει πλήρη πρόσβαση διαχειριστή στον κεντρικό υπολογιστή. Εάν μάλιστα ο χρήστης χρησιμοποιεί έναν λογαριασμό διαχειριστή ή έχει άλλα υψηλά προνόμια, η εκμετάλλευση της ευπάθειας θα είχε ως αποτέλεσμα τη πρόσβαση σε ολόκληρο το περιβάλλον. Αυτό είναι κάτι που οι απειλητικοί παράγοντες (threat actors) στοχοποιούν με μεγάλη ευκολία.

Ποιος αντιμετωπίζει έλλειψη από βέλτιστες πρακτικές ασφάλειας και πώς μπορώ να τις αξιοποιήσω, ώστε να αποκτήσω πρόσβαση στο περιβάλλον του; Έχοντας αυτά κατά νου, οι ευπάθειες προκύπτουν σε όλα τα «σχήματα και μεγέθη». Μπορούν να στοχοποιήσουν το λειτουργικό σύστημα, προγράμματα, διαδικτυακές εφαρμογές, υποδομές και ούτω καθεξής. Επίσης έχουν τη δυνατότητα να στοχοποιούν πρωτόκολλα, μεταφορές και επικοινωνίες μεταξύ συστημάτων, που πραγματοποιούνται μέσω ενσύρματων δικτύων και Wi-Fi, μέχρι τόνους ραδιοφωνικών συχνοτήτων. Ωστόσο, δεν επιδέχονται όλες οι ευπάθειες κακόβουλη εκμετάλλευση. Μερικές είναι επαληθεύσεις της γενικής ιδέας που επικρατεί, άλλες είναι αναξιόπιστες και άλλες καθίστανται όπλα, ή επιπλέον λειτουργούν ως εργαλεία απόπειρας εμπορικής διείσδυσης ή ως λογισμικά ανοιχτού κώδικα. Μερικές βρίσκονται στο σκοτεινό διαδίκτυο (dark web) με σκοπό να πωληθούν για ηλεκτονικά εγκλήματα και άλλες χρησιμοποιούνται αποκλειστικά από εθνοκράτη έως ότου επιδιορθωθούν μέσω ενός λογισμικού ενημέρωσης (patches) ή δημοσιοποιηθούν (σκοπίμως ή όχι).

Επί της ουσίας, οι ευπάθειες μπορούν να εμφανισθούν οπουδήποτε και οποτεδήποτε. Αυτό που τις καθιστά σημαντικές είναι το πώς θα αξιοποιηθούν. Εάν δηλαδή η ίδια η ευπάθεια συντελέσει στη κακόβουλη εκμετάλλευσή της, η οποία συνεπάγεται τη μεταβίβαση των δικαιωμάτων/ προνομίων (εκμετάλλευση των δικαιωμάτων (privileged escalation) του χρήστη από άλλους), τότε ο κίνδυνος μιας επικείμενης επίθεσης είναι υψηλός. Προς το παρόν, λιγότερες από το 10% όλων των ευπαθειών της Microsoft, κατόπιν ενημέρωσης λογισμικού (patches), επιτρέπουν τέτοιου είδους εκμετάλλευση.

Καθώς όλο αυτό αποτελεί μια πραγματική απειλή, εκατοντάδες ενημερώσεις λογισμικού εκδίδονται ετησίως για τη διευθέτηση αυτών των επιθέσεων. Προκειμένου να γίνουν κατανοητοί οι κίνδυνοι και να ταυτοποιηθούν οι ευπάθειες, το τμήμα ασφαλείας χρησιμοποιεί πολλαπλά πρότυπα, για να εξετάσει τον κίνδυνο, την απειλή και τη σημασία μιας ευπάθειας.

1.1.1 Πρότυπα ασφαλείας

Τα πιο συνηθισμένα πρότυπα ασφαλείας είναι τα ακόλουθα:

• Common Vulnerabilities and Exposure (CVE)- Πρότυπο που αφορά ονόματα και περιγραφές από ευπάθειες της ασφάλειας πληροφοριών.

• Common Vulnerability Scoring System (CVSS)- Μαθηματικό σύστημα αξιολόγησης του κινδύνου των ευπαθειών που ενυπάρχουν στον τομέα της Τεχνολογίας Πληροφοριών / Πληροφορικής (Information Technology).

• The Extensible Configuration Checklist Description Format (XCCDF)- Γλώσσα προδιαγραφών (specification language) για τη σύνταξη λιστών ελέγχου ασφαλείας, σημείων αναφοράς και άλλων σχετικών αρχείων.

• Open Vulnerability Assessment Language (OVAL)- Μια κοινοτική προσπάθεια ασφάλειας πληροφοριών για τη τυποποίηση του τρόπου αξιολόγησης και υποβολής εκθέσεων σχετικά με το μηχανισμό των συστημάτων υπολογιστών.

• Information Assurance Vulnerability Alert (IAVA)- Ανακοίνωση για την ύπαρξη ευπάθειας σε μορφή ειδοποιήσεων, ενημερωτικών δελτίων και τεχνικών οδηγιών αναγνωρίσιμων από πιστοποίηση του Υπουργείου Άμυνας (DoD- CERT), τμήμα του Cyber Command των Ηνωμένων Πολιτειών και αποτελούν διατεταγμένο σημείο αναφοράς για την αποκατάσταση των ευπαθειών, το οποίο δρα εντός του κυβερνητικού πλαισίου και του Υπουργείου Άμυνας (DOD).

• Common Configuration Enumeration (CCE)- Παρέχει μοναδικούς κωδικούς αναφοράς σε ζητήματα που αφορούν τη ρύθμιση παραμέτρων του συστήματος, διευκολύνοντας τον γρήγορο και ακριβή συσχετισμό των δεδομένων ρύθμισης, σε πολλαπλές πηγές πληροφοριών και εργαλεία.

• Common Weakness Enumeration (CWE)- Παρέχει μια κοινή γλώσσα για την εξέταση, εύρεση και αντιμετώπιση των αιτιών των ευπαθειών της ασφάλειας λογισμικού, που εντοπίζονται στον κώδικα.

• Common Platform Enumeration (CPE)- Ένα δομημένο σύστημα ονοματοδότησης για πληροφοριακά (IT) συστήματα, λογισμικό και πακέτα.

• Common Configuration Scoring System (CCSS)- Ένα σύνολο από μέτρα που έχουν σχεδιαστεί για τη μέτρηση της σοβαρότητας των ζητημάτων, που προκύπτουν κατά τη διαμόρφωση ασφάλειας λογισμικού. Το πρότυπο ασφαλείας CCSS προέρχεται από το CVSS.

• Open Checklist Interactive Language (OCIL)- Αποτελεί ένα εννοιολογικό πλαίσιο για την αναπαράσταση ενός συνόλου ερωτήσεων που θα υποβληθούν σε έναν χρήστη και των διαδικασιών που αντιστοιχούν στην ερμηνεία των απαντήσεων σε αυτές τις ερωτήσεις, οι οποίες είναι μη-αυτοματοποιημένες. Ουσιαστικά, αποτελούν ερωτηματολόγια που απαιτούν ανθρώπινη παρέμβαση για να απαντηθούν, αλλά αποδίδονται σε μια τυποποιημένη γλώσσα σήμανσης/ προγραμματισμού (mark-up language).

• Asset Reporting Format (ARF)- Μοντέλο δεδομένων που εκφράζει έναν τύπο αναφοράς πληροφοριών σχετικά με τους πόρους του συστήματος (assets) και τη σχέση μεταξύ αυτών και των αναφορών. Το τυποποιημένο αυτό μοντέλο δεδομένων διευκολύνει την αναφορά, τη συσχέτιση και τη συγχώνευση πληροφοριών, σχετικά με τους πόρους του συστήματος (assets), για την παροχή λύσεων, τόσο σε κρατικούς, όσο και σε ανεξάρτητους οργανισμούς.

• Security Content Automation Protocol (SCAP)- Σύνοψη λειτουργικών προδιαγραφών βασισμένη σε υπάρχοντα πρότυπα. Για παράδειγμα, η επίσημη έκδοση 1.2 του προτύπου SCAP αποτελείται από τα πρότυπα XCCDF, OVAL, OCIL, ARF, CCE, CPE, CVE, CVSS και CCSS ως

μεμονωμένες εκδόσεις. Αυτό επιτρέπει σε κάθε πρότυπο να αναπτυχθεί ξεχωριστά, αλλά ταυτόχρονα διασφαλίζεται η ενοποίηση τους ως συλλογή προτύπων.

• Open Web Application Security Project (OWASP)- Διαδικτυακή κοινότητα που λειτουργεί μη κερδοσκοπικά, για την ανάπτυξη της ασφάλειας των διαδικτυακών εφαρμογών παρέχοντας

μεθοδολογίες, εργαλεία, τεχνολογία και μια προσέγγιση αξιολόγησης για παρόχους, οργανισμούς και τελικούς χρήστες.

Τα αποτελέσματα που προκύπτουν από όλες αυτές τις πληροφορίες, επιτρέπουν στους επαγγελματίες του τομέα ασφαλείας και στις ομάδες διαχείρισης, να μελετήσουν και να δώσουν προτεραιότητα στους κινδύνους, που προκύπτουν από τις ευπάθειες. Θα πρέπει λοιπόν να εμποδίσουν αυτή την εκμετάλλευση των ευπαθειών και να αποκλείσουν κάθε πιθανό μέσο επίθεσης που μπορεί να προκύψει απο τη κατάχρηση τους. Ωστόσο, χωρίς την ύπαρξη μιας κοινής γλώσσας (common language) και δομής, αναγκαίων για τη μελέτη των ευπαθειών, μια κοινή αξιολόγηση τους προς τους παρόχους, τις εταιρείες και τους οργανισμούς, με σκοπό την εφαρμογή βέλτιστων πρακτικών ασφαλείας, είναι σχεδόν ανούσια. Ένας κίνδυνος που μπορεί να αποβεί μοιραίος για ένα είδος επιχείρησης, μπορεί για μια άλλη επιχείρηση, να μην είναι καν υπαρκτός. Πρότυπα ασφαλείας, όπως το CVSS, επιτρέπουν τη σωστή επικοινωνία ενός τέτοιου κινδύνου επικείμενης επίθεσης, μεταξύ όλων των εμπλεκομένων φορέων.

1.1.2 Ρυθμιστικοί παράμετροι συστήματος

Τα ελαττώματα στις ρυθμιστικές παραμέτρους του συστήματος αποτελούν ένα ακόμη είδος ευπάθειας. Ωστόσο, τα ελαττώματα αυτά δεν επιδέχονται διόρθωση, παρά μόνο μείωση του κινδύνου. Πρότυπα, όπως το CCE, συμβάλλουν στην αναγνώριση και γνωστοποίηση τέτοιου είδους ελαττωμάτων, χρησιμοποιώντας μια κοινή τυποποιημένη γλώσσα προγραμματισμού.

Η διαφοροποίηση μεταξύ αποκατάστασης και απλού μετριασμού των ευπαθειών είναι καθοριστικής σημασίας. Η αποκατάσταση συνεπάγεται την ανάπτυξη ενημέρωσης λογισμικού (software patch) ή ενημέρωσης του μικροκώδικα/υλικολογισμικού (firmware) με σκοπό τη διόρθωση της ευπάθειας. Αυτή η διαδικασία ονομάζεται κοινώς Διαχείριση Ενημερώσεων Κώδικα (Patch Management).

Ο μετριασμός μιας ευπάθειας, σε απλά λόγια, αποτρέπει έως ένα βαθμό τον αντίκτυπο που μπορεί να έχει η εκμετάλλευση μιας ευπάθειας, κυρίως όταν η ενημέρωση κώδικα δεν είναι ακόμη διαθέσιμη. Μπορεί να είναι μια απλή αλλαγή σε κάποιο έγγραφο, σε κάποια πολιτική ομάδας (group policy) ή σε πιστοποιητικά ενημερώσεων. Τελικά, αυτές είναι ευπάθειες που οφείλονται σε αδύναμες ρυθμιστικές παραμέτρους του συστήματος (configuration) και μπορούν πολύ εύκολα να χρησιμοποιηθούν ως μέσο επίθεσης, από ένα κακόβουλο λογισμικό (threat actor).

Τα συνηθέστερα προβλήματα στις ρυθμιστικές παραμέτρους του συστήματος (configuration problems), τα οποία μπορούν να αξιοποιηθούν με κακόβουλο τρόπο, χαρακτηρίζονται από ελλειπείς προεπιλεγμένες βέλτιστες πρακτικές ασφαλείας. Αυτά θα μπορούσαν να είναι κενοί ή προεπιλεγμένοι κωδικοί πρόσβασης σε κάποια αρχική ρύθμιση των παραμέτρων του συστήματος, που αφορά διαχειριστικούς ή προνομιακής πρόσβασης λογαριασμους ή ευάλωτα κανάλια επικοινωνίας, που δεν έχουν κλειδώσει και προστατευτεί καταλλήλως, μετά από την αρχική εγκατάσταση, λόγω της έλλειψης κατάλληλης τεχνογνωσίας ή κάποιας παρατυπίας.

Ωστόσο, τα ελαττώματα αυτά στις παραμέτρους του συστήματος είναι ευμετάβλητα και «θεραπεύσιμα». Εάν βέβαια το σύστημα είναι σε μεγάλο βαθμό ελαττωματικό, τότε το κακόβουλο λογισμικό μπορεί να αποκτήσει δικαιώματα προνομιακής πρόσβασης, χωρίς να προβεί σε εκμετάλλευση του κώδικα και της ευπάθειας.

1.1.3 Εκμετάλλευση των ευπαθειών

Η εκμετάλλευση προϋποθέτει την ύπαρξη μιας ευπάθειας. Εάν δεν υπάρχει ένα τεκμηριωμένο ελάττωμα στο σύστημα, τότε η εκμετάλλευση δεν υφίσταται. Η εφαρμογή της πρακτικής της αντίστροφης μηχανικής (reverse engineering) από τους ειδικούς στον τομέα της ασφάλειας, για τον εντοπισμό και τη διόρθωση του είδους της εκμετάλλευσης σφάλματος, απαιτεί χρόνο. Στην ουσία αποτελεί μια αρκετά τεχνική και εγκληματολογικής φύσεως πρακτική.

Επίσης, όπως προαναφέρθηκε κιόλας, η εκμετάλλευση μιας ευπάθειας μπορεί να πάρει ποικίλα «σχήματα και μεγέθη». Μπορεί να χρησιμοποιηθεί για τη διαρροή πληροφοριών, εγκατάσταση κακόβουλου λογισμικού (malware), την παροχή εποπτείας, αλλά μακροπρόθεσμα ο στόχος είναι η δημιουργία ενός βιώσιμου και μη ανιχνεύσιμου προγεφυρώματος (beachhead) εντός ενός συστήματος ή η άμεση δημιουργία χάους και καταστροφής.

Η εκμετάλλευση των ευπαθειών μπορεί από μόνη της να αποβεί ιδιαίτερα καταστροφική, στις μεθόδους που χρησιμοποιεί κατά την εκτέλεση της, αλλά οι πιο επιτυχημένες κάνουν ακριβώς το αντίθετο. Μια εκμετάλλευση, η οποία μπορεί να αποκτήσει δικαιώματα πρόσβασης, να εκτελεί κώδικα, να επιτρέπει επιθέσεις πλευρικής κίνησης (lateral movement), τη διαρροή δεδομένων και ταυτόχρονα να είναι μη ανιχνεύσιμη, εξαρτάται σε μεγάλο βαθμό από την ίδια την ευπάθεια, αλλά βασίζεται επίσης στα δικαιώματα πρόσβασης της εκμετάλλευσης, όταν αυτή είναι σε δράση. Αυτός είναι και ο λόγος για τον οποίο η διαχείριση μια ευπάθειας, η αξιολόγηση του κινδύνου και η ενημέρωση λογισμικού είναι τόσο σημαντικές διαδικασίες.

Η εκμετάλλευση μιας ευπάθειας μπορεί μόνο να δράσει εντός ενός συστήματος που βρίσκεται σε κίνδυνο εξαιτίας αυτής. Στην περίπτωση που δεν υπάρχει κάποιου είδους ευπάθεια λόγω αποκατάστασης του συστήματος, η εκμετάλλευση δεν μπορεί να εκτελεστεί. Εάν τα δικαιώματα πρόσβασης του χρήστη ή της εφαρμογής με την ευπάθεια είναι περιορισμένα (τυπικός χρήστης) και η εκμετάλλευση των δικαιωμάτων αυτών δεν είναι πιθανή, τότε η δυνατότητα επίθεσης είναι περιορισμένη. Ωστόσο η εκμετάλλευση, ακόμη κι όταν αφορά τα δικαιώματα πρόσβασης του τυπικού χρήστη, μπορεί να προκαλέσει καταστροφές με τη μορφή κάποιου κακόβουλου λογισμικού (ransomware) ή κάποιας άλλης κακόβουλης επίθεσης.

Ευτυχώς, στη συντριπτική τους πλειοψηφία, οι ευπάθειες που αξιοποιούνται κακόβουλα, μπορούν να μετριαστούν περιορίζοντας και μόνο τα δικαιώματα πρόσβασης και κατά συνέπεια ελαχιστοποιώντας τις πιθανότητες ανάπτυξης επιθέσεων. Οι διάφοροι τρόποι εκμετάλλευσης των ευπαθειών έχουν μεγαλύτερο ποσοστό επιτυχίας όταν αφορούν τη παραβίαση δικαιωμάτων των προνομιούχων χρηστών-διαχειριστών ή κάποιο σφάλμα, που επιτρέπει στην ίδια την εκμετάλλευση να αναβαθμίσει τα δικαιώματα. Επομένως, η παύση των εκμεταλλεύσεων αυτών μπορεί να επέλθει με την αποκατάσταση των ευπαθειών (διαχείριση ενημέρωσης λογισμικού), το μετριασμό τους (αν υπάρχει η δυνατότητα) και τον περιορισμό των δικαιωμάτων/ προνομίων. Ο περιορισμός των δικαιωμάτων/ προνομίων δεν διορθώνει την ύπαρξη ευπάθειας, αλλά τη πιθανότητα επιτυχούς επίθεσης και δεν αποτελεί από μόνος του έναν αποδεκτό τρόπο διόρθωσης σφαλμάτων ασφαλείας.

1.2 Μορφές ευπάθειας

Όπως αναφέρθηκε και προηγουμένως, υπάρχουν τρία είδη καταστάσεων ευπάθειας, που μπορούν να εντοπιστούν σε οποιοδήποτε πόρο του συστήματος:

- Ενεργή (Active) – Το σφάλμα «τρέχει» ενεργά σε κάποιον πόρο του συστήματος (asset) και στους καταναλωτικούς πόρους. Η ενεργή ευπάθεια σημαίνει ότι μια επιτυχής εκμετάλλευση, θα μπορούσε να θέσει σε κίνδυνο το σύστημα (ανάλογα με τους περιορισμούς της ευπάθειας).
- Αδρανής (Dormant) –Το σφάλμα κατοικεί στον κεντρικό υπολογιστή, αλλά δεν καταναλώνει ενεργά καθόλου πόρους. Μια αδρανής ευπάθεια θα μπορούσε να είναι οπουδήποτε, από μια απενεργοποιημένη υπηρεσία, μέχρι μια εγκατεστημένη εφαρμογή η οποία δεν χρησιμοποιείται τη δεδομένη χρονική στιγμή. Εάν η εφαρμογή εκτελείται, η ευπάθεια δεν είναι πια

αδρανής και θα μπορούσε να χαρακτηριστεί πλέον ως ενεργή κατά τη διάρκεια του χρόνου εκτέλεσής της.

• Φορέας (Carrier) – Σε αυτή τη περίπτωση, το σφάλμα αντιστοιχεί στη μακράν πιο ασαφή κατηγοριοποίηση ευπάθειας, καθώς περιέχει ένα υποθετικό στοιχείο. Ένας φορέας μπορεί να εμφανιστεί με διπλή μορφή σε κάποιον πόρο του συστήματος, αν και δεν είναι ρυθμισμένος ακόμη, είτε ως αδρανής είτε ως ενεργός. Για την αλλαγή της κατάστασης απαιτούνται επιπλέον μέτρα, αλλά δεν υπάρχει ανάγκη για χρήση εξωτερικών μέσων ή για σύνδεση στο Διαδίκτυο. Για παράδειγμα, η προσθήκη ιδιοτήτων στους πόρους ενός συστήματος Windows μπορεί να πραγματοποιηθεί, με τη χρήση των απαραίτητων διαπιστευτηρίων και χωρίς τη βοήθεια εξωτερικών πόρων. Από τη στιγμή που θα ολοκληρωθεί η ρυθμιστική αλλαγή, μια ευπάθεια μπορεί να βρίσκεται σε αδρανή ή ενεργή κατάσταση μέχρι να πραματοποιηθεί η αποκατάσταση της.

Καμία από αυτές τις έννοιες δεν αναφέρεται κατά την αξιολόγηση μιας ευπάθειας, παρά το γεγονός ότι η κοινή λογική μας λέει – ορθώς – ότι οι ενεργές ή δυνητικά εκμεταλλεύσιμες ευπάθειες θα έπρεπε να επιδέχονται πρώτες αποκατάσταση.

Τα σύγχρονα πρότυπα δεν λαμβάνουν υπόψη τις τρεις αυτές καταστάσεις, κατά την αναφορά ευπαθειών, οπότε εξαρτάται αποκλειστικά από τη δραστηριότητα του παρόχου ασφαλείας το να αναπτυχθούν λειτουργικά πρότυπα, με σκοπό την επιτυχή υλοποίηση αξιολόγησης. Με αυτόν τον τρόπο, η υφιστάμενη κατάσταση θυμίζει σε μεγάλο βαθμό τις πρώιμες τεχνικές αξιολόγησης της δεκαετίας του ‘90.

Τα παρακάτω αποτελούν πολύ σημαντικές λεπτομέρειες σχετικά με κάθε μια από αυτές τις τρεις καταστάσεις ευπάθειας, οι οποίες θα πρέπει πάντα να λαμβάνονται υπόψη.

1.2.1 Ενεργές ευπάθειες

Οι ενεργές ευπάθειες συνιστούν σαφώς τη μεγαλύτερη απειλή, για οποιονδήποτε οργανισμό. Αυτές αποτελούν τρωτά σημεία, τα οποία φέρονται ως ενεργά στο λειτουργικό σύστημα ή σε μια εφαρμογή (στον καθημερινό κώδικα που τρέχει) και είναι ευάλωτα σε δυνητική εκμετάλλευση.

Στα σημερινά εργαλεία αξιολόγησης ευπάθειας, όλες οι ευπάθειες χαρακτηρίζονται ως ενεργές, ανεξάρτητα από τα μέτρα περιορισμού, που λαμβάνονται από τον τελικό χρήστη. Είναι αρμοδιότητα των διαχειριστών των εργαλειών αυτών, να γνωρίζουν, ότι θα έπρεπε να αποκλείουν μια ευπάθεια ύστερα από περιορισμό του κινδύνου ή να αλλάζουν χειροκίνητα τα αποτελέσματα της εκτίμησης του κινδύνου, γνωρίζοντας την εγγενή αδρανή κατάσταση μιας ευπάθειας.

Οι τεχνολογίες σάρωσης εντοπίζουν απλώς μια έκδοση αρχείου, έναν κατατεμαχισμό (hash), ένα κλειδί μητρώου ή ένα πακέτο και δεν εξετάζουν τη κατάσταση του προγράμματος. Αυτό αποτελεί τη βάση του προβλήματος.

1.2.2 Αδρανείς ευπάθειες

Οι αδρανείς ευπάθειες αποτελούν έναν άγνωστο κίνδυνο για τον οργανισμό έναν πραγματικό κίνδυνο που θα μπορούσε να αποβεί το ίδιο σημαντικός με μια ενεργή ευπάθεια.

Δεν είναι σπάνιο φαινόμενο ένα πρόγραμμα, ενώ παραμένει αδρανές για μεγάλο χρονικό διάστημα, μετά να εκτελεστεί και να παρουσιάσει έναν πραγματικό κίνδυνο στον οργανισμό. Σκέψου τις desktop εφαρμογές, όπως είναι η Microsoft Help, WinZip ή Adobe Acrobat, οι οποίες, όπως πολλές άλλες, μπορεί να μην εκτελούνται πολύ συχνά. Η εφαρμογή δεν δημιουργεί κάποια απειλή όταν δεν χρησιμοποιείται, αλλά έχει τη δυνατότητα να αποτελέσει κίνδυνο.

Μια αδρανής ευπάθεια παρουσιάζεται ως ένας άγνωστος κίνδυνος, έως ότου χρησιμοποιηθεί και η χρήση της να μπορεί να αξιολογηθεί ποσοτικά. Σε κάθε δεδομένη στιγμή, οι εφαρμογές είναι «Αδρανείς», αλλά παρ’όλα αυτά τα αρχεία που αντιστοιχούν σε αυτές (όπως το

PDF➤ Acrobat Reader) μπορούν να τεθούν σε προτεραιότητα. Σαφώς, εάν ένα πρόγραμμα και τα αρχεία που το συνοδεύουν δεν χρησιμοποιούνται καθόλου, τότε ο κίνδυνος είναι μηδενικός.

Η κοινή λογική θα πρόσταζε την απεγκατάσταση, κατάργηση ή τη τοποθέτηση κάποιου άλλου ελέγχου περιορισμού του κινδύνου γύρω από το πρόγραμμα, αλλά στην πραγματικότητα αυτό μπορεί να μην είναι πάντα δυνατό.

Για παράδειγμα, δεν μπορείς να απεγκαταστήσεις το Microsoft Help ή στη περίπτωση του Red Hat Linux να αφήσεις ένα αντίγραφο του προηγούμενου πυρήνα στο δίσκο, ως αντίγραφο ασφαλείας.

Επομένως, το να εντοπίσεις απλά την ευπάθεια, αποτελεί μια λογική διαδικασία εντός των συστημάτων αξιολόγησης, τα οποία χρησιμοποιούμε σήμερα. Ωστόσο, το πώς η εφαρμογή και η σχετική ευπάθεια χρησιμοποιούνται πραγματικά αντιστοιχεί στη μεταβολή της ευπάθειας από αδρανή σε ενεργή και κανένα σύστημα αξιολόγησης δεν το έχει εξετάσει αυτό, μέχρι και σήμερα.

Είναι στην ευχέρεια του κάθε παρόχου ασφαλείας, το να εκθέσει και να θέσει σε προτεραιότητα τις πληροφορίες, με τον δικό του μοναδικό τρόπο.

1.2.3 Φορείς Ευπάθειας

Οι ευπάθειες φορείς λειτουργούν όπως ένας ιός στο ανθρώπινο σώμα. Είναι πάντοτε παρούσες, όχι πάντα ανιχνεύσιμες και θα μπορούσαν να ενεργοποιηθούν με διάφορους και ποικίλους τρόπους, προκαλώντας σοβαρή βλάβη.

Η πιο συνηθισμένη μορφή ευπάθειας φορέα είναι τα προσωρινά αποθηκευμένα αρχεία εγκατάστασης. Για παράδειγμα, οι σύγχρονες εκδόσεις λειτουργικών συστημάτων της Microsoft και εφαρμογών αποθηκεύουν προσωρινά τα αρχεία του προγράμματος εγκατάστασης, στο σκληρό δίσκο, σε περίπτωση που προστεθούν λειτουργίες ή έστω πραγματοποιηθεί κάποιο σχετικό αίτημα για πρώτη φορά. Η διαδικασία εγκατάστασης θα μπορούσε ενδεχομένως να περιλαμβάνει και την εγκατάσταση ευπαθών στοιχείων, τα οποία έπειτα θα πρέπει να επισημανθούν από μια σάρωση αξιολόγησης ευπάθειας. Οι τροποποιήσεις θα μπορούσαν τότε να είναι είτε σε αδρανή είτε σε ενεργή κατάσταση. Ένα χαρακτηριστικό παράδειγμα θα ήταν η εγκατάσταση του .NET Framework ή ακόμη και του Microsoft WSUS από μια διαδικασία εγκατάστασης προσωρινής μνήμης.

Ένας χρήστης θα χρειαστεί να τρέξει μια ενημέρωση συστήματος Windows ή να χρησιμοποιήσει ένα εργαλείο, για τη διαχείριση των ενημερώσεων κώδικα, κατά την αποκατάσταση των νέων ευπαθειών. Το πρόβλημα σχετίζεται με αδρανή αρχεία εγκατάστασης (τα οποία φέρονται ως ευάλωτα ύστερα από μια σάρωση ευπάθειας) και αρχεία αντιγράφου ασφαλείας, τα οποία βρίσκονται στο σύστημα και δημιούργησαν την ευπάθεια εξαρχής.

Παρ'όλο που αυτή η έννοια μπορεί να μοιάζει διφορούμενη, είναι πολύ συχνή όσον αφορά στο λογισμικό bloatware που βρίσκεται εγκατεστημένο σε προεπιλεγμένες εικόνες και κινητές συσκευές.

Σε πολλές περιπτώσεις, τα προγράμματα δεν είναι πλήρως εγκατεστημένα, μέχρι τη πρώτη φορά που χρησιμοποιούνται (και μέχρι την ενδεχόμενη αποδοχή μιας σύμβασης EULA) και συνεπώς μια υπηρεσία αξιολόγησης μπορεί να αποτύχει στην εύρεση τους, εξαιτίας της αποκλειστικής χρήσης ενός πακέτου παροχών (unique vendor packaging).

1.3 Καταστάσεις ευπάθειας και κίνδυνος

Η διαδικασία αξιολόγησης ευπάθειας αναγνωρίζει κινδύνους ασφαλείας στους πόρους του συστήματος, οι οποίοι εμφανίζονται με τη μορφή ευπαθειών λογισμικού, απουσίας ενημερώσεων κώδικα και τρωτών σημείων στις ρυθμιστικές παραμέτρους. Η αξιολόγηση μπορεί να

χρησιμοποιηθεί στα πάντα, από λειτουργικά συστήματα και εφαρμογές λογισμικού μέχρι εφαρμογές Παγκόσμιου Ιστού (Web) και εικονικά περιβάλλοντα. Τα δεδομένα που προκύπτουν κατηγοριοποιούνται ως κίνδυνοι ευπάθειας. Υπάρχουν πολλά πρότυπα για την υποβολή αναφορών σχετικών με αυτούς τους κινδύνους κι ακόμη περισσότερα ρυθμιστικά πρότυπα παγκοσμίου επιπέδου, τα οποία αξιολογούν τα αποτελέσματα και ορίζουν συμφωνίες, σε υπηρεσιακό επίπεδο, που αφορούν την αποκατάσταση του συστήματος και τον καθορισμό προτεραιοτήτων.

Η διαδικασία αξιολόγησης ευπάθειας έχει σημειώσει τρομερή εξέλιξη από τότε που ξεκίνησε, στα τέλη της δεκαετίας του ’90.

Αρχικά, οι συσκευές ελέγχονταν μέσω του Πρωτοκόλλου TCP/IP και μιας τεχνολογίας σάρωσης δικτύου, με τη χρήση διαδοχικών λιστών στόχων και διευθύνσεων IP.

Στις μέρες μας η τεχνολογία έχει εξελιχθεί, ώστε να γίνεται χρήση κατανεμημένων συστημάτων (distributed state machines), στόχευση με τη χρήση προηγμένων λογισμικών σύνδεσης για τεχνολογίες όπως η Amazon AWS ή η Vmware καθώς και να υπάρχει η δυνατότητα εις βάθος αξιολόγησης των στόχων, μέσω τεχνολογιών, που βασίζονται σε κάποιον διαμεσολαβητή και μιας ποικιλίας μηχανισμών διαπίστευσης.

Μια ατυχής έλλειψη, που αντιμετωπίζει όλη αυτή η εξέλιξη, είναι το γεγονός ότι οι μηχανισμοί αξιολόγησης (με εξαίρεση τις περιβαλλοντικές μετρήσεις του CVSS) βασίζονται στη σοβαρότητα της ίδιας της ευπάθειας και δεν επηρεάζονται από ελέγχους για τον περιορισμό του κινδύνου ή από τη κρισιμότητα, που φέρει η ευπάθεια, σε πόρους (asset) υπηρεσιών και επιχειρησιακών διαδικασιών. Ενώ, στοιχεία όπως το πώς εντοπίστηκε η ευπάθεια και τι σημαίνει πραγματικά για τους πόρους του συστήματος, (asset), αποτελούν προβληματισμούς που έχουν αγνοηθεί.

Ας πάρουμε, για παράδειγμα, το σφάλμα CVE-2014-160 με βαθμολογία CVSS μόνο 5,0. Για πολλούς, αυτό το σφάλμα είναι γνωστό με την ονομασία «Heartbleed».

Αυτή η ιστορική, αξιοσημείωτη ευπάθεια μπορεί να παρουσιαστεί σε πολλούς διαφορετικούς τύπους συστημάτων· ωστόσο όλοι τους αντιμετωπίζουν τον ίδιο βαθμό κινδύνου.

Το σφάλμα μπορεί να εντοπιστεί σε μια διαδικτυακή υπηρεσία ή σε μια βιβλιοθήκη του τοπικού συστήματος, αλλά ανεξάρτητα από το εάν εμφανίζεται ως ενεργό στη μνήμη και επιδέχεται δυνητική εκμετάλλευση ή ως ανενεργό και ανεκμετάλλευτο σε μια βιβλιοθήκη στον δίσκο, οι λύσεις αξιολόγησης ευπάθειας θα αναφέρουν και τις δυο περιπτώσεις ως κρίσιμες παρά το βαθμό επικινδυνότητας, σύμφωνα με τις προδιαγραφές του κλάδου.

Η βασική διαφορά εδώ είναι οι ενεργές διαδικασίες. Οι κλασσικές λύσεις δικτύου, που αφορούν την αξιολόγηση ευπάθειας, δεν λαμβάνουν υπόψη τις διαφορετικές «καταστάσεις» ευπάθειας.

Η παρούσα ενότητα εξετάζει τρεις πιθανές καταστάσεις ευπάθειας, οι οποίες εντοπίζονται μέσω διαδικασιών αξιολόγησης ευπάθειας, και τον αντίκτυπο των στρατηγικών αποκατάστασης ευπάθειας στις επιχειρήσεις.

1.3.1 Κίνδυνος ευπάθειας ανάλογα με την κατάσταση

Οι κλασσικές λύσεις αξιολόγησης ευπάθειας εκτιμούν τα αποτελέσματα, που προκύπτουν με βάση τον υπάρχοντα κίνδυνο. Οι προηγμένες λύσεις περιέχουν δεδομένα που παρέχονται από τους τελικούς χρήστες, προκειμένου να αξιολογήσουν τον κίνδυνο, που προσβάλλει κάποιον πόρο του συστήματος (ή τη διεύθυνση IP).

Η «Business Ready Solutions» συγκεκτρώνει αυτές τις πληροφορίες σε λογικές ομάδες και μετά αξιολογεί μια ολόκληρη ομάδα, σε σύγκριση με τις άλλες ομάδες εντός του οργανισμού, με σκοπό τη κατανόηση μιας λογικής ομαδοποίησης, έναντι μιας άλλης. Αυτή η πρακτική μπορεί να χρησιμοποιηθεί για τα πάντα, από τη διαδικασία καθορισμού προτεραιοτήτων, μέχρι συμφωνίες σε υπηρεσιακό επίπεδο.

Οι κύριοι μηχανισμοί αξιολόγησης κινδύνου, αναφορικά με οποιοδήποτε προϊόν, ακολουθούν τη παρακάτω μεθοδολογία:

- Proprietary Risk Score¬ – Ένας δείκτης κινδύνου ο οποίος καθορίζεται από τον πάροχο και είναι είτε αριθμητικός είτε βαθμονομημένος [για παράδειγμα, γίνεται χρήση ορολογίας όπως χαμηλός (low), μέτριος (medium), υψηλός (high), κρίσιμος (critical) ή μέγιστος (extreme)]. Αυτός ο μηχανισμός εμφανίστηκε στην αρχή της διαδικασίας σάρωσης για την αξιολόγηση ευπάθειας, προτού εξελιχθούν τα πρότυπα έτσι ώστε να δίνουν τη δυνατότητα σε όλους τους παρόχους, να αξιολογούν τις ευπάθειες με τον ίδιο τρόπο.
- CVSS – Το πρότυπο Common Vulnerability Scoring System, αναπτύχθηκε για πρώτη φορά το 2005 για να αντιμετωπίσει τις ελλείψεις των συστημάτων αξιολόγησης, τα οποία βασίζονται σε κάποιο πάροχο, και να δημιουργήσει ένα πρωτόκολλο (έναν μαθηματικό υπολογισμό διανύσματος), για τον καθορισμό της πραγματικής σημασίας μιας ευπάθειας με τυποποιημένο τρόπο. Το πρότυπο έχει εξελιχθεί και περιλαμβάνει διάφορα κριτήρια, που

αφορούν χρονικούς και περιβαλλοντικούς παράγοντες. Ο υπολογισμός των αποτελεσμάτων της αξιολόγησης εξακολουθεί να πυροδοτεί αντιπαραθέσεις στον κλάδο και οι πρόσφατες δοκιμαστικές εκδόσεις επιχειρούν να ανταποκριθούν σε σύγχρονες τεχνολογίες και σε τεχνικές περιορισμού του κινδύνου, ως μέρος της διαδικασίας υπολογισμού.

- PCI DSS – Το Payment Card Industry (PCI) Data Security Standard (DSS) περιλαμβάνει μια τροποποιημένη έκδοση του προτύπου CVSS προκειμένου να αξιολογήσει τον κίνδυνο για τα αρχεία PCI ROCs (Records of Compliance). Αυτή η τροποποιημένη έκδοση θέτει παράγοντες, όπως την επίθεση Denial of Service, εντός του πλαισίου αξιολόγησης, με σκοπό την αντιμετώπιση προβλημάτων όπως είναι η μειωμένη διαθεσιμότητα ιστότοπου και διακοπή λειτουργίας ή η απώλεια δεδομένων του κατόχου κάρτας.
- IAVA – Το Information Assurance Vulnerability Alert δεν αποτελεί από μόνο του μηχανισμό αξιολόγησης. Το IAVA είναι μια ειδοποίηση, από το τμήμα Cyber Command των Ηνωμένων Πολιτειών, για την ύπαρξη ευπάθειας στο λογισμικό εφαρμογής ή στα λειτουργικά συστήματα, η οποία θα πρέπει να αντιμετωπιστεί από τις συνεργαζόμενες κυβερνητικές υπηρεσίες. Η υπηρεσία Defense Information Systems Agency έχει αναπτύξει και διατηρεί μια βάση δεδομένων IAVA για να διασφαλίσει έναν μηχανισμό θετικού ελέγχου για τους διαχειριστές του συστήματος, ώστε να λάβουν, να αναγνωρίσουν και να συμμορφωθούν με τις ειδοποιήσεις ευπάθειας του συστήματος. Εντός της βάσης δεδομένων IAVA, οι ευπάθειες εκφράζονται μέσω μιας Κατηγορίας Αξιολόγησης, η οποία κυμαίνεται από το 1 μέχρι το 4, για την εκτίμηση της επικινδυνότητας. Το DISA ορίζει τις τιμές, αλλά κατά κανόνα αυτές οι τιμές ακολουθούν τις συστάσεις του CVSS.

Οι παραπάνω μηχανισμοί αξιολόγησης χρήζουν θεμελιώδους σημασίας, για τη κατανόηση του κινδύνου, καθώς αυτοί διασφαλίζουν ότι ανεξαρτήτως του πώς εμφανίζεται μια ευπάθεια σε έναν πόρο του συστήματος, αυτή αξιολογείται με τον ίδιο τρόπο.

Για παράδειγμα, εάν στον πόρο ενός συστήματος Microsoft Windows το σύστημα έχει εγκατεστημένα πολλαπλά προγράμματα περιήγησης Διαδικτύου, ακόμη κι αν μόνο ένα από αυτά χρησιμοποιείται από τους τελικούς χρήστες, το αποτέλεσμα που προκύπτει από την αξιολόγηση ευπάθειας, είναι ακριβώς το ίδιο για όλες τις περιπτώσεις προγραμμάτων περιήγησης, ανεξάρτητα από το εάν ένα πρόγραμμα περιήγησης χρησιμοποιείται ενεργά, εάν είναι αδρανές και μόλις έχει εγκατασταθεί στο σύστημα ή μεταφέρθηκε ως μέρος του λειτουργικού συστήματος και δεν είναι καν πλήρως εγκατεστημένο.

Σύμφωνα με τους οδηγούς διαχείρισης ευπάθειας, απαιτείται η αποκατάσταση όλων των κρίσιμων ευπαθειών. Σε αυτή τη περίπτωση, υπάρχει ένας σαφής καθορισμός προτεραιοτήτων όσον αφορά το πρόγραμμα περιήγησης που είναι σε χρήση αλλά δεν μπορεί να πραγματοποιηθεί ακριβής μέτρηση του κινδύνου, σε κανένα από τα βασικά συστήματα αναφοράς ευπάθειας, που είναι διαθέσιμα.

Επιπλέον, οι υπάρχοντες μηχανισμοί μέτρησης κινδύνου αποτυγχάνουν (εκτός από τον χειροκίνητο αποκλεισμό μιας ευπάθειας ή τη τροποποίηση των αποτελεσμάτων του συστήματος αξιολόγησης CVSS ανά πόρο συστήματος και ευπάθεια) να αντιμετωπίσουν τη περίπτωση των ευπαθειών, οι οποίες έχουν περιοριστεί καταλλήλως μέσω της απενεργοποίησης σχετικών υπηρεσιών. Αυτό αποτελεί μια έγκυρη τεχνική περιορισμού του κινδύνου, ενώ μια λύση αξιολόγησης ευπάθειας, δεν μπορεί απαραίτητα να διακρίνει μια πιθανότητα ύπαρξης ευπάθειας, από ένα ενεργό σφάλμα εντός του συστήματος.

Επομένως, οι τεχνικές αξιολόγησης της ευπάθειας πρέπει να εξελιχθούν και να αποκαταστήσουν τον πόρο του συστήματος και τις εφαρμογές που χρησιμοποιούνται, αντί απλώς να πραγματοποιούν ελέγχους για αρχεία, κλειδιά μητρώου, banners και εγκατεστημένα πακέτα. Αυτό θα οδηγήσει σε ένα μέλλον με στρατηγική σημασία, αναφορικά με τις τεχνολογίες αξιολόγησης ευπάθειας και τις τρείς πιθανές καταστάσεις ευπάθειας.

1.4 Δομή της διατριβής

Στο παρόν και πρώτο κεφάλαιο της εργασίας, θεωρείται ότι δόθηκε σαφώς το περιεχόμενο της έννοιας της ευπάθειας και έγιναν αντιληπτοί οι πιθανοί κίνδυνοι που μπορεί να υφίστανται και δυνητικά να εμφανίζονται στα ψηφιακά περιβάλλοντα. Οι επιθέσεις αυτές, είναι σε θέση να προκαλούν σημαντικές βλάβες στα ηλεκτρονικά συστήματα, ενώ υπάρχουν και περαιτέρω δεινές επιβαρύνσεις οι οποίες μπορεί και να έχουν και οικονομικό ή άλλο αντίκτυπο.

Στο δεύτερο κεφάλαιο της εργασίας, έτσι, αναλύονται τα στάδια που χρειάζεται να ακολουθηθούν προκειμένου να αναπτυχθεί ένα πρόγραμμα που θα είναι σε θέση να προφυλάξει ένα σύστημα από τις ευπάθειες, καθώς και το πλαίσιο αποτίμησής τους. Πιο συγκεκριμένα, αφού γίνεται λόγος για την ιεράρχηση των καταστάσεων και τις αρχές κατηγοριοποίησης των ευπαθειών, παρέχεται πληροφόρηση για όλα τα στάδια ενός προγράμματος διαχείρισης ευπαθειών που ξεκινά από τον σχεδιασμό και καταλήγει στην πλήρη ανάπτυξη. Επιπρόσθετα, γίνεται αναφορά για τις διαδικασίες ελέγχου και αποτίμησης των ευπαθειών που όπως και οι ίδιες οι ευπάθειες, μπορεί να λαμβάνουν διάφορες μορφές. Σε ξεχωριστή ενότητα γίνεται, επιπρόσθετα, λόγος για την σάρωση της ευπάθειας, ενώ αναφέρονται και οι τυχόν περιορισμοί κατά την διαδικασία αυτή. Στο κεφάλαιο αυτό, αναφέρονται και οι κανονισμοί που υπάρχουν αναφορικά με τα πρότυπα αναφοράς μιας ευπάθειας.

Στο τρίτο κεφάλαιο της εργασίας, σχολιάζονται τα βασικά εργαλεία αξιολόγησης των ρυθμιστικών παραμέτρων ενός συστήματος, όπως το SCAP, καθώς και όσα αφορούν στην μέτρηση του κινδύνου εμφάνισης ευπάθειας, όπως είναι το CVE και το OVAL, μεταξύ άλλων.

Η κατανόηση και η εφαρμογή των τεχνικών όρων που αναφέρονται στην εργασία, γίνεται πιο σαφής με την παράθεση συγκεκριμένων παραδειγμάτων που περιλαμβάνονται στο κεφάλαιο 4, ενώ στο πέμπτο και τελευταίο κεφάλαιο της εργασίας, εξάγονται τα συμπεράσματα από το σύνολο των αναφορών και παρατίθενται μελλοντικές προτάσεις για έρευνα.

ΚΕΦΑΛΑΙΟ 2. ΕΠΙΣΚΟΠΗΣΗ ΜΕΘΟΔΟΛΟΓΙΩΝ ΚΑΙ ΠΛΑΙΣΙΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΠΟΤΙΜΗΣΗΣ ΕΥΠΑΘΕΙΩΝ

2.1 Ιεράρχηση καταστάσεων

Αυτή η ορολογία αναπτύχθηκε για τη κατηγοριοποίηση των καταστάσεων ευπάθειας, για τους σκοπούς αυτού του βιβλίου. Αν και η διαδικασία ιεράρχησης των καταστάσεων είναι σαφής, βάσει αυτής της συζήτησης, αφήνει ορισμένα κενά, όταν μεταφραστεί σε ρυθμιστικά πρότυπα.

Για παράδειγμα, το PCI DSS αναφέρει ρητά ότι όλες οι σημαντικές ευπάθειες θα πρέπει να αποκαταστηθούν εντός 30 ημερών. Ενώ λοιπόν αυτό φαίνεται απολύτως λογικό για ένα σύστημα που βρίσκεται εντός του πεδίου εφαρμογής του PCI, δεν λαμβάνει υπόψη μεγάλο μέρος συστημάτων, τα οποία βρίσκονται εκτός του PCI , αλλά που όμως βρίσκονται υπό τη διαχείριση ενός οργανισμού που χρησιμοποιεί τις ίδιες διαδικασίες.

Θα μπορούσε ακόμη να τεθεί και το επιχείρημα ότι μια αδρανής ευπάθεια παρουσιάζει την ίδια επικινδυνότητα (βάσει μιας τυπικής αξιολόγησης) και ότι μια ευπάθεια φορέας θα έπρεπε να υπόκεινται σε κατάλληλους ελέγχους τροποποιήσεων και σωστή διαχείριση ενημερώσεων κώδικα.

Ωστόσο, στη πραγματικότητα, αυτό συμβαίνει σπάνια.

Ο προσδιορισμός στοιχείων αναφορικά με αυτές τις καταστάσεις ευπάθειας βοηθά τους οργανισμούς σχετικά με τα εξής:

- Ιεράρχηση των υψηλότερων κινδύνων ευπάθειας πρώτα – ανεξάρτητα από τις τυπικές ελλείψεις της αξιολόγησης·
- Επίσπευση της αποκατάστασης ευπαθειών οι οποίες αντιστοιχούν σε πραγματικούς ενεργούς κινδύνους – ανεξαρτήτως από το εάν μια εκμετάλλευση είναι δημόσια διαθέσιμη.
- Ποσοτικοποίηση των ευπαθειών με βάση τη πραγματική χρήση της εφαρμογής και όχι μόνο τις θεωρητικές εκμεταλλεύσεις.
- Αύξηση της ενημέρωσης σχετικά με τις επιπρόσθετες ενέργειες, που μπορεί να απαιτούνται κατά τον έλεγχο των αλλαγών, που προκύπτουν όταν το λειτουργικό σύστημα ή η εφαρμογή, προβαίνει σε τροποποιήσεις, οι οποίες επηρεάζουν την ασφάλεια.
- Αναγνώριση του μερικώς διαμορφωμένου ή εγκατεστημένου λογισμικού παρόχου, το οποίο θα μπορούσε να αποτελέσει κίνδυνο εάν επιτρεπόταν η εκτέλεση του.

Ένα ενδεχομένως περιττό ακρωνύμιο θα μπορούσε να είναι το «ADC»: Ενεργές, Αδρανείς και Ευπάθειες Φορείς, σε σειρά προτεραιότητας.

Κατά την επανεξέταση μιας αναφοράς ευπαθειών, πρέπει αυτές να αντιμετωπιστούν, ως ένα πολύ σημαντικό μέρος της διαδικασίας ιεράρχησης των κινδύνων και να διαπιστωθεί εάν είναι εφικτή, η ακριβής αναγνώριση των διαφορετικών τύπων ευπάθειας. Εάν όντως μια εφαρμογή λειτουργεί (ενεργή), θα πρέπει αυτή, να τίθεται πάντα σε υψηλότερη προτεραιότητα, από μια που δεν χρησιμοποιείται ποτέ (αδρανής).

2.2 Αρχές κατηγοριοποίησης ευπαθειών

Από τα τέλη της δεκαετίας του ‘90, πάροχοι, τελικοί χρήστες και κυβερνήσεις έχουν καταβάλλει προσπάθειες, για την κατά τρόπο συνεπή, κατηγοριοποίηση και γνωστοποίηση ευπαθειών. Ως επακόλουθο, προκύπτει μια πληθώρα προτύπων, που έχουν ως σκοπό, τη γνωστοποίηση των ευπαθειών και την ανεξαρτήτως παρόχου αποθήκευση, επεξεργασία και εκτέλεση, δημοσίων ανακοινώσεων από κυβερνητικά όργανα.

Παρ' όλο που έχει δημιουργηθεί ένα ευρύ φάσμα οργανισμών, για τη γνωστοποίηση των ευρημάτων, λίγοι είναι αυτοί που παρέχουν στήριξη, για τις δημοσιοποιημένες πληροφορίες. Οι πιο γνωστοί περιγράφονται στον πιο κάτω πίνακα. Αυτοί αποτελούν τους οργανισμούς, οι οποίοι γνωστοποιούν και καταγράφουν όλα τα χαρακτηριστικά και τους δείκτες μέτρησης, που αφορούν έναν πιθανό κίνδυνο.

Πίνακας 1. Φορείς γνωστοποίησης ευπαθειών

Abbreviation	Full Name	Description	URL
US-CERT	United States Computer Emergency Readiness Team	US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cyber security information with trusted partners around the world.	https://www.us-cert.gov/
CERT	Software Engineering Institute at Carnegie Mellon University	CERT is a division of the Software Engineering Institute (SEI) that studies and solves problems with widespread cyber security implications. CERT collects, analyzes, and validates emerging vulnerabilities to common computing platforms, and will broadly notify operators of vulnerabilities as well as provide mitigation and remediation guidance.	https://www.cert.org

(*continued*)

Abbreviation	Full Name	Description	URL
DISA	Defense Information Systems Agency	DISA is a combat support agency of the Department of Defense (DoD). The agency is composed of military personnel from the Army, Air Force, navy, and Marine Corps; and defense contractors. The agency provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of military operations.	http://www.disa.mil http://www.disa.mil/Cybersecurity http://www.disa.mil/Cybersecurity/Secure-Configuration-Guidance
bUGTRAQ	bugtraq or bugtrag Identifier	SecurityFocus has been a mainstay in the security community since 1999 and supports the back end for bugtraq IDs. Their technology provides a high volume, full-disclosure mailing list for announcement of new vulnerabilities; and a database to view history and discussions on each potential threat.	http://www.securityfocus.com

(*continued*)

VULnERABILITy AUThoRITIES

Abbreviation	Full Name	Description	URL
MITRE	Mitre	The MITRE Corporation is a not-for-profit company that operates multiple federally funded research and development centers. It provides standards for vulnerability classifications and scoring like CVE that is used throughout the industry.	https://www.mitre.org https://cve.mitre.org
nVD	national Vulnerability Database	The nVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation protocol (SCAp). The nVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.	

Image source:
www.us-cert.gov
www.cert.org
www.disa.mil/cybersecurity/secure-configuration-guidance
www.securityfocus.com
www.mitre.org
www.cve.mitre.org

2.3 Πρόγραμμα διαχείρισης ευπάθειας- στάδια

Με τη πρόσφατη έξαρση των παραβιάσεων σημαντικών δεδομένων, οι οργανισμοί που ασχολούνται με θέματα ασφάλειας, κατανοούν ότι η οικονομική τους βιωσιμότητα και η διασφάλιση των επιχειρησιακών δραστηριοτήτων τους, εξαρτώνται από την αποτελεσματική διαχείριση κινδύνων, που αφορούν την ασφάλεια Τεχνολογίας Πληροφοριών (IT).

Λαμβάνοντας υπόψη τις πιθανές επιπτώσεις μιας παράβασης, πολλοί οργανισμοί στηρίζονται σε πρωτοβουλίες διαχείρισης ευπάθειας και συμμόρφωσης, προκειμένου να διαφυλάξουν τις σημαντικές τους πληροφορίες, να προστατεύσουν τα ευπαθή συστήματα και να επιδείξουν συμμόρφωση, με τις κανονιστικές απαιτήσεις. Αυτές οι προσπάθειες γίνονται πιο πολύπλοκες, λόγω της ανάπτυξης νέων ευπαθειών ασφάλειας, που προκύπτουν από μια πληθώρα εφαρμογών, συσκευές που ανήκουν σε εργαζομένους, φορητούς υπολογιστές,

κοινωνικά δίκτυα, αποθηκευτικό χώρο cloud και άλλες επεκτεινόμενες επιφάνειες έκθεσης σε επίθεση.

Υπάρχουν σημαντικοί ρυθμιστικοί κανόνες συμμόρφωσης, όπως οι PCI, HIPAA και Sarbanes-Oxley, που επίσης επιβάλλουν συγκεκριμένους ελέγχους ασφαλείας, σχετικά με τη διαχείριση ευπάθειας. Δυστυχώς, δεν υπάρχει τρόπος διαφυγής από τη σκληρή πραγματικότητα ότι η παραβατικότητα επιφέρει κυρώσεις, αναστολή επιχειρηματικών δραστηριοτήτων και άλλες έμμεσες απώλειες. Επιπλέον, ο συντονισμός των εσωτερικών διαδικασιών ασφαλείας με κανονισμούς και η παροχή σημαντικών αναφορών στους αρμόδιους της διαχείρισης και τους ελεγκτές αποτελούν εμφανώς χρονοβόρες και δαπανηρές εφαρμογές.

Ενώ σε γενικές γραμμές, ένας οργανισμός δεν μπορεί να θέσει υπό τον έλεγχο του τις απειλές που αντιμετωπίζει, αυτός μπορεί να ανταποκριθεί σε αυτές τις απειλές, περιορίζοντας τους σχετικούς κινδύνους, μέσω της μείωσης είτε των τρωτών σημείων που απειλούνται είτε του πιθανού αντίκτυπού τους στις επιχειρήσεις. Για την εκτέλεση ενός τέτοιου προγράμματος, υπάρχουν τέσσερα στάδια:

1. Σχεδιασμός,
2. Ανάπτυξη,
3. Εφαρμογή
4. και Λειτουργία, όπως απεικονίζονται και στον πίνακα που ακολουθεί.

Πίνακας 2. Στάδια προγράμματος διαχείρισης ευπάθειας

Phase	Objectives	Task Items
design	Requirements Goals Budget	➢ Review business requirements for the vulnerability processes ➢ Create a VM strategy with timelines, priorities, measurements, and goals ➢ Determine a budget and cost analysis for the VM program
develop	Requirements Plan Creation Selection	➢ Translate business requirements into technical requirements ➢ Vulnerability plan creation & validation ➢ Selection and procurement of supporting technologies
deploy	Deployment Team Training Handoff	➢ Install, test, and validate VM program ➢ Educate and train key stakeholders ➢ Transition VM plan to operational and security staff
operate	Operate Measure Expand	➢ Operate VM program (Assess, Prioritize, Report, Remediate) ➢ Measure effectiveness of program versus stated goals ➢ Expand scope and mature VM program over life cycle

image source: www.bakertilly.com/

2.3.1 Σχεδιασμός

Ο ρόλος μιας ομάδας, που ασχολείται με την ασφάλεια Τεχνολογίας Πληροφοριών (IT) είναι να συνεργαστεί με βασικά στελέχη του οργανισμού, ώστε να αναπτύξουν επιχειρησιακές

δραστηριότητες και σχέδια εφαρμογής νέων έργων ασφαλείας, καθώς και να πραγματοποιήσουν αξιολογήσεις για την ύπαρξη κινδύνων, στα υπάρχοντα συστήματα ελέγχου και στα οργανωμένα πληροφοριακά συστήματα. Από που ξεκινάει λοιπόν αυτή η διαδικασία;

Βάσει κοινής λογικής θα έπρεπε να ξεκινήσει με τους πιο σημαντικούς πόρους, οι οποίοι θα μπορούσαν να έχουν πολύ σοβαρό αντίκτυπο στο σύστημα, εάν είχαν εκτεθεί. Αυτοί είναι, που θα έχρηζαν άμεσης προστασίας. Αλλά με ποιο τρόπο θέτεις σε προτεραιότητα αυτούς τους πόρους; Πώς τους προστατεύεις; Πώς αξιολογείς τα υφιστάμενα και οργανωμένα συστήματα ελέγχου; Τα πάντα βρίσκονται στη λεπτομέρεια και η διερεύνηση του σχεδιασμού και του προγραμματισμού, θα πραγματοποιηθεί σε επόμενα κεφάλαια.

2.3.2 Ανάπτυξη

Κατά τη διαδικασία ανάπτυξης, η ομάδα που ασχολείται με θέματα ασφαλείας,αναθέτει στους τεχνικούς ασφαλείας και διαχείρισης ευπαθειών, τη μετατροπή της στρατηγικής και του σχεδιασμού, που αφορούν στις τεχνικές απαιτήσεις της επιχείρησης και μπορούν να εφαρμοστούν και να επιβληθούν σε όλα τα τμήματα. Καθώς η διαδικασία ξεκινάει και διασφαλίζεται η έγκριση των τεχνικών απαιτήσεων, η ομάδα θα πρέπει να συνεργαστεί και με άλλα τμήματα ώστε να εξεταστούν οι δυνατότητες συντονισμού συστημάτων (integration) και αυτοματοποίησης διαδικασιών, (automation,) με τη βοήθεια υφιστάμενων διαδικασιών τεχνολογίας πληροφοριών, συμπεριλαμβανομένης της διαχείρισης των πόρων του συστήματος, της διαδικασίας ελέγχου ασφαλείας, των αξιολογήσεων ελεγκτικών διαδικασιών και του ελέγχου των τροποποιήσεων.

Ο σκοπός του σχεδιασμού θα πρέπει να είναι η συμβολή στη λειτουργικότητα της ασφάλειας όσον αφορά στη λήψη καθημερινών αποφάσεων, εντός του οργανισμού. Ένας από τους καλύτερους τρόπους για να επιτευχθεί αυτό το έργο είναι ο συντονισμός με τις υφιστάμενες διαδικασίες και συστήματα ώστε να ενσωματωθεί η διαδικασία διαχείρισης ευπαθειών, στο πλαίσιο της συνήθους επιχειρησιακής δραστηριότητας.

2.3.3 Εφαρμογή

Η ανάπτυξη, η εξακρίβωση της δυνατότητας υλοποίησης και η εφαρμογή οποιασδήποτε νέας τεχνολογίας θα πρέπει να ελέγχεται, να πραγματοποείται επανεξέταση κώδικα (εάν απαιτείται) και να αξιολογείται για την ύπαρξη κινδύνων πριν την εφαρμογή του προϊόντος.

Σε αυτή τη διαδικασία περιλαμβάνεται ακόμη και η ίδια η διαδικασία και οι εφαρμογές διαχείρισης ευπάθειας! Αυτή συμπεριλαμβάνει, εκτός από αξιολογήσεις ευπάθειας, μέτρα ασφαλείας, που αφορούν στη διαμόρφωση του συστήματος και τη δημιουργία ζωνών ασφαλείας εντός του περιβάλλοντος. Συχνά κατά τη διάρκεια του σταδίου εφαρμογής, οι οργανισμοί θα συνεργαστούν με παρόχους και εξωτερικούς συνεργάτες, προκειμένου να εκτελέσουν τη διαδικασία εφαρμογής, σε κάποιο τμήμα του περιβάλλοντος δικτύου.

Σε αυτό το διάστημα η ομάδα που ασχολείται με τη διαδικασία εφαρμογής δύναταινα παρέχει κατάρτιση, σχετικά με την ανάπτυξη των εσωτερικών πόρων, που αφορούν την ολοκλήρωση της ευρύτερης ανάπτυξης και εφαρμογής - λογισμικού - και να εκπαιδεύσει το τεχνικό προσωπικό, ώστε να αναλάβει τη συνεχή διαχείριση και συντήρηση μετά την εφαρμογή. Επιπλέον, κατά το στάδιο εφαρμογής, οι βελτιστοποιήσεις στις επιχειρησιακές διαδικασίες μπορούν να οριστικοποιηθούν και τα κενά ασφαλείας, μπορούν να αναγνωριστούν και να περιοριστούν κατά την ανάπτυξη τους.

2.3.4 Λειτουργία

Τώρα που η διαδικασία αξιολόγησης έχει σαφώς καθοριστεί, οι κάτοχοι πόρων συστήματος έχουν ενημερωθεί, η κατάρτιση έχει ολοκληρωθεί και οι διαδικασίες έχουν μεταβιβαστεί στους τεχνικούς ευπάθειας, οι οποίοι θα επιβλέπουν τις καθημερινές λειτουργίες, ξεκινάει η δύσκολη δουλειά.

Πολύ συχνά εντοπίζονται οργανισμοί που προσπαθούν να περάσουν απευθείας στο στάδιο – «Λειτουργία» χωρίς να έχει γίνει κατάλληλος σχεδιασμός και κατάρτιση ή χωρίς τη συναίνεση από ειδικούς και κατόχους πόρων συστήματος. Αυτό συνήθως οδηγεί σε εσφαλμένες προσδοκίες καθώς και διαφωνίες μεταξύ της ομάδας, που ασχολείται με θέματα ασφάλειας και των άλλων ομάδων, που πλήττονται από την ύπαρξη ευπάθειας.

Κατά τη δημιουργία ενός επιτυχούς προγράμματος διαχείρισης ευπάθειας, είναι απαραίτητος ο σχεδιασμός τόσο του τι θα χρειαστεί, για την έκδοση και εφαρμογή του προγράμματος, όσο και για το τι πραγματικά απαιτείται, για τη διαχείριση των συστημάτων και την εκτέλεση της κατάλληλης αποκατάστασης σε συνεχή βάση. Αυτό απαιτείται για τη σωστή διατήρηση του προγράμματος καθώς και για τη πλήρη ανάπτυξη μιας λύσης, για την αντιμετώπιση της ευπάθειας, πέρα από αυτά τα τέσσερα στάδια.

2.3.5 Πλήρης ανάπτυξη- κατηγορίες ανάπτυξης

Στόχος κάθε εφαρμογής είναι η πλήρης ανάπτυξη, σε μια κατάσταση που καθιστά αδιάκοπες τις μεθόδους, τις διαδικασίες και τη ροή εργασιών, αναφορικά με τις καθημερινές επιχειρησιακές δραστηριότητες. Ένα επιτυχές πρόγραμμα διαχείρισης ευπάθειας προϋποθέτει τη δημιουργία ενός κύκλου ζωής που θα λειτουργεί ανεξαρτήτως κλάδου και κανονισμών. Ο πίνακας που δίνεται στην συνέχεια, περιγράφει αυτή τη γενική ιδέα.

Πίνακας 3. Κύκλος ζωής προγράμματος διαχείρισης ευπάθειας

Descriptions					
Solution	**Assessments**	**Patch**	**Reporting**	**Ownership**	
Assessments are security, business, and regulatory compliance-driven	Assessments drive compliance requirements	Patch is measured in compliance terms	Regulatory compliance reporting	Auditors are included in ownership	
Dynamic response based on multiple data sources	Assessments are evaluated for business partners and third party technology	Service level agreements are generated internally and for third parties	Reporting expands into risk and threats for the business units	Team response is included in ownership tasks	
Vulnerability solution integrates with bi-directional with third party solutions	Assessments have multiple data feeds and sources	Resources are segmented or isolated until patching occurs	Reporting and events are present in third party governance and security solutions	Ownership between departments is documented and followed	
Network scanners are supplemented with agents and third party tools	Assessments can be triggered by events or API	DevOps processes can remediate as needed	Reporting is scheduled and provided to teams ad hoc	Clear ownership and fully documented policies	
Centralized enterprise vulnerability management with network scanners	Assessments are scheduled (null session and credential)	Remediation workflow is defined	Vulnerability and patch management reporting is consistent	Base policies and SLA's are in place	
Vulnerability assessment solution partially deployed	Assessments on an as needed basis	Reactive remediation and patching	Simple reporting on coverage generated ad hoc	Basic directives to minimize risk	
Minimal or no assessments, tools, or policies	Targeted or manual checks only	Incomplete remediation and mitigation	No measurement or reporting	Inconsistent management directives	

image source: https://blog.rsisecurity.com/what-are-the-stages-of-the-vulnerability-management-lifecycle/

Όσον αφορά τις κατηγορίες ανάπτυξης, αυτές έχουν ως κάτωθι:

• Χωρίς εκτιμήσεις κινδύνου: Η έλλειψη οποιασδήποτε διαδικασίας και πολιτικής για τη διαχείριση ευπάθειας και πώς να μετριάσετε τυχόν απειλές που εντοπίζονται.

• Ad Hoc Αξιολογήσεις: Οι λύσεις μπορεί να είναι διαθέσιμες στην ομάδα και οι αξιολογήσεις διεξάγονται σε βάση που απαιτείται ανάλογα με την απειλή της ημερήσιας ή ρυθμιστικής έρευνας. Δεν υπάρχει καθιερωμένη διαδικασία ή πολιτική που να επιβλέπει την πρωτοβουλία για την ασφάλεια.

• Περιοδικές Αξιολογήσεις: Καθιερωμένη διαδικασία και πολιτικές για προγραμματισμένες αξιολογήσεις. Τα αποτελέσματα έχουν μια ροή εργασίας για αποκατάσταση, αλλά παρέχουν μόνο ένα στιγμιότυπο εγκαίρως με βάση προγραμματισμένες αξιολογήσεις.

• Συνεχής παρακολούθηση και αξιολόγηση ενεργού κινδύνου: Οι πολιτικές και οι διαδικασίες είναι ώριμες και επιτρέπουν αξιολογήσεις ευπάθειας σε πραγματικό χρόνο και ενεργό εντοπισμό ευπαθών εφαρμογών. Όλα τα αποτελέσματα αντιμετωπίζονται με παραδοσιακή βαθμολογία και δεν έχουν προτεραιότητα με βάση πραγματικές απειλές ούτε ενεργά κατορθώματα.

• Προτεραιότητα στην απειλή και τον κίνδυνο: Οι πραγματικές απειλές για την ασφάλεια συνδυάζονται με εντοπισμένες ευπάθειες ανεξάρτητα από την πηγή: ad hoc, περιοδική ή συνεχής παρακολούθηση. Αυτές οι πληροφορίες επιτρέπουν την ιεράρχηση της συνάφειας που βασίζεται σε απειλές για την επιχείρηση και τις εφαρμογές.

• Μετριασμός επιθέσεων και στρατηγική αποκατάσταση: Με βάση όλες τις πληροφορίες ευπάθειας και απειλής που συλλέγονται, οι στρατηγικές αποκατάστασης και μετριασμού μπορούν να αυτοματοποιηθούν. Αυτό είναι ένα βασικό βήμα για την ενσωμάτωση.

2.3.6 Περιγραφές

• Λύση – Η ωριμότητα της ανάπτυξης και η πιθανή χρήση δυνατοτήτων και δυνατοτήτων εντός της λύσης.

• Αξιολογήσεις – Η τεχνική πολυπλοκότητα και οι απαιτήσεις που απαιτούνται από την επιχείρηση για την επιτυχή εκτέλεση μιας αξιολόγησης ευπάθειας και τη δημιουργία ενός προγράμματος διαχείρισης ευπάθειας.

• Patch – Οι στρατηγικές αποκατάστασης και μετριασμού δεν βασίζονται μόνο στην απειλή, την κρισιμότητα, αλλά και τον δυνητικό αντίκτυπο στην επιχείρηση με βάση τους στόχους και τις πραγματικές απειλές.

• Υποβολή εκθέσεων – Η αναφορά πληροφοριών ευπάθειας ωριμάζει ανά επιχειρηματική γραμμή και σχετίζεται με τα ενδιαφερόμενα μέρη έναντι της τεχνικής και της στόχευσης μόνο σε ομάδες ασφάλειας και λειτουργίας.

• Ιδιοκτησία – Η κυριότητα των δεδομένων και οι διαδικασίες και οι πολιτικές καθορίζονται σε όλα τα επίπεδα του οργανισμού και έχουν μετρήσιμη ροή εργασίας για κάθε ομάδα για να βελτιώσουν τους χρόνους απόκρισης.

2.4 Έλεγχοι της ευπάθειας

2.4.1 Ψευδώς θετικοί έλεγχοι

Οι πάροχοι εργαλείων διαχείρισης των ευπαθειών χρησιμοποιούν ποικίλους όρους, για να περιγράψουν τους πραγματικούς τους ελέγχους, τα πρωτόκολλα και τις ρυθμίσεις σάρωσης. Αυτές οι πρακτικές δεν συνηθίζουν να χρησιμοποιούνται ως λύση και όροι όπως έρευνα, πολιτικές, επιλογές, μη ασφαλής έλεγχος, ομάδες μπορούν να πάρουν διαφορετική σημασία στο πλαίσιο διαφορετικών εργαλείων. Ενώ οι διαφοροποιήσεις είναι μηδαμινές, όλοι οι πάροχοι χρησιμοποιούν, εκτός των καθιερωμένων όρων, ορισμένες κοινές ορολογίες. Ένας πολύ σημαντικός όρος φέρει τον τίτλο «Ψευδώς Θετικό». Μια ψευδώς θετική διάγνωση είναι μια θετικά φερόμενη αναγνώριση ευπάθειας, σε κάποιον πόρο του συστήματος, ενώ στη πραγματικότητα ο κίνδυνος δεν υφίσταται ή η απειλή έχει εξαλειφθεί ή μετριαστεί.

Οι πάροχοι διαχείρισης των ευπαθειών κάνουν μεγάλη προσπάθεια, να κρατήσουν το ποσοστό τους όσο χαμηλότερο γίνεται, αλλά υπάρχει μια πληθώρα αιτιών, που μπορούν να προκαλέσουν μια ψευδώς θετική διάγνωση:

• Ανεπαρκώς τεκμηριωμένοι έλεγχοι ευπαθειών, οι οποίοι δεν καλύπτουν όλες τις πτυχές της ευπάθειας, τα χαρακτηριστικά της και τις λειτουργικές της παραμέτρους.

• Το backporting (Η μεταφορά) των ενημερώσεων του κώδικα ασφαλείας, το οποίο εμποδίζει την αναγνώριση της ευπάθειας.

• Έλεγχοι για την ύπαρξη ευπάθειας που φέρουν αόριστα ή ανεπαρκή αποτελέσματα και δημιουργούν αμφιβολίες για τα ευρήματα.

• Αντικατάσταση εκδόσεων και ενημερώσεων, που δεν αναγνωρίζουν τις διάφορες εκδόσεις ενός προϊόντος ή νεότερες ενημερώσεις που έχουν εφαρμοσθεί για την αποκατάσταση της ευπάθειας.

Γενικά, οι ψευδώς θετικές διαγνώσεις αποτελούν ιδιαιτέρως ανεπιθύμητα αποτελέσματα, που προκύπτουν ύστερα από τον έλεγχο για την ύπαρξη ευπαθειών. Ο περιορισμός τους είναι καθοριστικής σημασίας, καθώς μπορεί να αποτρέψει την εξέταση ενός στην πραγματικότητα, ανύπαρκτου προβλήματος. Για τα ψευδώς θετικά αποτελέσματα, που δεν εξαλείφονται εύκολα, πολλοί πάροχοι εργαλειών διαχείρισης ευπάθειας προσφέρουν μια λειτουργία που ονομάζεται «Εξαιρέσεις» (“Exclusions”). Αυτή η λειτουργία υποβαθμίζει την αξία του ευρήματος και το ανάγει ως μιας χαμηλής σημασίας αναγνωρισμένη ευπάθεια, εξαιτίας μιας ψευδώς θετικής διάγνωσης ή άλλων λόγων, που δεν μπορεί να διορθωθεί από τον κατασκευαστή.

Οι ψευδώς θετικές διαγνώσεις αποτελούν ένα σημαντικό μέρος των συζητήσεων μας, καθώς έχουμε την ανάγκη να γνωρίζουμε αν ο εντοπισμός μιας ευπάθειας είναι έγκυρος· αλλά στη πραγματικότητα, κάθε ηλεκτρονικό περιβάλλον έχει να αντιμετωπίσει το ποσοστό των ψευδώς θετικών διαγνώσεων, που του αντιστοιχεί κατά τον κύκλο της ζωής του. Από τη πλευρά του παρόχου δε, κατά την εκτέλεση ελέγχων ευπάθειας, οι πάροχοι προτιμούν την υπερέκθεση ενός ευρήματος σφάλματος ακόμη κι αν είναι ψευδώς θετικό, έναντι της δημιουργίας ενός αισθήματος λανθασμένης ασφάλειας που προκύπτει από έναν ψευδώς αρνητικό έλεγχο.

2.4.2 Ψευδώς αρνητικοί έλεγχοι

Το αντίθετο ενός ψευδώς θετικού ελέγχου είναι ένας ψευδώς αρνητικός, αλλά όχι για τους λόγους που μπορεί να φαντάζεται κανείς. Ο «Ψευδώς Αρνητικός» έλεγχος γίνεται όταν υπάρχει μια ευπάθεια, αλλά η εκτίμηση που γίνεται για την αναγνώριση της αποτυγχάνει.

Υπάρχουν πολλοί λόγοι που οδηγούν σε έναν ψευδώς αρνητικό έλεγχο:

• Ο πάροχος να μην ελέγχει την ύπαρξη ευπάθειας.

• Ο πάροχος να μην υποστηρίζει ελέγχους, για μια συγκεκριμένη ευπάθεια σε ένα συγκεκριμένο λειτουργικό σύστημα, εφαρμογή ή πλατφόρμα.

• Ο έλεγχος του παρόχου να είναι ανεπαρκής και να μην καλύπτει όλες τις απαιτήσεις.

• Τα διαπιστευτήρια και η επικύρωση που απαιτώνται για την εγκυροποίηση του ελέγχου, να είναι λανθασμένα ή και απόντα.

• Η χρονική καθυστέρηση του παρόχου να εκδόσει έναν αξιόπιστο έλεγχο, επηρεάζοντας έτσι τις διαδικασίες αξιολόγησης των ευπαθειών.

Οι ψευδώς αρνητικοί έλεγχοι αποτελούν τη χειρότερη ενδεχόμενη εξέλιξη για έναν οργανισμό. Μια ευπάθεια παραλείπεται από τις αξιολογήσεις και τις αναφορές που γίνονται, και εάν η απειλή είναι αρκετά μεγάλη, ο κίνδυνος είναι σχεδόν αδύνατο να τεθεί σε προτεραιότητα και να αντιμετωπιστεί. Ενώ τα τελευταία χρόνια ο αριθμός των ψευδώς αρνητικών ελέγχων, ανάμεσα στις λύσεις που προσφέρουν οι πάροχοι, έχει μειωθεί σημαντικά, ακόμη αποτελεί ένα πραγματικό πρόβλημα, το οποίο κάνει την εμφάνιση του κατά καιρούς. Για τη διαχείριση αυτού του προβλήματος, κάποια ηλεκτρονικά περιβάλλοντα δεν βασίζονται σε μια μόνο λύση, όσον αφορά την αναγνώριση των ευπαθειών.

Οποιαδήποτε ευπάθεια έχει εντοπιστεί κατά τη διάρκεια μιας συγκεκριμένης διαδικασίας επίλυσης σφάλματος και όχι μιας άλλης, τότε μπορεί να κατηγοριοποιηθεί είτε ως ψευδώς θετική είτε ως ψευδώς αρνητική, εάν οι συνθήκες αξιολόγησης είναι ίσης δυναμικής.

2.5 Αξιολόγηση ευπάθειας

Η αξιολόγηση μιας ευπάθειας είναι η διαδικασία, κατά την οποία εκτιμάται ο κίνδυνος που επιφέρουν οι ευπάθειες, οι οποίες συναντώνται σε ένα ευρύ φάσμα υπολογιστών, εφαρμογών και συσκευών, εντός ενός οργανισμού.

Το αποτέλεσμα που προκύπτει από τη διαδικασία σάρωσης της ευπάθειας, επισημαίνει την πιθανή επιφάνεια έκθεσης σε επίθεση, η οποία μπορεί να αξιοποιηθεί από τους χάκερς/ εισβολείς για την απόκτηση παράνομης πρόσβασης σε συστήματα, εφαρμογές και δεδομένα.

Για τη συλλογή των σχετικών πληροφοριών, οι οργανισμοί έχουν την επιλογή να προβούν σε μια ενεργή σάρωση ευπάθειας, σε μια παθητική σάρωση ευπάθειας ή σε έναν συνδυασμό των δύο αυτών τεχνικών.

Σε μια ενεργή σάρωση ευπάθειας, υπάρχουν δύο μεθοδολογίες, που χρησιμοποιούνται για την εκτέλεση της αξιολόγησης ευπάθειας, ανεξαρτήτως της αξιολόγησης των διορθωτικών ενημερώσεων κώδικα (patch assessment) ή της επαλήθευσης συμμόρφωσης.

Η μια φιλοσοφία περιστρέφεται γύρω από την ανάγκη διείσδυσης στο σύστημα, προκειμένου να αποδειχθεί η ευπάθεια του και η άλλη χρησιμοποιεί τις διαθέσιμες πληροφορίες, για να συμπεράνει τη κατάσταση της ευπάθειας.

Στο επίκεντρο μακροχρόνιων συζητήσεων έχουν βρεθεί τα πλεονεκτήματα και των δύο τύπων σάρωσης ευπάθειας, καθώς και τα πιθανά τους μειονεκτήματα.

Συνοπτικά, δεδομένου ότι ένας σαρωτής αξιολόγησης ευπάθειας μπορεί και προσομοιώνει μια επίθεση, κάθε μια από τις δύο αυτές μεθόδους, αντικατοπτρίζει τον τρόπο με τον οποίο ο επιτιθέμενος θέτει σε κίνδυνο τον κεντρικό υπολογιστή.

2.5.1 Ενεργή σάρωση ευπάθειας

Η Ενεργή Σάρωση Ευπάθειας προϋποθέτει ότι το λογισμικό απομακρυσμένης σάρωσης επικοινωνεί και συνδέεται με έναν κόμβο δικτύου. Σε αυτό το σημείο, ο σαρωτής ευπάθειας στέλνει δεδομένα στους κόμβους του δικτύου, και εξετάζοντας τα αποτελέσματα, αξιολογεί εάν ένας συγκεκριμένος κόμβος, εντός του δικτύου, παρουσιάζει κάποιο σφάλμα.

Ένας διαχειριστής δικτύου μπορεί επίσης να χρησιμοποιήσει έναν ενεργό σαρωτή για να προσομοιώσει μια επίθεση στο δίκτυο, εντοπίζοντας αδυναμίες, τις οποίες θα μπορούσε να ανακαλύψει ενδεχομένως ένας χάκερ, ή για να εξετάσει έναν κόμβο που έχει δεχθεί επίθεση, ώστε να ελέγξει τον τρόπο με τον οποίο ένας χάκερ παραβίασε την ασφάλεια.

Οι ενεργοί σαρωτές μπορούν να δράσουν αυτόνομα, προκειμένου να επιλύσουν θέματα ασφαλείας, όπως για παράδειγμα μπλοκάροντας μια ενδεχομένως επικίνδυνη διεύθυνση IP, σε συνδυασμό και με άλλες λύσεις.

2.5.2 Παθητική σάρωση ευπάθειας

Οι παθητικοί σαρωτές μπορούν να αναγνωρίσουν τα ενεργά λειτουργικά συστήματα, τις εφαρμογές και τις θύρες (ports) εντός ενός δικτύου, παρακολουθώντας τη δραστηριότητα του δικτύου, προκειμένου να κρίνουν κατά πόσο υπάρχουν ευπάθειες. Αυτές οι σαρώσεις συνήθως εφαρμόζονται, χρησιμοποιώντας κατοπτρική θύρα (port mirroring), ενσωματωμένα TAP δικτύου (inline network taps) ή θύρα προσδιορισμού (port spanning).

Παρ'όλο που οι παθητικοί σαρωτές μπορούν να δώσουν πληροφορίες σχετικά με ευπάθειες, δεν μπορούν να προβούν σε επίλυση των προβλημάτων από μόνοι τους, καθώς αυτοί απλώς παρακολουθούν τη κίνηση δεδομένων του δικτύου. Οι παθητικοί σαρωτές μπορούν να ελέγξουν το τρέχον λογισμικό και τις εκδόσεις ενημέρωσης κώδικα των διαδικτυακών συσκευών, παρακολουθώντας τη μη κρυπτογραφημένη κίνηση - των δεδομένων τους - εντός ενός δικτύου και αναλύοντας τις επικοινωνίες, που αφορούν τον αριθμό θύρας και τη διεύθυνση δικτύου (IP) . Αυτό δείχνει ποιες συσκευές χρησιμοποιούν λογισμικό, το οποίο περιέχει μια πιθανή πύλη

πρόσβασης για τους χάκερς και ποια εργαλεία μπορούν να διασυνδέσουν αυτή τη πληροφορία, με δημόσιες βάσεις δεδομένων, που εμπεριέχουν λίστες από αναγνωρισμένες απειλές και τρέχουσες ενημερώσεις.

Ένας διαχειριστής δικτύου μπορεί να ρυθμίσει τους παθητικούς σαρωτές, να λειτουργούν είτε συνεχόμενα είτε ανά προκαθορισμένα χρονικά διαστήματα. Ο πρωταρχικός σκοπός είναι, να γίνουν παθητικοί αποδέκτες πληροφοριών, που σχετίζονται με τη κίνηση δεδομένων του δικτύου, ώστε να απομονώσουν τις εφαρμογές, που ενδέχεται να έχουν ευπάθειες.

Επί της ουσίας, η σάρωση αυτή θυμίζει μια IDS/ IPS υπηρεσία, αλλά αντί να ψάχνει για μια άμεση απειλή, χρησιμοποιεί τα αποτελέσματα της, για να αποφασίσει εάν υπάρχει ενδεχόμενος κίνδυνος. Ακόμη, σε αντίθεση με τις υπηρεσίες IDS/ IPS, η λύση, η οποία προσφέρεται από τη παθητική σάρωση, κατά κανόνα δεν βρίσκεται ενσωματωμένη στη κίνηση - δεδομένων - του δικτύου, αλλά αντιθέτως ανιχνεύει και εντοπίζει σφάλματα σε αυτή.

2.5.3 Παρεμβατική σάρωση

Οι φορείς παρεμβατικής σάρωσης εκθέτουν τη δυνατότητα πρόσβασης, η οποία μπορεί να πραγματοποιηθεί ανά πάσα στιγμή, σε ένα αρχείο εντολών επίθεσης, που έχει σκοπό την εκμετάλλευση της ευπάθειας. Αυτοί υποθέτουν ότι μια επίθεση στο σύστημα, η οποία θα γίνει με τον ίδιο ακριβώς τρόπο, που θα το έκανε ένας πιθανός εισβολέας, είναι ο καλύτερος τρόπος για να επιτευχθούν πιο ακριβή αποτελέσματα.

Αυτά μπορούν να ενταχθούν στη κατηγορία των επιλύσεων με τη μορφή επισφαλών ελέγχων ευπάθειας ή αξιολόγησης της ευπάθειας, που εκτελείται από μια διαδικασία διεισδυτικού ελέγχου.

Χωρίς αμφιβολία, υπάρχουν και μερικά πλεονεκτήματα σε αυτή τη προσέγγιση «επιδρομής» στο σύστημα. Με τη χρήση ενός αρχείου εντολών για την αυτοματοποίηση της επίθεσης, ένα ενδεχόμενο διείσδυσης, όπου η μηχανική πρόσβαση είναι εφικτή, αποδεικνύει ότι η συσκευή ήταν ευάλωτη σε μια επίθεση και θα μπορούσε μελλοντικά να τεθεί σε κίνδυνο.

Ωστόσο, η χρήση αυτής της προσέγγισης είναι προβληματική από την άποψη ότι το αρχείο καταγραφής των τροποποιήσεων που έχουν γίνει, είναι ελλιπές και ενδεχομένως δημιουργεί περισσότερες ερωτήσεις, παρά απαντήσεις.

Για παράδειγμα, πολλά αρχεία εντολών επίθεσης (attack scripts), τα οποία είναι διαθέσιμα στο Ίντερνετ, είναι ελαττωματικά και μπορούν να οδηγήσουν σε μια λανθάνουσα αίσθηση ασφαλείας, με τη μορφή ενός ψευδώς αρνητικού ελέγχου. Αυτό σημαίνει ότι δεν λειτουργούν όπως θα ήταν επιθυμητό, ακόμη κι αν το σύστημα που βρίσκεται στο στόχαστρο, είναι πράγματι εκμεταλλεύσιμο.

Ανεπιτυχείς έλεγχοι διείσδυσης, που βασίζονται σε πιθανώς ελαττωματικά αρχεία εντολών (scripts), μπορούν να δώσουν μια λανθάνουσα αίσθηση ασφάλειας.

Τα εργαλεία αξιολόγησης ευπαθειών, τα οποία χρησιμοποιούν παρεμβατικά αρχεία αντολών (scripts), μπορούν να γίνουν επιβλαβή καθώς αφήνουν το σύστημα εκτεθειμένο σε μελλοντικές επιθέσεις, οι οποίες κανονικά δεν θα ήταν προς εκμετάλλευση, ή ακόμη χειρότερα εμποδίζουν σημαντικές εμπορικές δραστηριότητες, από το να λειτουργούν σωστά.

Ο έλεγχος για την ύπαρξη ευπάθειας, ο οποίος γίνεται με τη μορφή επιδρομής, έχει τη τάση να απενεργοποιεί λειτουργίες - του συστήματος - κατά τη διάρκεια της επίθεσης. Αυτό σημαίνει ότι κατά το διάστημα στο οποίο μια λειτουργία βρίσκεται υπό επίθεση, αυτή πιθανώς δεν είναι διαθέσιμη προς κανονική χρήση και έτσι ένα ολόκληρο δίκτυο μπορεί να παραλύσει· να προκληθεί ένα σφάλμα «μπλε οθόνης» (blue screened)· ή ακόμη χειρότερα, η επίθεση αυτή θα μπορούσε να διεισδύσει στο δίκτυο και να δημιουργήσει εκ νέου ένα πρόσφορο έδαφος για πραγματικές επιθέσεις.

Τελικά, ίσως το μεγαλύτερο επιχείρημα εναντίον αυτού του ελέγχου, που γίνεται σε μορφή επιδρομής, να είναι ότι αυτός δημιουργεί ένα αλλοιώμενο περιβάλλον αξιολόγησης κινδύνου. Με την άμεση εκτέλεση μιας επίθεσης εναντίον ενός συστήματος, το οποίο βρίσκεται υπό εξέταση, το αρχείο εντολών επίθεσης (attack script) μπορεί να οδηγήσει το σύστημα σε μια άγνωστη κατάσταση - ή να το παραλύσει τελείως - καθιστώντας το απομακρυσμένο σύστημα ανίκανο να εξεταστεί περαιτέρω και ουσιαστικά εξαλείφοντας τη πιθανότητα επίτευξης λεπτομερών αναφορών ευπάθειας, εναντίον αυτής της συσκευής, μέσω μελλοντικών ελέγχων.

Χωρίς να δημιουργηθεί παρεξήγηση, τα εργαλεία διεισδυτικού ελέγχου είναι εξαιρετικά, αλλά απαιτούν χρόνο και τεχνογνωσία ώστε να γίνει σωστή χρήση τους. Αυτά μπορεί να αφήσουν τα συστήματα, που βρίσκονται στο στόχαστρο, εκτεθειμένα σε μια ανενεργή κατάσταση και να χειριστούν μόνο ένα μικρό ποσοστό αναγνωρισμένων ευπαθειών, καθώς οφείλουν να θέσουν υπό τον έλεγχο τους πραγματικές περιπτώσεις εκμετάλλευσης του λειτουργικού συστήματος.

Για τα περισσότερα εργαλεία ελέχγου εμπορικής διείσδυσης, σχεδόν το 10% όλων των ευπαθειών, που έχουν κοινοποιηθεί τα τελευταία χρόνια, αφορούν λειτουργικά συστήματα Microsoft Windows.

Τελικά, οι έλεγχοι ύπαρξης ευπαθειών οι οποίοι είναι «επισφαλείς» μπορούν να κάνουν τα πάντα, από αποκλεισμούς λογαριασμών μέχρι να αφήσουν τους πόρους του συστήματος ευάλωτους σε επιθέσεις κατόπιν αξιολόγησης. Έτσι λοιπόν η παρεμβατική σάρωση καθίσταται λιγότερο επιθυμητή στα συστήματα παραγωγής, εξαιτίας όλων αυτών των κινδύνων που προκαλούν.

2.5.4 Μη παρεμβατική σάρωση

Οι μεθοδικοί εισβολείς συνήθως επιλέγουν να συλλέξουν όσες περισσότερες πληροφορίες γίνεται για το στόχο τους, ακολουθώντας έναν επαγωγικό συλλογισμό, ώστε να εντοπίσουν πιθανά τρωτά σημεία εντός ενός οργανισμού και των στοιχείων Τεχνολογίας Πληροφοριών (IT). Οι υποστηρικτές αυτής της «κρυφής» μεθοδολογίας, βασίζονται σε μια πληθώρα πληροφοριών, που λαμβάνουν από τα συστήματα δικτύου και εξάγουν μια ακόμη μεγαλύτερη ποσότητα πληροφοριών δημιουργώντας λογικές συνδέσεις και βγάζοντας λογικά συμπεράσματα βάση των διαθέσιμων δεδομένων. Περιλαμβάνει τα πάντα από κοινωνική μηχανική (social engineering) μέχρι απόκτηση γνώσεων για τις εφαρμογές και τους παρόχους, στους οποίους βασίζεται η επιχείρηση.

Με αυτές τις πληροφορίες, οι αναγνωρισμένες ευπάθειες και τα τρωτά σημεία - του συστήματος - γίνονται εύκολοι στόχοι για τον εισβολέα του συστήματος, ώστε να επιχειρήσει την εκμετάλλευση τους.

Σε αντίθεση με τις τεχνικές παρεμβατικής σάρωσης, οι διαχειριστές στον τομέα της Τεχνολογίας Πληροφοριών (IT) μπορούν να χρησιμοποιήσουν μη διεισδυτικούς ή μη παρεμβατικούς ελέγχους για τον εντοπισμό πιθανώς εκμεταλλεύσιμων συστημάτων, προτού αυτά γίνουν προβληματικά.

Με την υλοποίηση μη παρεμβατικών ελέγχων, οι εταιρίες μπορούν να αποφύγουν τη διαταραχή των λειτουργιών του συστήματος, ενώ πραγματοποιείται η εκτέλεση μια εκτενούς αξιολόγησης ευπάθειας.

Οι εισβολείς χρησιμοποιούν παρόμοιες τεχνικές για να διερευνήσουν, με λεπτό τρόπο, την ύπαρξη ευπαθειών χωρίς να προκαλέσουν διακοπή της λειτουργίας του συστήματος και ενδεχομένως να πυροδοτήσουν συστήματα IPS, IDS και προειδοποιητικούς αισθητήρες του τείχους προστασίας.

Οι οργανισμοί μπορούν να αξιοποιήσουν την ίδια μη παρεμβατική τεχνολογία, για να συγκεντρώσουν μεγάλες ποσότητες πληροφοριών και να ακολουθήσουν μια βέλτιστη πρακτική ανάλυσης των δεδομένων ευπάθειας, προκειμένου να προσδιορίσουν τον κίνδυνο σε ένα περιβάλλον.

Αυτή η διαδικασία συνήθως επαναλαμβάνεται κυκλικά, με σκοπό τη περαιτέρω βελτίωση και ενίσχυση των ευρυμάτων. Επίσης, η ίδια διαδικασία χρησιμοποιείται για να εξακριβωθεί ότι οι προσπάθειες αποκατάστασης ήταν επιτυχείς και η ευπάθεια δεν αποτελεί πλέον απειλή.

Λαμβάνοντας μια σαφή εικόνα του ολοκληρωμένου τρόπου δομής, μια επιχείρηση μπορεί να αναγνωρίσει καλύτερα τα τρωτά σημεία στο δίκτυο, σύμφωνα με την εταιρική πολιτική και να προνοήσει να εμποδίσει εισβολές, καθώς και τη διακοπή επιχειρηματικών δραστηριοτήτων.

Αδιαμφισβήτητα, η μη παρεμβατική σάρωση προσφέρει οφέλη, τα οποία δύνανται να προσδιοριστούν ποσοτικά, και εντυπωσιακά λιγότερους κινδύνους συγκριτικά με τη παρεμβατική σάρωση. Οι περισσότεροι οργανισμοί δεν έχουν επαρκή εξοπλισμό, για να διαχειριστούν σωστά το σενάριο ενός παρεμβατικού διεισδυτικού ελέγχου, ειδικά εκείνοι που δεν διαθέτουν αντίγραφα δικτύων. Στη περίπτωση που οι ελεγκτές δεν είναι προσεκτικοί, η πιθανή ζημιά που προκαλείται από τη παρεμβατική σάρωση, θα μπορούσε να υπερβαίνει τα πλεονεκτήματα μιας πραγματικής ανίχνευσης. Επιπλέον, ο πλήρης έλεγχος και τα ίχνη αποκατάστασης που προκύπτουν από τη μη παρεμβατική σάρωση, θα δημιουργήσουν μια αξιόπιστη και ανθεκτική υποδομή σε πολύ σύντομο χρονικό διάστημα. Τα ποσοτικώς προσδιορίσιμα και επαληθεύσιμα αποτελέσματα, συνοδευόμενα από ένα αξιόπιστο και καθοριστικό σχέδιο ενεργειών, θα αποκαταστήσουν την ευπάθεια και θα συνεισφέρουν σε οποιαδήποτε αξιολόγηση ενημέρωσης κώδικα και απαίτηση συμμόρφωσης.

Το γενικό συμπέρασμα που προκύπτει από την επιλογή ενός μη παρεμβατικού ελέγχου είναι αρκετά σαφές.

Παρακαλώ, σκεφτείτε την εξής διατύπωση: Με εξαίρεση κάποιες ακραίες περιπτώσεις, ο εντοπισμός μιας ευπάθειας και η επιδιόρθωση της είναι πιο σημαντικές ενέργειες , από την επαλήθευση της δυνατότητας εκμετάλλευσης της.

Επομένως, οι διαχειριστές και μηχανικοί μπορούν να προστατεύσουν τους καθοριστικής σημασίας πόρους τους, χωρίς να τους θέσουν στο πεδίο βολής των ενδεχομένως προβληματικών ελέγχων. Παρέχοντας στο προσωπικό υποστήριξης δικτύου έγκαιρες και έγκυρες πληροφορίες σχετικά με υπάρχουσες ευπάθειες, ο χρόνος αποκατάστασης τους μπορεί να βελτιωθεί πολύ σημαντικά και οι καταστάσεις που αφορούν την ακριβή ασφάλεια, να αξιολογηθούν χωρίς τη δημιουργία επιπρόσθετων περιττών κινδύνων ασφαλείας ή τη διακοπή των επιχειρησιακών εργασιών. Όπως συμβαίνει με όλες τις διαδικασίες ασφαλείας και τις κανονιστικές συμμορφώσεις, αυτό θα έπρεπε να επαναλαμβάνεται συχνά, ώστε οι διαχειριστές να παρακολουθούν τη τρέχουσα κατάσταση της ευπάθειας του δικτύου και το επίπεδο επικινδυνότητας, εντός του οργανισμού.

Η μη παρεμβατική σάρωση για την αξιολόγηση της ευπάθειας έχει αποτελέσει, παγκοσμίως, ένα βιομηχανικό πρότυπο, για τα προγράμματα και τους κανόνες διαχείρισης της ευπάθειας, λόγω της φιλοσοφίας και της αξιοπιστίας της ,να αναγνωρίζει και να αναφέρει όλους τους πιθανούς κινδύνους εντός ενός οργανισμού.

2.5.5 Περιορισμοί κι ελλείψεις της σάρωσης ευπάθειας

Ενώ οι σαρωτές ευπάθειας μπορούν να διευκολύνουν τις εργασίες, που αφορούν την ασφάλεια του δικτύου, αυτοί δεν μπορούν να αντικαταστήσουν τη τεχνογνωσία που διαθέτει το ειδικευμένο προσωπικό. Οι σαρωτές ενδέχεται να παρέχουν ψευδώς θετικούς ελέγχους, να υποδεικνύουν τρωτά σημεία - στο σύστημα - που δεν υπάρχουν, καθώς και ψευδώς αρνητικούς ελέγχους, κατά τους οποίους ο σαρωτής παραβλέπει έναν κίνδυνο που αφορά την ασφάλεια. Το καταρτισμένο προσωπικό πρέπει να ελέγχει προσεκτικά τα δεδομένα που παρέχουν οι σαρωτές τους, προκειμένου να ανιχνεύσει λανθασμένα αποτελέσματα.

Η αξιολόγηση ενός σαρωτή για την ύπαρξη απειλής βασίζεται αποκλειστικά στη βάση δεδομένων του, που αφορούν αναγνωρισμένους κινδύνους· ένας σαρωτής δεν μπορεί να χρησιμοποιήσει τα δεδομένα που εντοπίζει για να βγάλει συμπεράσματα που στοχεύουν στη

κατανόηση νέων και καινοτόμων μεθόδων, τις οποίες μπορεί να αξιοποιήσει ένας χάκερ ώστε να επιτεθεί στο δίκτυο.

Ένα σημαντικό μειονέκτημα που σχετίζεται με τη μη παρεμβατική σάρωση, εντοπίζεται στον τρόπο με τον οποίο αναλύονται οι πληροφορίες, μετά την εκτέλεση της σάρωσης.

Τα συστήματα τα οποία είναι επιρρεπή σε παρεμβάσεις, εμφανίζουν άμεσα αποτελέσματα μετά από μια στοχευμένη επίθεση· είτε αυτή είναι επιτυχής είτε ανεπιτυχής. Είτε μπορούν να χακαριστούν είτε όχι.

Οι μη παρεμβατικού χαρακτήρα λύσεις προϋποθέτουν τα αποτελέσματα να είναι σχετικά μεταξύ τους και η κατάσταση - του συστήματος - να υπόκειται σε παρεμβολή βάση των ληφθέντων δεδομένων. Μια εμπεριστατωμένη αναφορά, ανάλυση και διαδικασία αποκατάστασης είναι απαραίτητη για τη μετατροπή των αποτελεσμάτων σε λειτουργικά οφέλη προς την επιχείρηση.

Τα εργαλεία σάρωσης τα οποία απλά παρέχουν μια μη διαχειρίσιμη λίστα ευπαθειών, χωρίς την ύπαρξη κατάλληλων λεπτομερειών και διορθωτικών μέτρων, τείνουν να δυσκολεύουν τη διαδικασία. Για αυτό το λόγο, η λειτουργία της αξιολόγησης των ευπαθειών αποτελεί απλώς, μια από τις πολλές διαδικασίες, εντός ενός σωστού και ισχυρού προγράμματος διαχείρισης ευπάθειας. Η απλή γνώση των πληροφοριών δεν είναι αρκετή.

Εν τέλει, η σάρωση ευπάθειας μπορεί ενδεχομένως να χρησιμοποιήσει ένα αξιόλογο εύρος μεταφοράς δεδομένων (bandwidth), επιβραδύνοντας πιθανώς την απόδοση του δικτύου. Βάζοντας στο στόχαστρο κάθε δικτυακό κόμβο, με δεκάδες χιλιάδες ελέγχους και έχοντας ταυτοχρόνως πολλαπλούς σκοπούς, η κατανάλωση του εύρους μεταφοράς δεδομένων (bandwidth consumption) αυξάνεται γραμμικά.

Από τη στιγμή που εντοπίζονται οι ευπάθειες, πρέπει να τεθούν σε προτεραιότητα και να αντιμετωπιστούν· να αποκατασταθούν ή να προστατευθούν από πιθανές επιθέσεις. Από αυτή την άποψη, το πρόγραμμα διαχείρισης της ευπάθειας εντός ενός οργανισμού πρέπει να συντονιστεί με άλλες εσωτερικές διαδικασίες, συμπεριλαμβανομένης της διαχείρισης της ενημέρωσης κώδικα (patch) και των ρυθμιστικών παραμέτρων του συστήματος - οι οποίες τυπικά διαχειρίζονται από τις επιχειρησιακές ομάδες – για να χρησιμοποιήσει καταλλήλως τους πόρους του δικτύου, καθώς η ανάπτυξη και αξιολόγηση της ενημέρωσης κώδικα (patch deployment and assessment), όταν συμβαίνουν ταυτόχρονα, μπορούν ενδεχομένως να παραλύσουν το δίκτυο. Αυτό λοιπόν, καθίσταται ένα εγχείρημα σωστού σχεδιασμού και ομαδικής συνεργασίας.

2.6 Αξιολόγηση των ρυθμιστικών παραμέτρων του συστήματος

Τα τελευταία χρόνια υπήρξε ένας αυξανόμενος αριθμός νομοθετικών κανονιστικών εντολών, με τις οποίες πρέπει να συμμορφωθούν οι οργανισμοί, για να επικυρώσουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών, που βρίσκονται αποθηκευμένες στα συστήματα τους και παρέχονται μέσω εξωτερικών φορέων. Μετά την ανάγνωση διαφόρων ενημερωτικών εγγράφων (white papers), ιστοσελίδων και άλλων άρθρων τα οποία χρησιμοποιούν τους όρους «PCI, HIPAA, SOX, CIS, NIST, ISO, CIS, COBiT, FISMA και FDCC», εντός ενός γενικού και αόριστου πλαισίου, προκαλείται ίλιγγος. Όπως πολλοί ειδικοί ασφαλείας, έτσι και εμείς, αν και δεν είμαστε ελεγκτές ή δικηγόροι, βομβαρδιζόμαστε συνεχώς με όλα αυτά τα ακρωνύμια σε εβδομαδιαία βάση.

Τα ακρωνύμια που αναφέρθηκαν προηγουμένως, μπορούν να αναλυθούν πρόχειρα σε τρεις κατηγορίες, ή αρχεία εντολών, τα οποία βοηθούν τους οργανισμούς να επιτύχουν συμμόρφωση και στόχους που αφορούν την ασφάλεια: Κανονισμοί (Regulations), Ρυθμιστικά πλαίσια (Frameworks) και Πρότυπα Αναφοράς (Benchmarks). Σε μερικές περιπτώσεις, τα όρια μεταξύ των τριών κατηγοριών δεν είναι ξεκάθαρα, αλλά η κατανόηση του σκοπού τους και της σχέσης που έχουν η μια κατηγορία με την άλλη, μπορούν να σε βοηθήσουν να καταλάβεις πώς αυτές μπορούν να συνδυαστούν, ώστε να ενισχύσουν συνολικά ένα πρόγραμμα, που αφορά την ασφάλεια και τη συμμόρφωση.

2.7 Γνωστοποίηση της ευπάθειας

Η γνωστοποίηση μιας ευπάθειας είναι η πολιτική, οι διαδικασίες και η πρακτική υποβολής μιας έκθεσης των σφαλμάτων του συστήματος στο λογισμικό (software), υλισμικό (hardware) ή μικροκώδικα (firmware) του υπολογιστή. Από τη στιγμή που θα αναγνωριστούν, οι ευπάθειες είναι δυνατόν να γνωστοποιηθούν στους δημιουργούς ή στη τεχνολογία επίλυσης ή στους συμβαλλόμενους στην υποστήριξη των επιλύσεων των ευπαθειών. Αυτό περιλαμβάνει δημόσιους και ιδιωτικούς παρόχους καθώς και κοινότητες ανοιχτού κώδικα (open source communities). Τυπικά, οι πάροχοι ή οι προγραμματιστές καθυστερούν να κοινοποιήσουν τις σχετικές με την ευπάθεια λεπτομέρειες έως ότου μια ενημέρωση ασφάλειας λογισμικού ή μια στρατηγική μετριασμού μιας ευπάθειας να είναι διαθέσιμη. Όταν μια τέτοια πληροφορία δημοσιοποιείται προτού μια πιθανή διόρθωση του προβλήματος να είναι διαθέσιμη, η ευπάθεια συνήθως χαρακτηρίζεται ως ευπάθεια μηδενικής ημέρας (zero-day vulnerability).

Η γνωστοποίηση της ευπάθειας και οι πολιτικές που τη διέπουν, μπορούν να αποτελέσουν ένα συνεχές πρόβλημα προς επίλυση μεταξύ των παρόχων, των μελετητών και των τελικών χρηστών. Οι πάροχοι προτιμούν να περιμένουν μέχρι μια ενημέρωση να είναι διαθέσιμη και ύστερα να προβούν στη κοινοποίηση της ευπάθειας, ακόμη κι αν υπάρξει μια σχετικά μεγάλη καθυστέρηση. Πολλοί μελετητές προτιμούν να δίνουν στους παρόχους ένα χρονοδιάγραμμα 30, 60 ή 90 ημερών ώστε να αναπτύξουν και να εκδώσουν μια ενημέρωση κώδικα (patch), προτού κοινοποιήσουν λεπτομέρειες σχετικά με την ευπάθεια.

Παρ' όλο που αυτό αποτελεί υψηλότερο κίνδυνο, το να ξέρεις ότι μπορεί να κινδυνεύεις από μια απειλή με κάποιο συγκεκριμένο τρόπο, θεωρητικά είναι καλύτερο από το να υποθέτεις ότι ένα σύστημα είναι ασφαλές. Οι τελικοί χρήστες προτιμούν η όλη διαδικασία να γίνεται όσο το δυνατόν πιο σύντομα. Δηλαδή η αναγνώριση, η ενημέρωση και η γνωστοποίηση (ευπαθειών και σφαλμάτων) να προκύπτουν σε σύντομο χρονικό διάστημα, έτσι ώστε η διάρκεια έκθεσης στο πρόβλημα να ελαττωθεί και η ενημέρωση κώδικα (patch) να εφαρμοσθεί εγκαίρως.

Εκτός από τις προτιμήσεις των βασικών ομάδων χρηστών, υπάρχουν πολλαπλοί τύποι γνωστοποίησης ευπαθειών. Μια αξιόπιστη γνωστοποίηση ακολουθεί αυτή την απλή μορφή ροής:

Πίνακας 4. Ροή γνωστοποίησης ευπαθειών

Αναγνώριση ευπάθειας	Εμπιστευτική γνωστοποίηση	Εμπιστευτική έρευνα	Κοινοποίηση
Ερευνητές, ειδικοί για την ασφάλεια ή γνωστοποίηση μηδενικής ημέρας (zero-day)	Ειδοποίηση από πάροχο ή αξιόπιστο φορέα	60- 120 ή παραπάνω ημερών	Ανακοίνωση του παρόχου, έκδοση ενημέρωσης και προειδοποίηση στην Εθνική Βάση Δεδομένων Ευπάθειας (NVD)*

*Η Εθνική Βάση Δεδομένων Ευπάθειας (NVD) είναι το αμερικανικό δημόσιο αποθετήριο δεδομένων διαχείρισης ευπάθειας, που βασίζεται σε πρότυπα, τα οποία αποδίδονται μέσω του Πρωτοκόλλου Αυτοματοποίησης Περιεχομένου Ασφαλείας (SCAP). Αυτά τα δεδομένα επιτρέπουν την αυτοματοποίηση της διαδικασίας διαχείρισης της ευπάθειας, τη μέτρηση ασφάλειας και τη συμμόρφωση. Το NVD περιλαμβάνει βάσεις δεδομένων από αναφορές λιστών ελέγχου ασφαλείας, ελαττώματα λογισμικού που σχετίζονται με την ασφάλεια, εσφαλμένες διαμορφώσεις, ονόματα προϊόντων και μετρήσεις του αντικτύπου. Είναι σημαντικό να σημειωθεί ότι δεν συμμετέχουν όλοι οι πάροχοι στις κοινοποιήσεις επισήμανσης και ταξινόμησης του NVD και CVE.

Από τότε που εμφανίστηκε αυτό το σύγχρονο πρόβλημα ύπαρξης ευπαθειών και της αντίστοιχης εκμετάλλευσης τους, η αξιοσημείωτη διαδικασία γνωστοποίησης της ευπάθειας έχει συμπεριλάβει ερευνητές και παρόχους, οι οποίοι συνεργάζονται ώστε να αντιληφθούν την απειλή, τις τεχνικές εκμετάλλευσης και να εξετάσουν στρατηγικές αποκατάστασης του προβλήματος. Άλλωστε, μια ανεπαρκής επιδιόρθωση μπορεί να οδηγήσει σε άλλες ευπάθειες και απλώς να χειροτερέψει τη κατάσταση. Αυτό έχει συμβεί στο παρελθόν, δηλαδή στρατηγικές αποκατάστασης του σφάλματος, να προκαλούν μέχρι και βλάβες στη λειτουργικότητα του συστήματος.

Βάσει αυτής της συνεργασίας/ σύμπραξης ή της απουσίας της, προκύπτουν διάφορες επιλογές αποκατάστασης του σφάλματος:

- Αυτο-Αποκάλυψη (Self-Disclosure)- Όταν οι προμηθευτές επιλύσεων για σφάλματα κοινοποιούν αναφορές ευπαθειών. Αυτό συμβαίνει συνήθως όταν μια διόρθωση ευπάθειας είναι διαθέσιμη έναντι της απλής έκθεσης ενός αμετάβλητου κινδύνου.
- Γνωστοποιήσεις Τρίτων (Third-Party Disclosure)- Όταν η κοινοποίηση της ευπάθειας δεν πραγματοποιείται από τον πάροχο ή τον αρμόδιο κατασκευαστή της τεχνολογίας που χρησιμοποιείται. Οι γνωστοποιήσεις τρίτων, συνήθως εκτελούνται από τους ερευνητές στον τομέα της ασφάλειας, αλλά μπορούν επίσης και να προέλθουν από πηγές διαρροής στοιχείων, όπως το Wikileaks, το οποίο αξιοποιεί πληροφορίες, που έχουν αποκτηθεί παράνομα. Η γνωστοποίηση αυτή μπορεί να γίνει είτε με αξιοπιστία προς διοικητικά σώματα, όπως το NVD ή το CERT είτε όχι. Όταν δεν πραγματοποιείται με αξιοπιστία, συνήθως δημιουργείται αδίκως η εντύπωση ότι ο πάροχος καθυστερεί να βρεί λύση για την αποκατάσταση του σφάλματος.
- Γνωστοποιήσεις Προμηθευτή (Vendor Disclosure)- Όταν ο ερευνητής στον τομέα της ασφάλειας παρέχει μια έκθεση σφαλμάτων απευθείας στους παρόχους ή στα αρμόδια τμήματα και δεν επιδιώκει κανένα άλλο είδος κοινοποίησης τους.
- Πλήρης Αποκάλυψη (Full Disclosure)- Προκύπτει όταν μια ολοκληρωμένη κοινοποίηση της ευπάθειας ανακοινώνεται και μπορεί να πραγματοποιηθεί οποιαδήποτε στιγμή καθ'όλη τη διάρκεια της γνωστοποίησης της ίδιας της ευπάθειας.

Σύμφωνα με την Εθνική Διοίκηση Τηλεπικοινωνιών και Πληροφοριών (NTIA), οι οργανισμοί και οι ερευνητές θα πρέπει να αναπτύξουν και να διατηρήσουν μια Πολιτική Αποκάλυψης Ευπάθειας (VDP). Αυτή η πολιτική (VDP) είναι μια αξιόπιστη μέθοδος για ανθρώπους, οργανισμούς και υπηρεσίες για τη διαχείριση της διαδικασίας γνωστοποίησης της ευπάθειας.

Μια VDP πολιτική θα πρέπει να περιλαμβάνει τα εξής:

- Δήλωση Ασφαλείας (Security Statement)- Μια δέσμευση, συχνά με τη μορφή σύμβασης παροχής υπηρεσιών, για την έγκαιρη αντιμετώπιση των κινδύνων ασφαλείας και την αξιόπιστη εκτέλεση της γνωστοποίησης όλων των αναγνωρισμένων απειλών.
- Πεδίο Ασφαλείας (Security Scope)- Μια εμπιστευτική δήλωση (private statement) για το ποιες τεχνολογίες εφαρμόζονται στη Δήλωση Ασφαλείας. Τυπικά, τα εσωτερικά συστήματα δεν αποτελούν εύκολο στόχο για τους ερευνητές, στον τομέα της Ασφάλειας Τρίτων (Third-Party Security), εκτός κι αν έχουν ρητή σύμβαση για διεισδυτική εξέταση ή άλλες αξιολογήσεις ασφαλείας.
- Νομικά Ζητήματα (Legal Issues)- Εάν μια έρευνα διεξάγεται παράνομα εντός ενός οργανισμού ή χωρίς ενδεδειγμένη συγκατάθεση, ποιες είναι οι επιπτώσεις, βάση νόμου, για τον ερευνητή; Αυτό μπορεί επίσης να ισχύει για κώδικα που έχει συνταχθεί, όταν ο ερευνητής επιχειρεί να αποσυναρμολογήσει (reverse-engineer) ένα προϊόν προκειμένου να αποκαλύψει τα σφάλματα που αφορούν την ασφάλεια. Οι πάροχοι έχουν προβεί σε απειλές για άσκηση αγωγής στους ειδικούς του τομέα της ασφάλειας εάν αυτό συμβεί και τυπικά αποτελεί επικίνδυνο εγχείρημα κατά τη διεξαγωγή μιας έρευνας.
- Επικοινωνία- Μια Πολιτική Αποκάλυψης Ευπάθειας (VDP) θα πρέπει να παρέχει ένα μέσο για ασφαλείς επικοινωνίες χωρίς κινδύνους και επιπτώσεις μεταξύ των ερευνητών στον τομέα της ασφάλειας και ενός οργανισμού. Συνήθως, αυτό το μέσο επικοινωνίας διατίθεται

δημόσια και διέπεται από κανόνες, που ρυθμίζουν τη παρατήρηση και γνωστοποίηση σφαλμάτων. Σε αυτούς τους κανόνες μπορεί να περιλαμβάνονται τα εξής:

ο Καμία κοινοποίηση σφάλματος έως ότου μια ενημέρωση του κώδικα (patch) να είναι διαθέσιμη.

ο Ένα χρονοδιάγραμμα διαβουλεύσεων και πότε μπορεί να πραγματοποιηθεί αίτημα παράτασης.

ο Μια πιθανή ανταμοιβή για τη τήρηση των οδηγιών και όρων πληρωμής.

ο Το δικαίωμα του ορισμού της ευπάθειας βάση του υπάρχοντος σφάλματος ή κάποιου, βασιζόμενου σε έρευνα, κριτηρίου.

ο Κλιμάκωση της Διαδικασίας Εύρεσης Σφαλμάτων (Escalation of Findings)- Μια εσωτερική διαδικασία θα πρέπει να είναι σε θέση να επεξεργάζεται τις ευπάθειες, που έχουν αναγνωριστεί και να θέτει σε προτεραιότητα την αποκατάσταση τους με σωστό τρόπο.

Δυστυχώς, δεν συμφωνούν όλοι οι ερευνητές με αυτές τις διαδικασίες, τις οδηγίες της Πολιτικής Αποκάλυψης Ευπάθειας (VDP) ή τα χρονοδιαγράμματα κοινοποίησης των σφαλμάτων. Οι διαφωνίες, η αμέλεια, η απόρριψη των παρόχων και πολλά άλλα ανθρώπινα γνωρίσματα οδηγούν σε ακραίες παρεκκλίσεις από αυτές τις πολιτικές και διαδικασίες παγκοσμίως.

Η γνωστοποίηση μιας ευπάθειας μπορεί να αντιμετωπιστεί υπεύθυνα, αλλά δυστυχώς, οι πάροχοι δεν μπορούν πάντα να βασίζονται στις ειλικρινείς προθέσεις των ερευνητών στον τομέα της ασφάλειας (ή στη κυβέρνηση).

2.8 Κανονισμοί

Οι κανονισμοί αποτελούν νομικούς περιορισμούς που έχουν δημιουργηθεί, ρυθμιστεί και κοινοποιηθεί από κρατικούς διοικητικούς φορείς. Οι κανονισμοί τυπικά δεν παρέχουν λεπτομέρειες για την εκτέλεση, ρύθμιση και διαχείριση των συστημάτων Τεχνολογίας Πληροφοριών/ Πληροφορικής (IT), αλλά αυτοί υποδεικνύουν με σαφή τρόπο τους σκοπούς που πρέπει να εκλπηρώσει ένα πρόγραμμα ασφάλειας και συμμόρφωσης.

Στα παραδείγματα αυτών των κανονισμών, τα οποία θα συζητηθούν σε επόμενο κεφάλαιο, συμπεριλαμβάνονται τα Sarbanes-Oxley, HIPAA, GLBA, Basel II και GDPR.

Ο ορισμός της έννοιας των κανονισμών μπορεί να γίνει πολύπλοκος με την ύπαρξη προτύπων όπως το PCI DSS. Πολλοί κρατικοί και ιδιωτικοί φορείς πρέπει, όπως προβλέπεται, να είναι σύμφωνοι με το ειδικό Πρότυπο Payment Card Industry (PCI) Data Security Standard (DSS). Αυτό το πρότυπο περιγράφει ένα σύνολο από διεθνώς αναγνωρισμένες απαιτήσεις ασφαλείας, για τη προστασία των δεδομένων των κατόχων πιστωτικών καρτών. Για τη συμμόρφωση με το PCI DSS, οι οργανισμοί πρέπει επίσης να προχωρήσουν σε ενέργειες γνωστές ως απαιτήσεις επικύρωσης, στις οποίες εμπεριέχεται μια απαίτηση για τρημιναία σάρωση ευπάθειας από έναν πάροχο σάρωσης εγκεκριμένο από το PCI. Αυτό το πρότυπο καθιστά δυσδιάκριτα τα όρια μεταξύ κανονισμού και εξουσιοδοτημένων εντολών, και δεν είναι θεσμοθετημένο από κάποιο φορέα δημόσιας διοίκησης αλλά από την ίδια τη βιομηχανία πιστωτικών καρτών. Σε αυτό το σημείο συνήθως είναι που μπερδεύεται ο κόσμος.

2.9 Ρυθμιστικά πλαίσια

Τα ρυθμιστικά πλαίσια παρέχουν μια καθορισμένη δομή στήριξης, στο πλαίσιο της οποίας μπορεί ένα εγχείρημα να οργανωθεί και αναπτυχθεί. Τα ρυθμιστικά πλαίσια είναι σχεδιασμένα, ώστε να προσφέρουν ένα πρόγραμμα ολοκληρωμένης ασφάλειας, για έναν οργανισμό. Αυτά τα πλαίσια μπορούν να εφαρμοσθούν για να στηρίξουν τους σκοπούς των πολλαπλών κανονισμών και συχνά συστήνονται για τη παγίωση των βέλτιστων πρακτικών ή προτύπων αναφοράς, και μπορούν να χρησιμοποιηθούν σε περιπτώσεις τεχνικής προστασίας.

Παραδείγματα ρυθμιστικών πλαισίων αποτελούν μεταξύ άλλων τα ITIL, CobiT και COSO, NIST 800-53, ISO 17799 / 27002. Είναι σημαντικό να σημειωθεί ότι ρυθμιστικά πλαίσια όπως τα NIST και ISO συχνά αναφέρονται λανθασμένα ως κανονισμοί εξαιτίας της συμπερίληψης τους σε συμβάσεις ή άλλα πρότυπα. Όταν συμβαίνει αυτό, τα ρυθμιστικά πλαίσια γίνονται κανονισμοί, αλλά δεν ισχύει το ίδιο όταν λειτουργούν ως ανεξάρτητα εργαλεία. Μια σύμβαση ή κάποιο άλλο μέσο καθιστά δυνατή την επιβολή ενεργειών, πέραν από τις βέλτιστες πρακτικές και τις απαιτήσεις ασφαλείας που έχουν ορίσει. Ακόμη πιο περίπλοκο;

2.10 Πρότυπα αναφοράς

Τα πρότυπα αναφοράς συχνά χρησιμοποιούνται για τη μέτρηση και παρακολούθηση κοινών δεδομένων, που σχετίζονται με την ασφάλεια και τις υποδομές της Τεχνολογίας Πληροφοριών (IT), μια διαδικασία που είναι γνωστή ως « γενικοί έλεγχοι υπολογιστών».

Τα πρότυπα αναφοράς περιγράφουν ένα σύνολο κριτηρίων (μερικά από τα οποία μπορεί να έχουν υποχρεωτικό χαρακτήρα), προαιρετικές κατευθυντήριες γραμμές και βέλτιστες πρακτικές.

Ενώ τα ρυθμιστικά πλαίσια (frameworks) παρουσιάζουν ασαφείς σκοπούς, τα πρότυπα αναφοράς (benchmarks) παρέχουν ένα κανονιστικό πλαίσιο οδηγιών για τους ελέγχους και τις ρυθμίσεις που θα πρέπει να πραγματοποιηθούν, για να καταστήσουν το περιβάλλον πληροφορικής (IT) ανθεκτικό και να προστατεύσουν τους πόρους του συστήματος πληροφορικής (IT assets), ενάντια σε συγκεκριμένους κινδύνους.

Σε αυτό το σημείο είναι που το τοπίο αρχίζει να ξεκαθαρίζει. Ανάμεσα στα παραδείγματα προτύπων βρίσκονται οι βέλτιστες πρακτικές παρόχων και πελατών, που προκύπτουν από τις καταστάσεις ελέγχου των CIS, SANS και DISA. Αυτές αποτελούν ρυθμίσεις, που είναι πραγματικά χρήσιμες, προκειμένου τα συστήματα να γίνουν πιο ανθεκτικά, όσον αφορά στις ρυθμίσεις διαμόρφωσης του συστήματος.

Ο πίνακας 2 περιγράφει τα κυριότερα πρότυπα αναφοράς από αναγνωρισμένους αρμόδιους φορείς και γνωστούς παρόχους.

Πίνακας 5. Πρότυπα αναφοράς από αναγνωρισμένους αρμόδιους φορείς και γνωστούς παρόχους.

Organization Name		*Public Website URL*	*Coverage*	
Cis	Center for internet security	https://www.cisecurity.org/cis-benchmarks/	operating systems (multiple), server software, Cloud providers, mobile Devices, network Devices, Desktop software and multi-function Devices	Configuration assessment
	Description	a global community of cyber security experts collaborating on benchmark hardening guidelines for safeguarding the most prevalent technology implementations. it is important to note that many vendors like red hat and oracle, and security organizations like sans, reference Cis for their own best practices.		
nist	national institute of standards and technology	https://www.nist.gov		

(*continued*)

Organization Name		*Public Website URL*	*Coverage*
fDCC (obsolete)	federal Desktop Core Configuration	https://www.nist.gov/programs-projects/ federal-desktop-core-configuration-fdcc	Desktop operating systems (microsoft Windows Xp and Vista)
	Description	the federal Desktop Core Configuration (fDCC) is an omB-mandated security configuration. the fDCC currently exists for microsoft Windows Vista and Xp operating system software.	
usgCB	united states government Configuration Baseline	https://usgcb.nist.gov	operating systems (microsoftWindows Xp, 7, and Vista and red hat 5 Desktop), and microsoft Browsers, firewalls, and Virtual machines
	Description	the purpose of the usgCB initiative is to create security configuration baselines (benchmarks) for information technology products widely deployed across the federal agencies. the standard is a federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security.	

(*continued*)

Configuration assessment

Organization Name		*Public Website URL*	*Coverage*
stigs (Disa)	security technical implementation guides	https://iase.disa.mil/stigs/Pages/index. aspx	operating systems (multiple), server software, Cloud (private and public) providers, mobile Devices, network (infrastructure) solutions, Desktop software and multi-function Devices, and applications
	Description	the stigs are the configuration (benchmark) standards for united states Department of Defense (DoD) information assurance (ia) devices and systems. the stigs contain technical guidance to "lock down" information systems and software that might otherwise be vulnerable to a malicious computer attack due to poor configurations.	

(*continued*)

Configuration assessment

Organization	*Name*	*Public Website URL*	*Coverage*
ms	microsoft	https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx	operating systems (microsoft Desktops and servers) and microsoft applications
	Description	microsoft provides ready-to-deploy policies and configuration packs that are tested and fully supported. Baselines are based on microsoft security guide recommendations and industry best practices, to manage configuration drift, address compliance requirements, and reduce security threats.	
Vmware	Vmware	https://www.vmware.com/security/hardening-guides.html	VmWare hypervisors (Vsphere, nsX, and vrealize)

Configuration assessment

image source:
www.nist.gov
www.Nist.gov/programs-projects/federal-desktop-core-configurationj-fdee
www.usgcb.nist.gov
www.cisecurity.org/cis-benchmarks
technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx
www.vmware.com/security/hardining-guides.html

Θα πρέπει να σημειωθεί ότι δεν είναι όλες οι καταστάσεις ελέγχων, που έχουν παγιωθεί, και οι δοκιμές προτύπων αναφοράς ισοδύναμες. Υπάρχουν διαφόρων ειδών περιπτώσεις εφαρμογής, για κάθε ένα από αυτά και η μορφή αυτών μπορεί να κυμαίνεται από μια δημόσια γνωστοποίηση, που αφορά μη ευαίσθητες πληροφορίες, μέχρι μια καθοριστικής σημασίας αποστολή, που αφορά εξαιρετικά ευαίσθητα δεδομένα.

Αναλόγως με το περιβάλλον σου, θα χρειαστεί να κάνεις τη κατάλληλη επιλογή και να βεβαιωθείς, ότι τα μέτρα ασφαλείας των συστημάτων του κεντρικού υπολογιστή, δεν παραβιάζουν την ακεραιότητα της εφαρμογής ή της αποστολής.

Κατά γενικό κανόνα, πάντα να ενδυναμώνεις τους πόρους ενός συστήματος όσο πιο πολύ γίνεται, αλλά να εξακολουθείς να παρέχεις χρηστικότητα, υπηρεσίες διαχείρισης και αποκατάσταση καταστροφών, κατά τη διεκπεραίωση περιπτώσεων χρήσης, λειτουργώντας σύμφωνα με τα εσωτερικά πρωτόκολλα.

ΚΕΦΑΛΑΙΟ 3. ΕΠΙΣΚΟΠΗΣΗ ΕΡΓΑΛΕΙΩΝ

3.1 Εργαλεία αξιολόγησης των ρυθμιστικών παραμέτρων του συστήματος

Δεδομένου ότι είσαι μια μεγάλη αεροπορική εταιρία, μια επιχείρηση ή μια τοπική κυβέρνηση με χιλιάδες συστήματα, τα οποία θα πρέπει να είναι πανομοιότυπα, όσον αφορά τις ρυθμιστές παραμέτρους τους, αυτά θα μπορούσαν να είναι κιόσκια ελέγχου εισητηρίων μιας αεροπορικής γραμμής, ένα τηλεφωνικό κέντρο για τη διαχείριση της γραμμής υποστήριξης, ή μια κυβερνητική ή τοπικής αυτοδιοίκησης υπηρεσία, με ένα εικονικό πρότυπο για σταθερούς και φορητούς υπολογιστές.

Πώς ελέγχεις (ή θα ήλεγχες) τη διαμόρφωση των παραμέτρων αυτών των στοιχείων - του συστήματος - σε καθημερινή βάση;

Ενώ σαν ιδέα μπορεί να ακούγεται πολύ απλό, ο μη αυτόματος έλεγχος όλων αυτών των συστημάτων είναι απολύτως ανέφικτος και η χρήση τεχνολογίας, που βασίζεται σε κάποιον διαμεσολαβητή (agent-based), ή εφαρμογών σάρωσης, που έχουν σκοπό τη συμμόρφωση βάσει ειδικών ρυθμιστικών παραμέτρων, αποτελούσε τη μοναδική επιλογή, για τον έλεγχο των μεμονωμένων ρυθμίσεων του συστήματος, σε καθημερινή βάση. Αυτές οι υπηρεσίες θα ήταν, όπως συμπεραίνεται, πολύ ακριβές και η διαδικασία εγκατάστασης, ρύθμισης και διατήρησης τους, πιθανότατα θα απαιτούσε πολύ κόπο. Ένα πρόβλημα το οποίο θα ήταν αρκετά απλό κατά την αξιολόγηση των ρυθμιστικών παραμέτρων του συστήματος θα μπορούσε να αποτελεί ένα περίπλοκο θέμα κατά την εφαρμογή τους.

Μερικοί πάροχοι όπως η Microsoft έχουν εκδόσει τις δικές τους λύσεις αποκατάστασης προβλημάτων, για το δικό τους λογισμικό. Η Microsoft κυκλοφόρησε το εργαλείο Security Compliance Manager (SCM) το 2010 το οποίο επιτρέπει την εισαγωγή Προτύπων Αναφοράς που αφορούν Ρυθμιστικές Παραμέτρους Ασφαλείας (Security Configuration Benchmarks), από τον ίδιο τον Οδηγό Βέλτιστων Πρακτικών (Best Practice Guidelines) της Microsoft (ή από άλλες επιλύσεις τρίτων) και την αξιολόγηση τους χρησιμοποιώντας ένα διαδραστικό περιβάλλον χρήστη.

Το περιβάλλον του εργαλείου SCM δίνει τη δυνατότητα επιλογής ενός λειτουργικού συστήματος ή εφαρμογής και τη δυνατότητα αξιολόγησης των μεμονωμένων προτεινόμενων ρυθμίσεων διαμόρφωσης ασφαλείας, από το ρόλο του συστήματος.

Ένας χρήστης μπορεί να μεταβεί σε οποιαδήποτε από τις ρυθμίσεις και να προβεί σε αλλαγές των ρυθμίσεων, προκειμένου να τηρούν την εταιρική τους πολιτική. Αν και αυτή η διαδικασία μπορεί να ακούγεται κάπως κουραστική, ο χρήστης χρειάζεται να το κάνει μόνο μια φορά για κάθε πρότυπο διαμόρφωσης του συστήματος που πρέπει να ακολουθήσουν.

Ως επί το πλείστον, οι εταιρικές πολιτικές συνάδουν με αυτές τις ρυθμίσεις και είναι ανάλογες με τα πρότυπα που εκδόθηκαν από τα CIS, DISA (με βάση τους οδηγούς STIGs) και USGCB (NIST). Κανονικά το μόνο που έχει ανάγκη ο οργανισμός σου είναι μικρές τροποποιήσεις και εάν δεν είσαι σίγουρος για το ποια ρύθμιση διαμόρφωσης να επιλέξεις, η Microsoft έχει δώσει σαφείς κατευθυντήριες γραμμές που αφορούν τη τιμή (value) της κάθε ρύθμισης, προκειμένου να παρθεί μια συνειδητή απόφαση σε ό,τι αφορά τη προεπιλεγμένη τιμή (value) ρύθμισης που ενδείκνυται.

Μόλις ολοκληρωθούν όλες οι τροποποιήσεις, απέχεις μόνο μερικά κλικς από το να χρησιμοποιήσεις έναν ανεξάρτητο (agentless) σαρωτή δικτύου ή έναν τοπικό, συμβατό με το πρότυπο SCAP, διαμεσολαβητή και να εκτελέσεις μια αξιολόγηση σχετικά με τη συμβατότητα των ρυθμιστικών παραμέτρων.

Αυτό είναι κάτι που δεν ήταν εφικτό μέχρι και τα τελευταία χρόνια που γίνεται η χρήση ανοιχτού προτύπου. Η Microsoft έχει προσθέσει στο SCM τη δυνατότητα εξαγωγής όλων των ρυθμίσεων σε ένα πιστοποιημένο SCAP OVAL CAB αρχείο. Μετά την αποθήκευση του αρχείου, μπορείς να εισάγεις το πρότυπο αναφοράς (benchmark) σε μια αυτοματοποιημένη αξιολόγηση διαμόρφωσης των ρυθμίσεων με σκοπό την επαλήθευση των πόρων του συστήματος.

3.1.1 SCAP

Το Security Content Automation Protocol (SCAP, το οποίο προφέρεται S-cap) είναι μια σειρά από ανοιχτά πρότυπα, τα οποία όταν συσχετιστούν, φέρουν ως αποτέλεσμα μια αυτοματοποιημένη διαχείριση και μέτρηση ευπάθειας, καθώς και μια αξιολόγηση, βάσει πολιτικής, των πόρων του δικτύου (network assets).

Η πρώτη έκδοση αυτής της λίστας προτύπων (suite specification) επικεντρώνεται στη τυποποίηση της κοινοποίησης των δεδομένων, που σχετίζονται με το τελικό σημείο και στη παροχή μιας ενιαίας προσέγγισης, για τη διατήρηση της ασφάλειας των εταιρικών συστημάτων.

Παρέχει ένα μέσο αναγνώρισης, έκφρασης και μέτρησης των δεδομένων ασφαλείας με τους ίδιους συνήθεις τρόπους, που τα προϊόντα διαφόρων παρόχων μπορούν να καταναλώνουν ή παράγουν περιεχόμενο, από τις λίστες ελέγχου SCAP, για το συσχετισμό των πληροφοριών ασφαλείας. Κάθε επιμέρους πρότυπο, εντός του τεχνικού προτύπου SCAP (SCAP specification), διατηρείται ξεχωριστά και αφορά εκδόσεις συγκεκριμένων στοιχείων.

Για παράδειγμα, η έκδοση 1.0 του SCAP συμπεριλαμβάνει τα ακόλουθα πρότυπα και εκδόσεις: XCCDF 1.1.4, OVAL 5.3. CCE 5, CPE 2.2, CVE (χωρίς έκδοση), and CVSS 2. Καθώς αυτό το τεχνικό πρότυπο (specification) έχει εξελιχθεί, οι πρόσφατες εκδόσεις του περιλαμβάνουν νέα στοιχεία και τροποποιήσεις σε κάθε επιμέρους εκδοχή του.

Παρακάτω διατίθεται μια περίληψη κάθε μιας από τις τροποποιήσεις του τεχνικού προτύπου (specification) από την αρχή της έκδοσης του:

- Η έκδοση 1.1 αυτού του τεχνικού προτύπου (specification) διευρύνεται, έτσι ώστε να συμπεριλάβει το Open Checklist Interactive Language (OCIL, προφέρεται O-sil), και κάνει αλλαγές ώστε να ενσωματωθεί στην έκδοση 5.8 του τεχνικού προτύπου OVAL. Το OCIL αποτελεί ένα νέο συστατικό στοιχείο που ορίζει ένα πλαίσιο για την έκφραση ενός συνόλου ερωτήσεων τις οποίες πρέπει να απαντήσει ο χρήστης και αντίστοιχων διαδικασιών για την ερμηνεία των απαντήσεων σε αυτά τα ερωτηματολόγια. Το OCIL αναπτύχθηκε για να ενισχύσει τις λίστες ελέγχου ασφαλείας στον τομέα της Τεχνολογίας Πληροφοριών (IT security checklists) και όχι για να περιοριστεί στην ασφάλεια Τεχνολογίας Πληροφοριών και μόνο. Αυτό επιτρέπει την εκτέλεση μιας αξιολόγησης και τη καταχώρηση ζωτικής σημασίας πληροφοριών, που δεν μπορούν να εξεταστούν ηλεκτρονικά (δηλαδή, υπάρχει κάποιο κλειδί ασφαλείας κατά την είσοδο στο διακομιστή;).

  Αυτή η πληροφορία αποθηκεύεται μαζί με τα αποτελέσματα για την απόκτηση μιας πιο ξεκάθαρης εικόνας σχετικά με την ασφάλεια των στοιχείων του συστήματος.

- Η έκδοση 1.2 ενισχύει το τεχνικό πρότυπο με νέες και αναβαθμισμένες δυνατότητες, συμπεριλαμβανομένων των Common Configuration Scoring System (CCSS), Asset Identification και Asset Reporting Format (ARF), επεκτείνει το μοντέλο ροής δεδομένων, προσφέρει ασφαλείς επιλογές, το σήμα περιεχομένου SCAP καθώς και αποτελέσματα χρησιμοποιώντας το μοντέλο Trust Model for Security Automation Data (TMSAD). Επίσης αυτό παρέχει ενημερώσεις,για την υποστήριξη νέων εκδόσεων των ήδη συμπεριλαμβανομένων τεχνικών προτύπων, μεταξύ των οποίων είναι τα Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE) και Extensible Configuration Checklist Description Format (XCCDF).

- Η έκδοση 1.3 αποτελεί μια σταδιακή βελτίωση του τεχνικού προτύπου και τώρα περιλαμβάνει επιπρόσθετα στοιχεία που αφορούν τα Asset Identification (AI) 1.1 και Software Identification (SWID) Tags 2015. Το πρότυπο AI παρέχει τις απαραίτητες προϋποθέσεις για τον προσδιορισμό των πόρων του συστήματος, βάσει αναγνωρισμένων κωδικών αναφοράς

(identifiers) ή πληροφοριών σχετικά με τους πόρους του συστήματος. Το τεχνικό πρότυπο SWID, όπως ορίζεται από το πρότυπο ISO/IEC 19770-2:2015, αποτελεί ένα σημαντικό βήμα στήριξης του λογισμικού απογραφής και παρέχει στους οργανισμούς, έναν τρόπο να εντοπίζουν με διαφάνεια, το λογισμικό που έχει εγκατασταθεί στους πόρους του συστήματος τους. Αυτή, εκτός από μια σταδιακή έκδοση αποτελεί και ένα σύνολο αλλαγών, για άλλα εγκατεστημένα στοιχεία.

Οι δύο πιο συνηθισμένες περιπτώσεις εφαρμογής του πρωτοκόλλου SCAP (μέχρι τώρα), αφορούν την αξιολόγηση ευπάθειας και τη συμβατότητα των ρυθμίσεων. Με τη χρήση ορισμών OVAL, μια συμβατική (πιστοποιημένη) λύση SCAP μπορεί να κάνει λήψη ενός αρχείου XML με αναγνωριστικά ευπάθειας ή ελέγχους διαμόρφωσης των προτύπων αναφοράς (configuration benchmark checks) και να εκτελέσει μια τοπική η δικτυακή αξιολόγηση, για συστήματα τα οποία είναι μη συμμορφούμενα. Το προϊόν θα αποθηκεύσει τα αποτελέσματα της σάρωσης στη γλώσσα OVAL και σε μορφή αρχείου XCCDF και στο τελικό αρχείο XML κάνει αναφορές στα CVE, CCE, CPE, και CVSS χρησιμοποιώντας μια κοινή ορολογία για την περιγραφή του ευρήματος.

Ουσιαστικά, αυτή η διαδικασία αποσαφηνίζει τους τύπους ελέγχου και τους ορισμούς, χρησιμοποιώντας τη γλώσσα OVAL, καθώς και το πώς θα έπρεπε να γίνει η εφαρμογή αυτών των ελέγχων και η υποβολή σχετικών αναφορών, σε μορφη XCCDF και επίσης εξηγεί ότι το περιεχόμενο των αποτελεσμάτων περιέχει τις ίδιες παραμέτρους, ανεξαρτήτως προϊόντος. Αυτό καθιστά τη διαλειτουργικότητα, μεταξύ των πιστοποιημένων προϊόντων SCAP, ικανή να συμβάλει στη δημιουργία περιεχομένου OVAL, για την υποβολή εκθέσεων σχετικά με τα τελικά αποτελέσματα και την αποθήκευση σε μια βάση δεδομένων.

3.2 Μέτρηση κινδύνου

Η ασφάλεια στον τομέα της Τεχνολογίας Πληροφοριών / Πληροφορικής (IT) είναι σαφώς το βασικότερο ζήτημα, που απασχολεί τις επιχειρήσεις τη σήμερον ημέρα. Οι λέξεις «απειλή» και «επίθεση» χρησιμοποιούνται ευρέως με τέτοιο τρόπο, που είναι σαν να υποδηλώνουν κάποιο μονολιθικό κακό, το οποίο παραμονεύει την υποδομή των οργανισμών. Στην πραγματικότητα, υπάρχουν πολλά είδη απειλής και πολλές μορφές επίθεσης, που μπορούν να δημιουργηθούν και εντός και εκτός του οργανισμού.

Οι ευπάθειες στο περιβάλλον της Πληροφορικής (IT) μπορούν να προξενήσουν καταστροφές στις επιχειρηματικές δραστηριότητες. Αυτά τα τρωτά σημεία είναι συνήθη και μπορούν να αξιοποιηθούν με κακόβουλο τρόπο, από πολλές και διάφορες εξωτερικές και εσωτερικές απειλές, από άτομα με κακόβουλες προθέσεις και «χακτιβιστές», μέχρι εγκληματικά συνδικάτα διαδικτυακής πειρατείας και εθνοκράτη.

Η ανάγκη για προληπτική αντιμετώπιση των ευπαθειών εντείνεται λόγω των απαιτήσεων των υπηρεσιών προς επιχειρήσεις συνεχούς σύνδεσης, του υπολογιστικού νέφους (cloud-based computing) και της κανονιστικής συμμόρφωσης. Είναι λοιπόν απολύτως απαραίτητος ο σχεδιασμός και η εφαρμογή μιας ολοκληρωμένης στρατηγικής διαχείρισης της ασφάλειας με σκοπό τη διασφάλιση της συνεχούς λειτουργίας των επιχειρησιακών δραστηριοτήτων και την ελαχιστοποίηση του συνολικού κινδύνου που απειλεί τον οργανισμό.

Επίσης, η διαχείριση ευπαθειών αποτελεί μια πολύ σημαντική μεταβλητή στον υπολογισμό του συνολικού κινδύνου.

ΚΙΝΔΥΝΟΣ = ΑΝΤΙΚΤΥΠΟΣ × ΠΙΘΑΝΟΤΗΤΑ (RISK = IMPACT × PROBABILITY)

όπου:

- Κίνδυνος: Ο βαθμός στον οποίο ένας οργανισμός απειλείται από ένα πιθανό συμβάν.
- Αντίκτυπος: Το αναμενόμενο μέγεθος της ζημιάς που προκύπτει από τις συνέπειες ενός συμβάντος.

- Πιθανότητα: Το ενδεχόμενο ύπαρξης ενός απειλητικού συμβάντος.

Η διαδικασία της αξιολόγησης ενός κινδύνου χρησιμοποιείται για τη κατάταξη των κινδύνων σε σειρά προτεραιότητας ανάλογα με τη πιθανότητα ενός συμβάντος και τον αντίκτυπο του. Ωστόσο, για τη σαφή κατανόηση των όρων «Αντίκτυπος» και «Πιθανότητα», θα πρέπει να ψάξουμε πιο βαθιά και σε αυτό το σημείο είναι που μπορεί να βοηθήσει η διαχείριση ευπάθειας ως διαδικασία.

Ο ίδιος ο αντίκτυπος ενός συμβάντος μπορεί να παρουσιαστεί με ποικίλες μορφές, συμπεριλαμβανομένων των:

- Απώλεια ιδιόκτητων πληροφοριών.
- Απώλεια διαθεσιμότητας συστήματος.
- Απώλεια ή αλλοίωση δεδομένων ή εφαρμογών.
- Πτώση της παραγωγικότητας.
- Κανονιστική παράβαση.
- Φθορά των σχέσεων με τους πελάτες / της εικόνας της εμπορικής επωνυμίας (του brand).

Ο συνολικός αντίκτυπος ενός συμβάντος είναι μια συνάρτηση της κρισιμότητας των πόρων του συστήματος (assets) και του μεταβαλλόμενου τοπίου απειλών. Η κρισιμότητα των πόρων του συστήματος (asset) καθορίζεται από τις εφαρμογές ή από άλλες υπηρεσίες, οι οποίες εξαρτώνται από την ύπαρξη και τη σωστή λειτουργία αυτών.

Η απειλή είναι ο βαθμός ενδεχόμενης επικινδυνότητας, που αντιμετωπίζει ένας πόρος του συστήματος από πηγές, οι οποίες πιθανώς τον θεωρούν πολύτιμο στόχο, βάσει κριτηρίων που καθορίζονται από τον χρήστη και/ ή τον ρόλο του συστήματος. Η ίδια η απειλή είναι αποτέλεσμα πολλαπλών παραγόντων, μεταξύ των οποίων περιλαμβάνονται η πηγή της απειλής, το ενδεχόμενο μιας επίθεσης και η πιθανότητα επιτυχίας. Κατά την εκτίμηση της τρέχουσας απειλής, οι οργανισμοί μπορούν να χρησιμοποιήσουν έναν συνδυασμό ποιοτικών και ποσοτικών δεδομένων.

Ένας αξιόπιστος δείκτης απειλών εξετάζει τις πρακτικές καθώς και τα στατιστικά στοιχεία που αφορούν τη πιθανότητα μιας επίθεσης. Σε αυτό το σημείο οι ομάδες που ασχολούνται με τον τομέα της ασφάλειας, θα πρέπει να εξετάσουν πώς οι πόροι του συστήματος (assets) εντός του εταιρικού περιβάλλοντος εκτίθενται σε απειλές και τι είδους απειλές θέτουν σε κίνδυνο την ακεραιότητα, που απαιτείται για την εκτέλεση λειτουργιών της επιχείρησης και τη προστασία δεδομένων. Οι ομάδες ασφαλείας θα πρέπει ακόμη να εξετάσουν, το πόσο δεκτικό είναι ένα σύστημα σε επικείμενη επίθεση.

Αυτή η έκθεση στον κίνδυνο μπορεί να βασιστεί στον αριθμό των ανοιχτών θυρών, των δεδομένων που διανέμονται, των υπηρεσιών και των χρηστών που περιέχει ένας κεντρικός υπολογιστής, στην έλλειψη προστασίας, δηλαδή ενός τείχους προστασίας ή μιας λύσης κατά των ιών και στη παρουσία οποιωνδήποτε παράνομων ή αχρείαστων εφαρμογών, που έχουν εγκατασταθεί.

Όσον αφορά στην εξίσωση της επικινδυνότητας, αυτή αποτελεί μια συνάρτηση των ευπαθειών και των δραστηριοτήτων περιορισμού του κινδύνου. Ο όρος ευπάθειες εκφράζει τη ποσότητα και τη σοβαρότητα των τρωτών σημείων, που εντοπίζονται στο περιβάλλον πληροφορικής (IT) του οργανισμού. Οι εκτιμήσεις που γίνονται, βασίζονται σε παράγοντες όπως η έλλειψη κατάλληλης προστασίας των ενημερώσεων κώδικα (patch maintenance) του κεντρικού υπολογιστή ή τα ζητήματα συμμόρφωσης, που σχετίζονται με τη τρέχουσα εταιρική πολιτική ασφαλείας και τις βέλτιστες πρακτικές. Οι περιορισμοί που υφίστανται, προκύπτουν από τους ελέγχους οι οποίοι έχουν γίνει για την απαλειφή ή μείωση των κινδύνων, που σχετίζονται με την ύπαρξη ευπαθειών.

Υπάρχουν διάφορα Πλαίσια Διαχείρισης Κινδύνου, που θα συζητηθούν σε επόμενο κεφάλαιο, τα οποία εισηγούνται αυτούς τους τρόπους υπολογισμού του κινδύνου και τους ενσωματώνουν σε ένα ολοκληρωμένο πρόγραμμα διαχείρισης κινδύνου ενός οργανισμού.

Χάρη στη τεχνική μετάφραση της ορολογίας του τομέα των επιχειρήσεων, οι οργανισμοί μπορούν να έχουν στη διάθεση τους μια άμεση μέθοδο κατανόησης της κατάστασης ασφαλείας των πόρων του συστήματος (asset), των μη επεξεργασμένων τεχνικών δεδομένων και του αντίκτυπου στην επιχείρηση. Προς το παρόν, μια απλή αναλογία μπορεί να συμβάλλει σε μια καλύτερη κατανόηση αυτής της προσέγγισης, διαχείρισης του κινδύνου.

Φαντάσου ότι κάθε πόρος του συστήματος (asset) στο περιβάλλον σου είναι ένα κάστρο.

Η κατασκευή, τα αμυντικά μέσα, η τοποθεσία και ο θησαυρός του αποτελούν όλα παράγοντες για μια επικείμενη επίθεση. Τα τείχη του κάστρου προστατεύουν το εσωτερικό ιερό όπου βρίσκεται ένας θησαυρός από χρυσάφι (δεδομένα, επιχειρηματικές δραστηριότητες κτλ.). Τα στρατεύματα (χάκερς, worms κτλ.) προσπαθούν να παραβιάσουν τα τείχη του κάστρου και να διεισδύσουν στο εσωτερικό ιερό, για να πάρουν τον χρυσό ή να διαταράξουν τις συνθήκες κανονικής λειτουργίας του κάστρου.

Σε αυτή τη περίπτωση, οι φορείς ασφαλείας θα ορίζονταν ως εξής:

Η ύπαρξη ευπαθειών υποδηλώνει το πόσο εύκολο είναι να παραβιαστεί το εσωτερικό ιερό και κατά συνέπεια πόσο απλή θα ήταν η απόκτηση πρόσβασης στον χρυσό.

- Οι Επιθέσεις αντιστοιχούν σε βέλη, βόμβες και απόπειρες παραβίασης των τειχών και του εσωτερικού ιερού.
- Οι Εκθέσεις (Exposures) - στον κίνδυνο - αποκαλύπτουν το βαθμό στον οποίο τα τείχη και τα ανοίγματα του κάστρου μπορούν να δεχθούν επίθεση και πόσο κακή είναι η προστασία της περιφέρειας του κάστρου.
- Οι Απειλές είναι τα στρατεύματα που παραμονεύουν στους λόφους που περιβάλλουν το κάστρο και τα οποία προετοιμάζονται για επίθεση.

Όντας στη κορυφή, αυτοί οι τρεις φορείς έχουν καθοριστική σημασία για το ίδιο το κάστρο· με άλλα λόγια, αποδεικνύουν το πόσο πολύτιμο είναι το κάστρο και το εσωτερικό ιερό του για την αυτοκρατορία (τον οργανισμό σου). Τα δεδομένα που περιέχονται στο εσωτερικό, μπορούν να υπολογισθούν σύμφωνα με το Infonomics. Αυτό αποτελεί τη νομισματική αξία των δεδομένων τα οποία λειτουργούν ευεργετικά για τον οργανισμό, ανεξαρτήτως του αν κατά τη χρήση τους εντός του οργανισμού έχουν κλαπεί, πωληθεί ή έχουν ανταλλαχθεί.

Όπως φαίνεται, οι ευπάθειες αποτελούν ένα θεμελιώδες στοιχείο κατά την εξέταση και εκτίμηση του συνολικού κινδύνου που σχετίζεται με τα «κοσμήματα του στέματος». Τώρα κάνε ότι πυροβολάς με το χέρι σου στον αέρα. Μήπως αυτό θυμίζει το πως είναι να στρέφεσαι εναντίον των ευπαθειών σου; Εάν ναι, δεν είσαι μόνος. Έχεις κάνει μια σάρωση και βρήκες χιλιάδες ευπάθειες. Και τώρα, τι; Εσύ πρέπει να εντοπίσεις γρήγορα τις πιο κρίσιμες απειλές και να πραγματοποιήσεις ενημερώσεις στα πιο ευπαθή συστήματα –αλλά πώς;

Δεν είναι όλες οι ευπάθειες ίσης δυναμικής. Και το να ανακαλύψεις ποιες από αυτές θέτουν το μεγαλύτερο κίνδυνο απαιτεί μια πολύ πιο εξονυχιστική εξέταση της κατάστασης από αυτή που προσφέρουν τα αποτελέσματα του CVSS. Το να γνωρίζεις εάν οι ευπάθειες υφίστανται εκμετάλλευση, ποιες από αυτές υπόκεινται σε εκμετάλλευση από εξωτερικούς παράγοντες ή από κάποιον με προνομιακά δικαιώματα, εάν κάποιο ενεργό κακόβουλο λογισμικό τις εκμεταλλεύεται και αν μπορεί αυτό να διορθωθεί μέσω μιας ενημέρωσης κώδικα (patch) ή αλλαγής στις ρυθμιστικές παραμέτρους του συστήματος, αποτελούν όλα ερωτήματα που πρέπει να απαντηθούν πριν τον προσδιορισμό του κινδύνου.

Ας ρίξουμε μια ματιά στο πώς μπορούμε να αξιολογήσουμε και να συγκρίνουμε τις ευπάθειες μεταξύ συστημάτων και εταιριών για να διασφαλίσουμε ότι οι κίνδυνοι έχουν τεθεί σε σειρά προτεραιότητας και οι εργασίες αποκατάστασης έχουν ανατεθεί καταλλήλως.

Η βάση αυτού έχει ως αφετηρία τη χρήση βιομηχανικών προτύπων για τη περιγραφή των ευπαθειών.

3.2.1 CVE

Common Vulnerabilities and Exposures (CVE) είναι ένα πρόγραμμα που κυκλοφόρησε το 1999 από τον MITRE, έναν μη κερδοσκοπικό οργανισμό, με χρηματοδότηση της ομοσπονδιακής κυβέρνησης και με σκοπό την αναγνώριση και τη καταγραφή των ευπαθειών που εντοπίζονται στο λογισμικό (σε συστήματα εφαρμογών και λειτουργικά συστήματα) και στον μικροκώδικα (firmware). Οι οργανισμοί μπορούν να αξιοποιήσουν τη πηγή της ευπάθειας, προκειμένου να βελτιώσουν την ασφάλεια τους. Η λέξη «common» αποτελεί το πιο σημαντικό μέρος αυτού του προτύπου. Στην ουσία σου επιτρέπει να γνωρίζεις ότι κάθε εργαλείο, άρθρο και επίλυση εξετάζει την ίδια υποκείμενη ευπάθεια.

Οι οργανισμοί αναγνωρίζουν τα πληροφοριακά συστήματα που είναι προσβεβλημένα από γνωστοποιημένα σφάλματα λογισμικού καθώς και από πιθανές ευπάθειες, που προκύπτουν από αυτά τα σφάλματα και υποβάλλουν αυτές τις πληροφορίες στο ειδικευμένο οργανωτικό προσωπικό, το οποίο φέρει ευθύνες για την ασφάλεια αυτών των πληροφοριών. Ενημερώσεις λογισμικού, που είναι σχετικές με την ασφάλεια, περιλαμβάνουν για παράδειγμα, ενημερώσεις κώδικα (patches), πακέτα υπηρεσιών (service packs), άμεσες επιδιορθώσεις (hotfixes) και αναγνωριστικά προστασίας από ιούς (anti- virus signatures).

Επιπλέον, οι οργανισμοί αντιμετωπίζουν ελαττώματα που έχουν εντοπιστεί κατά τη διάρκεια αξιολογήσεων ασφαλείας, συνεχών παρακολουθήσεων, δραστηριοτήτων για την αντιμετώπιση συμβάντων και κατά τη διαχείριση σφαλμάτων του συστήματος. Άμεσα συνδεδεμένο με τη βάση δεδομένων του CVE είναι το πλαίσιο Common Weakness Enumeration (CWE), το οποίο παρέχει ένα ενιαίο πλαίσιο αναφοράς των διαφόρων ειδών ευπάθειας που εντοπίζονται σε ένα λογισμικό. Οι οργανισμοί επωφελούνται από διαθέσιμους πόρους, όπως οι βάσεις δεδομένων των Common Weakness Enumeration (CWE) ή Common Vulnerabilities and Exposures (CVE), με σκοπό την αποκατάσταση σφαλμάτων, που εντοπίζονται σε οργανωτικά πληροφοριακά συστήματα.

3.2.2 CVSS

Το πιο συνηθισμένο σύστημα αξιολόγησης ευπαθειών, το οποίο χρησιμοποιείται από παρόχους καθώς και στο πλαίσιο κανονιστικών πρωτοβουλιών, είναι το CVSS (το Common Vulnerability Scoring System). Αυτό παρέχει ένα ανοιχτό πρότυπο αξιολόγησης, που δεν εξαρτάται από κάποιον συγκεκριμένο πάροχο, το οποίο εκθέτει τη σοβαρότητα της ευπάθειας και προσφέρει έναν οδηγό για τον καθορισμό προτεραιότητας των προσπαθειών αποκατάστασης. Η Βασική Ομάδα Δεικτών Μέτρησης (Base) , που επιτρέπει την αξιολόγηση μιας ευπάθειας, βασίζεται στη δυναμική των επιμέρους στοιχείων που τη συγκροτούν, τα οποία στοιχεία είναι τα Access Vector, Access Complexity, Authentication Method κτλ.

Οι κύριοι δείκτες, οι οποίοι βρίσκονται εκτός της βάσης αξιολόγησης (base scoring) του CVSS, είναι οι Χρονικοί Δείκτες Μέτρησης (Temporal Metrics). Αυτοί αντιστοιχούν σε τρεις, χρονικά εξαρτώμενους, περιγραφικούς δείκτες ευπάθειας. Αυτοί είναι:

1. Ο δείκτης μέτρησης «Exploitability», παρέχει ένα μέτρο αξιολόγησης του πόσο περίπλοκη είναι η διαδικασία εκμετάλλευσης της ευπάθειας ενός συγκεκριμένου συστήματος, που βρίσκεται στο στόχαστρο. Αυτός ειδικεύεται στις ευπάθειες.

2. Ο δείκτης «Remediation Level» παρέχει ένα μέσο μέτρησης της αξίας της διαθέσιμης επίλυσης. Αυτή μπορεί να είναι οτιδήποτε, από μια επίσημη επιδιόρθωση ασφαλείας, μέχρι το να μην υπάρχει διαθέσιμη λύση ή να μην είναι δυνατόν να εφαρμοσθεί.

3. Ο δείκτης «Report Confidence» αξιολογεί την εμπιστοσύνη προς την υπάρχουσα ευπάθεια, καθώς και την αξιοπιστία της ίδιας της ύπαρξης της.

Να σημειωθεί ότι οι τιμές της χρονικής μέτρησης (temporal scores) μπορούν μόνο να μειώσουν το συνολικό αποτέλεσμα του CVSS, όχι να το αυξήσουν.

Ο δείκτης μέτρησης «Exploitability» είναι ο πιο σημαντικός σε αυτή την αξιολόγηση. Αυτός προσφέρει μια καθοδήγηση χρησιμοποιώντας τέσσερα διαφορετικά κριτήρια μέτρησης:

1. «Unproven»: Δεν υπάρχει διαθέσιμος κώδικας εκμετάλλευσης ευπάθειας (exploit code). (χρονικά εξαρτώμενο)

2. «Proof of Concept»: Ο κώδικας εκμετάλλευσης (exploit code) αυτής της μετρικής τιμής είναι διαθέσιμος τη στιγμή της αξιολόγησης.

3. «Functional»: Ο κώδικας εκμετάλλεσυης (exploit code) αυτής της μετρικής τιμής είναι διαθέσιμος.

4. «High»: Η εκμετάλλευση της ευπάθειας μπορεί να γίνει από έναν λειτουργικό κινητό αυτόνομο κώδικα ή δεν προβλέπεται η αυτόματη πραγματοποίηση εκμετάλλευσης και μπορεί να γίνει μη αυτόματη ενεργοποίηση της.

Αυτός ο δείκτης μέτρησης επιτρέπει τη βαθμολόγηση μιας ευπάθειας, κάνοντας χρήση του συστήματος αξιολόγησης CVSS, με βάση την δυνατότητα εκμετάλλευσης της. Γιατί όμως έχει σημασία αυτό;

Ο βαθμός επικινδυνότητας μια ευπάθειας δεν είναι αρκετός για να τεθούν σε προτεραιότητα οι προσπάθειες αποκατάστασης στο περιβάλλον σου. Η βασική μέτρηση ευπάθειας (base calculation) δεν λαμβάνει υπόψη εάν κάποιος (ή κάτι) μπορεί εύκολα να εκμεταλλευτεί την ευπάθεια, το πόσο δύσκολη θα είναι η μείωση του κινδύνου, καθώς και την ύπαρξη εμπιστοσύνης στην αξιοπιστία μιας ευπάθειας που έχει καταγραφεί, ιδίως όταν σχετίζεται με πόρους, που περιέχονται στην υποδομή του συστήματος.

Γι’αυτό το λόγο, οι Δείκτες Χρονικής Μέτρησης (Temporal Metrics) του συστήματος CVSS είναι τόσο σημαντικοί και ο Δείκτης Μέτρησης «Exploitability» είναι ζωτικής σημασίας, όσον αφορά τις προσπάθειες καθορισμού προτεραιότητας. Αυτός λαμβάνει υπόψη, όχι μόνο την σοβαρότητα της ευπάθειας, αλλά και το κατά πόσο υφίσταται απειλή εκμετάλλευσης στο περιβάλλον σου, σε μια οποιαδήποτε χρονική στιγμή.

3.2.3 STIG

Τα Security Technical Implementation Guides (αναφέρονται σχεδόν πάντα με το ακρωνύμιο τους – STIGs και προφέρονται όπως ο χαρακτήρας από το «Top Gear») αποτελούν πρότυπα διαμόρφωσης του συστήματος στο πλαίσιο της διαδικασίας Διασφάλισης Πληροφοριών (IA) του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών (DOD) και των πιστοποιημένων από τη διαδικασία Διασφάλισης Πληροφοριών (IA) πόρων (assets) και συστημάτων. Τα STIGs περιέχουν τεχνικές οδηγίες για τη λήψη μέτρων ασφαλείας των πληροφοριακών συστημάτων και του λογισμικού, τα οποία αλλιώς θα ήταν ευάλωτα σε κακόβουλες επιθέσεις κατά του υπολογιστή, λόγω των προεπιλεγμένων ή κοινών ρυθμίσεων τους. Αυτά αποτελούν Πρότυπα Αναφοράς (Benchmarks).

Τα STIGs υφίστανται ως έγγραφα τεκμηρίωσης (documentation), αλλά υπάρχουν και για επιλεγμένες πλατφόρμες και εφαρμογές, αρχεία εντολών και αρχεία INF με σκοπό να καταστήσουν την εφαρμογή σταθερή ανάλογα με τις περιπτώσεις χρήσης και το σκοπό της. Για παράδειγμα, υπάρχουν διαφορετικά STIGs διαθέσιμα για έναν Διακομιστή Windows (Windows Server) όταν χρησιμοποιείται ως διακομιστής ιστού και όταν χρησιμοποιείται ως ελεγκτής τομέα και άλλα αναλόγως με το εάν ο πόρος του συστήματος βρίσκεται σε δημόσιο ή απόρρητο δίκτυο.

Κάθε σύσταση που γίνεται εντός ενός συγκεκριμένου STIG, για τη δημιουργία ανθεκτικότητας, συνοδεύεται από μια Κατηγορία που αφορά τη σοβαρότητα του κινδύνου (risk severity Category). Αυτή επιτρέπει την αξιολόγηση του κινδύνου, τον οποίο αντιμετωπίζει ένας πόρος του συστήματος, με βάση τον αριθμό των συμβατών ρυθμίσεων, έναντι των μη συμβατών.

Οι παραβιάσεις της Κατηγορίας I είναι μη αποδεκτές και χρειάζεται άμεση μείωση του κινδύνου που αντιμετωπίζει η συσκευή, ειδάλλως δεν θα έπρεπε να επιτρέπεται η λειτουργία της εντός ενός δικτύου του Υπουργείου Άμυνας (DoD).

Οι πάροχοι διαχείρισης ευπάθειας έχουν μετατρέψει αυτές τις ρυθμίσεις σε ρυθμίσεις διαμόρφωσης προτύπων αναφοράς (configuration benchmark settings) και επιτρέπουν στα πρότυπα STIGs να προβούν σε έναν αυτοματοποιημένο έλεγχο της καταγραφής και αξιολόγησης της συμμόρφωσης. Είναι σημαντικό να σημειωθεί, ότι ούτε όλα τα πρότυπα STIGs μπορούν να αυτοματοποιηθούν, ούτε όλες οι πλατφόρμες επιτρέπουν ηλεκτρονικούς ελέγχους. Αυτό απαιτεί προσωπικό, το οποίο θα ελέγχει χειροκίνητα τις απαιτήσεις του προτύπου STIG και το οποίο επίσης μπορεί να χρειαστεί να συμπληρώσει χειροκίνητα φόρμες πιστοποίησης χρησιμοποιώντας ένα εργαλείο συμμόρφωσης OCIL ως μέρος του προτύπου SCAP.

Στον πιο κάτω πίνακα, απεικονίζεται το παράδειγμα ενός αποτελέσματος, σχετικού με λύσεις που αφορούν τη διαχείριση ευπάθειας, το οποίο προκύπτει από μια, συμβατή με το πρότυπο STIG, αξιολόγηση που πραγματοποιείται σε έναν διακομιστή Windows (Windows server) για την έκδοση πιστοποίησης.

Πίνακας 6. Δείγμα αποτελέσματος SCAP από μια αξιολόγηση προτύπου αναφοράς STIG.

Scan Summary

Computer Name:	Serenity.Cricklewood.local
Target Platform:	Windows Server 2012 R2 Datacenter
Benchmark Title:	Windows Server 2012 / 2012 R2 Domain Controller Security Technical Implementation Guide
Benchmark Platform:	cpe:/o:microsoft:windows_server_2012:-
Profile:	I - Mission Critical Classified
Scan Time:	04/04/2018 09:26:25

	Items	
Description	**Passed**	**Failed**
1 Unsupported Service Packs	1	0
2 Display Shutdown Button	1	0
3 NTFS Requirement	1	0
4 Legal Notice Display	0	1
5 Caching of logon credentials	0	1
6 Anonymous shares are not restricted	0	1
7 Bad Logon Attempts	0	1
8 Bad Logon Counter Reset	0	1
9 Lockout Duration	0	1
10 User Right - Act as part of OS	1	0
11 Maximum Password Age	1	0

Αυτά τα δεδομένα μπορούν, συνεπώς, να θέσουν σε προτεραιότητα τους κινδύνους των πόρων του συστήματος, αναφορικά με τις ρυθμιστικές παραμέτρους του και χρησιμοποιούνται σε συνδυασμό με τα αποτελέσματα της αξιολόγησης ευπάθειας, η οποία πραγματοποιείται προκειμένου να ορίσει τη συνολική κατάσταση ασφάλειας του λειτουργικού συστήματος, της πλατφόρμας και της εφαρμογής.

3.2.4 OVAL

Ένα δύσκολο ζήτημα που προκύπτει, αναφορικά με τις αξιολογήσεις ευπάθειας, είναι ότι κάθε πάροχος διαθέτει ένα διαφορετικό αναγνωριστικό (έλεγχο) για την ίδια ευπάθεια και CVE. Αυτό αποφέρει μερικούς ψευδώς θετικούς, καθώς και μερικούς ψευδώς αρνητικούς ελέγχους, ενώ στη πραγματικότητα θα περίμενε κανείς τη διαδικασία ανίχνευσης, να είναι ίδια ανεξαρτήτως παρόχου.

Ως επί το πλείστον, όλα λειτουργούν σωστά, αλλά κατά διαστήματα εμφανίζονται και αποκλίσεις· σε αυτό το σημείο είναι που έρχεται στο προσκήνιο το πρότυπο OVAL (Open Vulnerability and Assessment Language).

Το OVAL εισήχθη αρχικά από τον οργανισμό MITRE και πλέον διαχειρίζεται από το CIS (Center for Internet Security/ Κέντρο Διαδικτυακής Ασφάλειας).

Αποτελεί θεμελιώδες μέρος του SCAP (Security Content Automation Protocol) και είναι ένα ανοιχτό, ελεύθερο προς χρήση πρότυπο για τη καταγραφή αναγνωριστικών ύπαρξης ευπάθειας και τα μέτρα ασφαλείας που αφορούν τη διαμόρφωση του συστήματος.

Βάσει σχεδιασμού, όλα τα εργαλεία μπορούν να χρησιμοποιήσουν ελέγχους OVAL για την ανίχνευση μιας ευπάθειας με βάση τα ίδια κριτήρια και αναμένοντας τα ίδια αποτελέσματα. Ουσιαστικά αυτό εξισορροπεί τον ανταγωνισμό που υπάρχει μεταξύ όλων των παρόχων, όσον αφορά στην εύρεση ευπαθειών, αλλά δυστυχώς η δράση του σταματάει εκεί, εξαιτίας της έλλειψης ευρείας υποστήριξης, εκ μέρους του κλάδου, προς όλες τις τεχνολογίες.

Οι πάροχοι διαχείρισης ευπάθειας εξακολουθούν να διαφοροποιούν τις λύσεις που προσφέρουν, αξιοποιώντας αποκλειστικούς ελέγχους και μηχανές σάρωσης και κάνοντας χρήση του προτύπου OVAL προκειμένου να ενισχύσουν τις αξιολογήσεις τους, όταν από πρωτοβουλίες κανονιστικής συμμόρφωσης απαιτείται η υποβολή των εισροών και των εκροών των δεδομένων σε μορφή SCAP.

Ενώ το πρότυπο OVAL παρέχει ένα τυποποιημένο σύστημα μέτρησης των ευπαθειών, η απουσία ιδιοτήτων, πλατφόρμας υποστήριξης και τεχνικών ελέγχων, το καθιστούν εύχρηστο κυρίως από πελάτες-χρήστες του Υπουργείου Άμυνας (DoD) και από κυβερνητικούς φορείς για την απόκτηση πιστοποιητικού.

3.2.5 IAVA

Το Information Assurance Vulnerability Alert (IAVA) είναι η ανακοίνωση ύπαρξης ευπαθειών εντός ενός λογισμικού εφαρμογής για υπολογιστές ή η ειδοποίηση ύπαρξης τους εντός του λειτουργικού συστήματος με τη μορφή προειδοποιήσεων, ενημερωτικών δελτίων και τεχνικών συμβουλών, αναγνωρισμένων από το Υπουργείο Άμυνας (DoD) και την Υπηρεσία Πληροφοριακών Συστημάτων Άμυνας (DISA).

Αυτές οι επιλεγμένες ευπάθειες αποτελούν σημείο αναφοράς και χρήζουν επιτακτικής αποκατάστασης, σε όλα τα δίκτυα και και τους πόρους των συστημάτων του Υπουργείου Άμυνας (DoD).

Το τμήμα Cyber Command των Ηνωμένων Πολιτειών (United States Cyber Command) αναλύει κάθε ευπάθεια που έχει κοινοποιηθεί και αποφασίζει εάν είναι αναγκαία ή ωφέλιμη για το Υπουργείο Άμυνας (DoD) η έκδοση μιας ειδοποίησης IAVA.

Στόχος είναι η προστασία στρατιωτικών πόρων κάνοντας χρήση κοινών επικοινωνιών και τιμών αξιολόγησης, καθώς και η κατανόηση του κάθε κινδύνου από τους εμπορικούς ομόλογους μέσω του CVE, CVSS και άλλων δημοσιευμένων προτύπων.

Ακριβώς όπως και το CVSS, έτσι και το IAVA περιέχει έναν δείκτη επικινδυνότητας, ο οποίος έχει καθοριστεί από το Υπουργείο Άμυνας (DoD). Αναφορικά με τους στρατιωτικούς πόρους, αυτοί οι δείκτες επικινδυνότητας μπορεί να διαφέρουν από τους εμπορικούς ομόλογους τους και έχουν στόχο τη συνειδητοποίηση του κινδύνου ή τον καθορισμό προτεραιοτήτων.

Ως τελική παρατήρηση, τα IAVAs, κατά κανόνα, δεν χρησιμοποιούνται εκτός του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών και των εξωτερικών συνεργατών του.

Εάν ο οργανισμός σου έχει ως απαίτηση τη σύνταξη αναφορών, με γνώμονα το IAVA, ανά σύμβαση εργολαβίας ή υπεργολαβίας, θα χρειαστεί ρητή παραχώρηση άδειας χρήσης πρόσθετης τεχνολογίας από τον πάροχο διαχείρισης ευπάθειας με σκοπό την ενεργοποίηση αυτών των λειτουργιών και των κατάλληλων προτύπων αναφοράς (reporting modules).

ΚΕΦΑΛΑΙΟ 4. ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΦΑΡΜΟΓΩΝ

ΥΙΟΘΕΤΗΣΗ ΜΙΑΣ ΛΥΣΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΕΥΠΑΘΕΙΑΣ (ΠΑΡΑΔΕΙΓΜΑ)

Για να αντιμετωπίσουμε την τρέχουσα τάση της ασφάλειας των πληροφοριών και την εξελιγμένη απειλή στον κυβερνοχώρο, χρειαζόμαστε την πιο αποτελεσματική και καταλληλότερη λύση διαχείρισης ευπάθειας για την υποδομή μας καθώς και τις εφαρμογές μας. διαχείριση ευπάθειας ασχολείται με ανθρώπους, διαδικασίες και τεχνολογία. πρέπει να επιλέξουμε κάθε ένα από αυτά προσεκτικά. Η τεχνολογία είναι ο πυλώνας ο οποίος είναι τεράστιος και δεν μπορούμε να επιλέξουμε πολλαπλές ίδιες λύσεις. Πρέπει να είμαστε πολύ προσεκτικοί εάν αποφασίσουμε να επιλέξουμε πανομοιότυπές λύσεις. Παρακάτω περιγράφονται οι παράμετροι κατά την επιλογή μιας λύσης διαχείρισης ευπάθειας:

1.Δυνατότητα διαχείρισης αποθεμάτων περιουσιακών στοιχείων:

Η λύση παρέχει μια βάση δεδομένων απογραφής περιουσιακών στοιχείων. Εάν είναι εφικτή η επέκταση του σχήματος της βάσης δεδομένων για την υποστήριξη πρόσθετων πεδίων, όπως η ταξινόμηση περιουσιακών στοιχείων. Εάν όχι, μπορεί η τεχνολογία να ενσωματωθεί με άλλες λύσεις/αποθήκες διαχείρισης περιουσιακών στοιχείων;

2. Δυνατότητα κάλυψης για πολλαπλά περιβάλλοντα:

Δυνατότητα χειρισμού πολλαπλών λειτουργικών συστημάτων.Τι είναι το εύρος και κάλυψη πλατφόρμας της τεχνολογίας; Πολλές τεχνολογίες μπορούν να εκτελέσουν λειτουργίες έναντι των Windows. Επίσης θα χρειαστούν τεχνολογίες που μπορούν να λειτουργούν σε ετερογενές περιβάλλον και να υποστηρίζουν ποικιλία πλατφορμών, εφαρμογών και συσκευών υποδομής.

3. Υποστήριξη για προσέγγιση cloud και mobile:

Πρέπει να σκεφτεί κανείς και μια διορατική προσέγγιση. Για παράδειγμα ένα εργαλείο διαχείρισης ευπάθειας που σαρώνει υπηρεσίες cloud, όπως λογισμικό ως υπηρεσία ή υποδομή ως υπηρεσία;

4. Επεκτασιμότητα:

Ποια είναι η κλίμακα του εύρους που πρέπει να καλύπτεται στη διαχείριση ευπάθειας και εάν το εργαλείο είναι αρκετά ικανό να χειριστεί το εύρους αυτό. Σαφήνεια σχετικά με την ικανότητα του εργαλείου να χειρίζεται πολλαπλές συσκευές υποδομής, εφαρμογές κ.λπ.

5. Ευκολία λειτουργίας:

Ένα εργαλείο που είναι ακατάλληλο στην πλοήγηση ή παρουσιάζει μπερδεμένες πληροφορίες στον πίνακα εργαλείων δεν θα χρησιμοποιηθεί, τουλάχιστον όχι στο μέγιστο των δυνατοτήτων του. Ένα εργαλείο διαχείρισης ευπάθειας που απαιτεί τακτική συντήρηση γίνεται επίσης πρόβλημα για το προσωπικό, που συχνά είναι ήδη υπερβολικά επιβαρυμένο.

6. Αντιμετώπιση ψευδών θετικών και κρισιμότητας. (false positives & severity)

Τα περισσότερα από τα αυτοματοποιημένα εργαλεία επισημαίνουν ψευδώς θετικά στοιχεία καθώς κάποια ευπάθεια μπορεί να μην σχετίζεται με τον οργανισμό ή χρειάζεται επεξεργασία σχετικά με την σοβαρότητα των ‘’τρωτών’’ σημείων. Πρέπει το εργαλείο να διαθέτει την ικανότητα αντιμετώπισης ψευδών θετικών στοιχείων και προσαρμογής σοβαρότητας.

7. Δυνατότητα ενσωμάτωσης:

Πρέπει να υπάρχει η δυνατότητα της ενσωμάτωσης του εργαλείου σε υπάρχοντα εργαλεία διαχείρισης ενημερώσεων κώδικα, διαχείριση διαμόρφωσης, ανίχνευση εισβολής και/ή εργαλεία και υπηρεσίες παρακολούθησης

8. Δυνατότητα του εργαλείου να λειτουργεί μη παρεμβατικά:

Κατά τη σάρωση της υποδομής παραγωγής, είναι απαραίτητο να υπάρχει παθητική ή μη παρεμβατική προσέγγιση σάρωσης. Το εργαλείο πρέπει έχει τη δυνατότητα ασφαλούς σάρωσης.

9. Ροή εργασιών και σύστημα έκδοσης εισιτηρίων:

Να διαθέτει το προϊόν σύστημα ροής εργασιών που επιτρέπει την εκχώρηση και την παρακολούθηση ζητημάτων. Να μπορεί να εκχωρήσει αυτόματα εισιτήρια με βάση τα καθορισμένα σύνολα κανόνων (δηλαδή ευπάθεια, ιδιοκτήτης, ταξινόμηση περιουσιακών στοιχείων κ.λπ.); Αυτές είναι απαραίτητες δυνατότητες για μια λύση διαχείρισης.

10. Δυνατότητα έρευνας ευπάθειας και ενημέρωσης:

Κάποιος πρέπει να ελέγξει πόσο συχνά εκδίδονται ενημερώσεις από τον προμηθευτή. Ο μηχανισμός διανομής θα πρέπει να αξιοποιεί τα αναγνωρισμένα από τον κλάδο πρωτόκολλα επικοινωνιών ασφαλείας. Επίσης θα πρέπει αν εξεταστεί εάν Έχει ο πωλητής(vendor) τη δική του ερευνητική ομάδα ευπάθειας καθώς και το πώς έχει ανταποκριθεί σε ευπάθειες στα δικά του προϊόντα.

11. Zero-day vulnerability:

Ικανότητα αντιμετώπισης ευπάθειας Zero-day δηλαδή προγνωστική ανάλυση της απειλής στο περιβάλλον χωρίς να απαιτείται νέα σάρωση;

12. Αναφορά (Reporting):

Είναι η αναφορά λεπτομερή και προσαρμόσιμη; Μπορούμε να δημιουργήσουμε αναφορά σύμφωνα με τις νέες τάσεις. Καλό θα είναι οι τύποι αναφορών να επαναχρησιμοποιούνται και σε άλλα εργαλεία.

13. Επιβολή πολιτικής αποκατάστασης:

Να παρέχει το προϊόν τη δυνατότητα προσδιορισμού της επιλεγμένης αποκατάστασης σε διάφορα επίπεδα, από υποχρεωτικό (απαιτούμενο) έως απαγορευμένο (αποδεκτός κίνδυνος), μέσω μιας κεντρικής διεπαφής βάσει πολιτικής;

14. Τεχνική Υποστήριξη:

Αναζητήστε προμηθευτές που προσφέρουν υποστήριξη 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα, κατά προτίμηση μέσω τηλεφώνου, και μάθετε εάν οι πελάτες μπορούν να περιμένουν άμεση απάντηση.

15. Οικονομική προσέγγιση:

Πολλά εργαλεία παρέχουν διαφορετική κατηγορία δανειοδότησης. Κάποιος πρέπει να χαρτογραφήσει την απαίτηση με οικονομικό τρόπο. Λαμβάνοντας υπόψη και παραπάνω από τους 15 παράγοντες, έτσι θα βοηθήσει σίγουρα στην επιλογή της καλύτερης λύσης διαχείρισης ευπαθειών για τον Οργανισμό.

ΔΙΑΧΕΙΡΙΣΗ ΕΥΠΑΘΕΙΑΣ ΒΑΣΗ PCI DSS (ΠΑΡΑΔΕΙΓΜΑ)

Στον παρακάτω πίνακα μπορούμε να δούμε ένα ενδεικτικό αποτέλεσμα ενός Nessus vulnerability scan report βάση του προτύπου PCI το οποίο περιέχει την ευπάθεια την κατηγοριοποίησή της καθώς και τους τρόπους αντιμετώπισης.

Plugin ID	**CVE**	**CVSS**	**Name**	**Synopsis**	**Description**	**Mitigation Actions**	**Solution**
10043	CVE-1999	5.0	Chargen UDP Service Remote DoS	The remote host is	When contacted, chargen responds with some random	It is recommended to follow the solution instructions	- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the

	-01103			running a 'chargen' service.	characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection. The purpose of this service was to mostly test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third-party host using this host as a relay. An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.		following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service.
50686	CVE-	5.8	IP Forwardi	The remote	The remote host has IP forwarding	It is recommended to upgrade	On Linux, you can disable IP forwarding by doing :

	1999-0511		ng Enabled	host has IP forwarding enabled.	enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering. Unless the remote host is a router, it is recommended that you disable IP forwarding.	to JBoss EAP version 4.2.0.CP09 / 4.3.0.CP08.	echo 0 > /proc/sys/net/ipv4/ip_forward On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters On Mac OS X, you can disable IP forwarding by executing the command : sysctl -w net.inet.ip.forwarding=0 For other systems, check with your vendor.
121165	CVE-2018-3821	4.3	Kibana ESA-2018-05	The remote web server hosts a Java application that is vulnerable.	Kibana versions after 5.1.1 and before 5.6.7 and 6.1.3 had a cross-site scripting (XSS) vulnerability in the tag cloud visualization that could allow an attacker to obtain sensitive information from or perform destructive actions on behalf of other Kibana users.	It is recommended to upgrade Elastic Stack to the latest version. We were able to find a workaround using console_extensions.enabled: false. There doesn't seem to be a supported way to disable dependency chains.	Users should upgrade to Kibana version 6.1.3 or 5.6.7. There are no known workarounds for this issue.
77200	CVE-2010-5298	6.8	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.	The OpenSSL service on the remote host is vulnerable to a man-in-the-middle (MiTM) attack, based on its acceptance of a specially crafted handshake. This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been	It is recommended to upgrade OpenSSL to the latest version	OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

					exchanged, which causes predictable keys to be used to secure future traffic. Note that Nessus has only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory : - An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298) - An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache		

					side-channel attack. (CVE-2014-0076) - A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195) - An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198) - An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client. (CVE-2014-0221) - An error		

					exists in the 'dtls1_get_message_fragment' function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470) OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.		
30218		2.6	Terminal Services Encryption Level is not FIPS-140 Compliant	The remote host is not FIPS-140 compliant.	The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.	It is recommended to Change RDP encryption level to : 4. FIPS Compliant	Change RDP encryption level to : 4. FIPS Compliant
18262	CVE-1999-0183	5.0	TFTP Traversal Arbitrary File Access	The remote TFTP server can be used to read arbitrary files on the remo	The TFTP (Trivial File Transfer Protocol) server running on the remote host is vulnerable to a directory traversal attack that allows an attacker to read arbitrary files on the remote host by prepending their names with directory	It is recommended to disable the remote TFTP daemon, run it in a chrooted environment, or filter incoming traffic to this port.	Disable the remote TFTP daemon, run it in a chrooted environment, or filter incoming traffic to this port.

				te host.	traversal sequences.		

*Σημείωση:Το πεδίο solution δημιουργήθηκε χειροκίνητα

IV. ΣΥΜΠΕΡΑΣΜΑ

Χωρίς αυτή τη διαδικασία διαχείρισης ευπάθειας, ο οργανισμός βρίσκεται σε κίνδυνο σε όλη του την υποδομή. Ωστόσο, η υιοθέτηση της προαναφερόμενης προσέγγισης (πρόγραμμα διαχείρισης ευπάθειας) μπορεί σίγουρα να μειώσει τον κίνδυνο σε όλη την υποδομή του οργανισμού.

ΚΕΦΑΛΑΙΟ 5. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ

Η λύση διαχείρισης ευπάθειας που χρησιμοποιείτε θα πρέπει να σχεδιαστεί από την αρχή για να παρέχει στον οργανισμό, αξιολόγηση ευπαθειών και ανάλυση κινδύνου με επίγνωση του πλαισίου. Όλες οι αρχιτεκτονικές θα πρέπει να εξουσιοδοτούν τον οργανισμό να:

1. Γνωρίζει τι υπάρχει στο δίκτυό του μέσω μιας ολοκληρωμένης ανάλυσης όλων των περιουσιακών στοιχείων που βασίζονται σε IP, συμπεριλαμβανομένων των πλατφορμών ιστού, κινητών, cloud και εικονικών.

2. Εντοπίσει τι κρύβεται στις σκιές αναγνωρίζοντας γρήγορα άγνωστους κινδύνους που κρύβονται σε συσκευές BYOT, μη εξουσιοδοτημένες εφαρμογές και άγνωστες θύρες (shadow IT).

3. Μπορεί να διαχειρίζεται τα Δεδομένα τους με υψηλή ευκρίνεια με προβολές ασφαλείας που μπορούν να προσαρμόζονται, καθώς και αναφορές ελέγχου και συμμόρφωσης.

4. Συσχετίζοντας τα exploit με τα Metasploit, Exploit-Database, Canvas και Core Impact να μπορεί να εχει μια ολοκληρωμένη εικόνα για το attack surface.

5. Μπορεί να καλύψει τα κενά ευπάθειας του με βαθιά γνώση σε εικονικά(Virtual), φυσικά (hardware on prem) και cloud based περιβάλλοντα.

6. Να Ενοποιήσει (integration) την ευφυΐα (intelligence) ευπάθειας και απειλών για μια σαφέστερη, πιο ενημερωμένη εικόνα του επιχειρηματικού κινδύνου.

7. Μπορεί να εντοπίζει τις κρυφές απειλές με το Analytics συσχετίζοντας δεδομένα προνομίων (privileges), ευπάθειας και απειλών χαμηλού επιπέδου.

8. Πραγματοποιεί την ενημέρωση κώδικα μέσω αυτοματοποιημένης αποκατάστασης τρωτών σημείων Microsoft, JAVA, Adobe και άλλων, χρησιμοποιώντας ενσωματώσεις τρίτων.

9. Μοιράζεται πληροφορίες ευπάθειας και συνεργαστείτε με άλλα συστήματα πληροφορικής για να επιταχύνει μεγαλύτερη ευαισθητοποίηση σχετικά με την ασφάλεια.

10. Αυτοματοποιήσει τις σαρώσεις διαπιστευτηρίων με προνομιούχα διαπιστευτήρια που εναλλάσσονται συνεχώς.

Επομένως, ένας οργανισμός για να προστατέψει τα περιουσιακά στοιχεία και να δημιουργήσει μια σταθερή άμυνα, πρέπει να βάλει τα δεδομένα στο κατάλληλο πλαίσιο. Άνθρωποι με γνώση του αντικειμένου θα πρέπει να είναι υπεύθυνοι για τη μέτρηση και τον μετριασμό του κινδύνου στον οργανισμό, διότι δεν έχουν την πολυτέλεια να αποτύχουν λόγο της κρισιμότητας της διαδικασίας. Εάν ξεκινάτε εκ νέου, μόλις σας δόθηκε η ευκαιρία να δημιουργήσετε ένα πρόγραμμά μεθοδολογίας διαχείρισης και αποτίμησης ευπαθειών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) ISO/IEC, "Information technology -- Security techniques Code of practice for information security management “.

2) Quays, Vulnerability management for dummies. Chichester: John Wiley & Sons, 2008 eBook

3) Williams, A and Nicollet, M: Improve IT Security With Vulnerability Management, Edwards, Chandra Estelle

4) Finding trust in relational vulnerability: Interpersonal and intrapersonal influences on the intimacy process”.

5) Wikipedia. Vulnerability Management. Retrieved from http://en.wikipedia.org/wiki/Vulnerability_management.

6) Risk and Vulnerability Sustainable Development and Disaster Risk Reduction, Part of the series Disaster Risk Reduction H.W.Njogu, LJ,

7) JN kiere ” comprehensive vulnerability based alert management approach for large networks”

8) S.Furnell ” Vulnerability management: not a patch on where we should be?”Network Security, Volume 2016, Issue 4, April 2016,

9) GIAC certifications Research Papers https://www.giac.org/paper/gsec/32851/implementing-vulnerability-management-process.

10) Matthew Finifter, Devdatta Akhawe, and David Wagner ”An Empirical Study of Vulnerability Rewards Programs”

11) Software Engineering Institute Digital Library http://www.cert.org/archive/pdf/csirt-handbook.pdf13)

12) Weston Comstor Website events http://fr.security.westcon.com

13) W.knowles,D.Prince,D.Hutsion ”A survey of cyber security management in industrial control systems” IJCI Protection.15)

14) CIO Papers/Webcasts http://www.cio.com/article/2379124/secur16)

15) C.Alcarez, S.Zeadallt ”Critical infrastructure protection: Requirements and challenges for the 21st century”

16) Trustwave Services https://www.trustwave.com/Services/Vulnerability-Management.