Α.Τ.Ε.Ι. ΚΑΛΑΜΑΤΑΣ - ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ

Τμήμα Μηχανικών Πληροφορικής ΤΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΤΩΝ ΑΠΕΙΛΩΝ ΠΟΥ ΑΝΤΙΜΕΤΩΠΙΖΟΥΝ ΟΙ ΥΠΟΔΟΜΕΣ INTERNET ΚΑΙ ΠΩΣ ΑΝΤΙΚΡΟΥΟΝΤΑΙ

Επιβλέπων Καθηγητής: Δρ. Πικραμμένος Ιωάννης

Φοιτητής

Νικόλαος Τσεπέρκας *ΑΜ: 2008099*

Σπάρτη, Μάιος 2018

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ **ΥΠΟΓΡΑΦΕΣ**

1.

2.

3.

Ευχαριστίες

Έχοντας φτάσει στο τέλος της πτυχιακής μου εργασίας, αισθάνομαι υποχρεωμέν.. να μιλήσω για κάποιους ανθρώπους, που ο καθένας με τον δικό του τρόπο σηματοδότησε την πορεία των χρόνων μου στις προπτυχιακές σπουδές μου και να τους ευχαριστήσω.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα μου, κύριο Πικραμμένο Ιωάννη, Επιστημονικό Συνεργάτη του Τμήματος Μηχανικών Πληροφορικής ΤΕ του Α.Τ.Ε.Ι. Καλαμάτας, διότι η συνεργασία μαζί του ήταν ένας καταλύτης για την ολοκλήρωση των προπτυχιακών σπουδών μου. Τα αποτελέσματα της εργασίας αυτής είναι από τη συνεργασία με τον κ. Πικραμμένο. Η συνεργασία μας ξεκίνησε όταν ήμουν προπτυχιακός φοιτητής στο χειμερινό εξάμηνο του 2011 – 2012, στο μάθημα «Δίκτυα 1». Από τη συνεργασία αυτή, είχα την πρώτη εμπειρία στις επικοινωνίες. Η πλήρη ηθική στήριξή του και η εμπιστοσύνη του στο πρόσωπό μου, με όπλισαν με κουράγιο, δύναμη και μου έδωσε το θάρρος να αναλάβω την προσπάθεια για επίτευξη των στόχων μου!

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου Χαρίκλεια και Σταμάτη για την αμέριστη υποστήριξή τους όλα αυτά τα χρόνια, των προπτυχιακών σπουδών μου. Αφιερώνω αυτή την εργασία στους γονείς μου, ως ελάχιστη ευγνωμοσύνη για την κατανόηση και την υπομονή τους όλα αυτά τα χρόνια.

Τσεπέρκας Νικόλαος

Σπάρτη, 15/05/2018

Περιεχόμενα

Περίληψη

Η υποδομή του Διαδικτύου υποστηρίζει την παγκόσμια ανταλλαγή πληροφοριών μέσω φυσικών και λογικών πόρων, όπως καλώδια, διακομιστές, πρωτόκολλα, υπηρεσίες. Αυτά τα στοιχεία πάσχουν από διάφορες απειλές που μπορούν να παρεμποδίσουν τη σύνδεση δικτύου και να διαταράξουν το Διαδίκτυο.

Ως απειλητικό τοπίο, η μελέτη αυτή παρέχει μια λεπτομερή επισκόπηση των υφιστάμενων απειλών που αφορούν την υποδομή του Διαδικτύου και τις τάσεις της, έτσι ώστε οι ιδιοκτήτες υποδομών του Διαδικτύου να μπορούν να βελτιώσουν την ασφάλειά τους χρησιμοποιώντας ορθές πρακτικές.

Για το σκοπό αυτό, η μελέτη αυτή περιγράφει λεπτομερώς τα περιουσιακά στοιχεία της υποδομής Διαδικτύου (δομημένα σε οκτώ τύπους: υλικό, λογισμικό, πληροφορίες, ανθρώπινο δυναμικό, πρωτόκολλα, υπηρεσίες, διασυνδέσεις και υποδομή) και απαριθμεί τις απειλές που σχετίζονται με αυτά τα στοιχεία της υποδομής του Διαδικτύου. Αυτά τα αποτελέσματα είναι δομημένα στους χάρτες μυαλού. Στη συνέχεια, η μελέτη ταξινομεί σημαντικές συγκεκριμένες απειλές της υποδομής του Διαδικτύου - συγκεκριμένα απειλές δρομολόγησης, απειλές DNS, άρνηση παροχής υπηρεσιών και γενικές απειλές - και συνδέει κάθε απειλή με έναν κατάλογο περιουσιακών στοιχείων που εκτίθενται.

Ως οδηγός καλής πρακτικής, αυτή η μελέτη περιγράφει έναν κατάλογο καλών πρακτικών που στοχεύουν στην εξασφάλιση ενός ενεργητικού υποδομής του Διαδικτύου από σημαντικές συγκεκριμένες απειλές. Μια ανάλυση κενών εντοπίζει ότι ορισμένα στοιχεία ενεργητικού παραμένουν μη καλυπτόμενα από τις τρέχουσες καλές πρακτικές: ανθρώπινοι πόροι (διαχειριστές και χειριστές) για δρομολόγηση, DNS και άρνηση παροχής υπηρεσιών, καθώς και διαμόρφωση συστήματος και ουσιαστικά πρωτόκολλα διευθυνσιοδότησης για άρνηση παροχής υπηρεσιών.

Η μελέτη αυτή παρέχει στους ιδιοκτήτες υποδομών Διαδικτύου έναν οδηγό για την αξιολόγηση των απειλών που αφορούν τα περιουσιακά τους στοιχεία. Προτείνει συστάσεις για τη βελτίωση της ασφάλειας της υποδομής του Διαδικτύου. Αυτές οι συστάσεις ταξινομούνται σε:

Πέντε τεχνικές συστάσεις:

- Σύσταση 1: Για τους ιδιοκτήτες υποδομών του Διαδικτύου και για τους ρυθμιστικούς οργανισμούς δικτύων ηλεκτρονικών επικοινωνιών, να αξιολογήσετε το σημερινό επίπεδο ασφάλειας, κατανοώντας τα περιουσιακά στοιχεία που καλύπτονται (και δεν καλύπτονται) από τα υφιστάμενα μέτρα ασφαλείας.

- Σύσταση 2: Για τους ιδιοκτήτες υποδομών του Διαδικτύου, να αξιολογηθεί η εφαρμογή προσαρμοσμένων ορθών πρακτικών κατά τρόπο εστιασμένο.

- Σύσταση 3: Για τους ιδιοκτήτες υποδομών Διαδικτύου, συνεργάζονται με την κοινότητα για την ανταλλαγή πληροφοριών σχετικά με τις απειλές και για την προώθηση της εφαρμογής ορθών πρακτικών ως μέτρων άμβλυνσης.

- Σύσταση 4: Για τους χρήστες που χρησιμοποιούν οδηγούς καλών πρακτικών, αναφέρετε τις υλοποιήσεις τους, τα περιουσιακά στοιχεία που καλύπτονται και τα κενά που βρέθηκαν.

- Σύσταση 5: Οι λέξεις έχουν σημασία: Εξασφαλίστε τη σωστή χρήση όρων και ορισμών. Και τέσσερις οργανωτικές συστάσεις:

- Σύσταση 6: Για τους ιδιοκτήτες υποδομών Διαδικτύου, χρησιμοποιήστε τις κατάλληλες μεθόδους αξιολόγησης κινδύνου για να καταλάβετε τα ευπαθή περιουσιακά στοιχεία στην υποδομή σας στο διαδίκτυο και να δώσετε προτεραιότητα στις ενέργειες προστασίας σας.

- Σύσταση 7: Δημιουργία ενός προγράμματος ευαισθητοποίησης και κατάρτισης στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών.

- Σύσταση 8: Οι ιδιοκτήτες υποδομών διαδικτύου υποχρεώνουν τους τρίτους προμηθευτές να εφαρμόζουν μέτρα ασφαλείας.

- Σύσταση 9: Οι ιδιοκτήτες υποδομών διαδικτύου θα πρέπει να παραμένουν ενημερωμένοι για τυχόν ενημερώσεις

1. Εισαγωγή

Το Διαδίκτυο, ως δίκτυο ανεξάρτητων δικτύων υπολογιστών, έχει εξελιχθεί σε μια σημαντική παγκόσμια πλατφόρμα εμπορικού και ιδιωτικού ενδιαφέροντος, καθώς και για την ηλεκτρονική διακυβέρνηση και τις δημόσιες υπηρεσίες για την κοινωνία μας, καθιστώντας έτσι μια απαραίτητη χρησιμότητα για όλους τους τομείς της ζωής. Ως πολύπλοκο σύστημα, εξαρτάται σε μεγάλο βαθμό από διαφορετικά στοιχεία, μηχανισμούς και λειτουργίες σε διάφορα επίπεδα αφαίρεσης. Η υποδομή του Διαδικτύου, ως υποκείμενη βάση, περιλαμβάνει υλικό, υλική υποδομή, διασύνδεση, λογισμικό, πρωτόκολλα, πληροφορίες, υπηρεσίες και ανθρώπινο δυναμικό. Για παράδειγμα, τα δίκτυα (αυτόνομα συστήματα) συνδέονται με στοιχεία των φυσικών στρωμάτων, αλλά αντιμετωπίζονται με λογικά σχήματα διευθύνσεων, μεταφέροντας δεδομένα μέσω ενός συνόλου πρωτοκόλλων στον επιθυμητό προορισμό και χειριστές που μπορούν να πηδήξουν σε δράση όταν προκύψει πρόβλημα. Η αποτυχία αυτών των βασικών στοιχείων δεν προκαλεί μόνο μια διακοπή ενός δικτύου ή ορισμένων συμμετεχόντων, αλλά μπορεί επίσης να επηρεάσει ένα μεγάλο μέρος του Internet, στο σύνολό του.

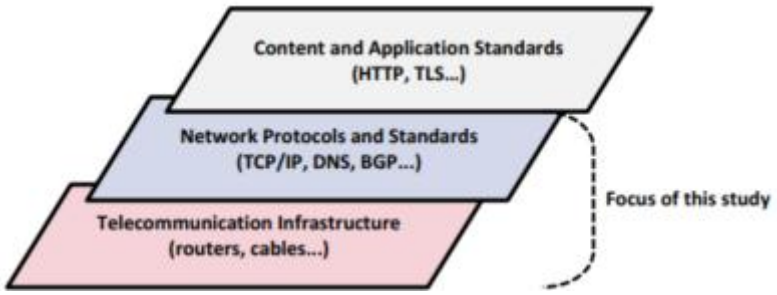
Η μελέτη αυτή αποσκοπεί στη βελτίωση της καθοδήγησης σχετικά με την ασφάλεια της υποδομής του Διαδικτύου. Με αυτόν τον τρόπο, ξεκινάει με την απογραφή των περιουσιακών στοιχείων που μπορούν να βρεθούν σε φορείς εκμετάλλευσης υποδομών του Διαδικτύου, όπως οι πάροχοι υπηρεσιών διαδικτύου (ISP), οι σταθμοί ανταλλαγής μέσω Internet (IXP) ή άλλοι φορείς δικτύου. Με βάση τα στοιχεία που εντοπίστηκαν, η μελέτη αυτή πραγματοποιεί αξιολόγηση απειλών λαμβάνοντας υπόψη τις ιδιαιτερότητες της υποδομής του Διαδικτύου και επιπλέον παρέχει ένα σημείο εκκίνησης για την υποστήριξη περαιτέρω αξιολογήσεων των κινδύνων. Αυτές οι απειλές χαρακτηρίζονται ως σημαντικές ειδικές απειλές για την υποδομή του Διαδικτύου. Τα περιουσιακά στοιχεία και οι απειλές συγκεντρώνονται για τον εντοπισμό των σημαντικότερων ανοιγμάτων. Οι δημιουργοί απειλών, δηλαδή οι παράγοντες απειλής, ταξινομούνται, περιγράφονται και χαρτογραφούνται στις απειλές που εντοπίστηκαν προηγουμένως. Λαμβάνεται περαιτέρω υπόψη για να αναπτυχθεί ένας κατάλογος με τα υπάρχοντα μέτρα, όπως ορθές πρακτικές που αποσκοπούν στη μείωση των επιφανειών προσβολής του περιουσιακού στοιχείου. Μετά από αυτό, εντοπίζονται περιουσιακά στοιχεία που δεν καλύπτονται και αιτιολογείται η έλλειψη μέτρων προστασίας.

1.1. Πεδίο εφαρμογής της μελέτης

Ο ορισμός του Διαδικτύου που χρησιμοποιείται σε ολόκληρη αυτή τη μελέτη είναι παρόμοιος με τον ορισμό που χρησιμοποιείται από το RFC 2026:

Το Διαδίκτυο, μια χαλαρά οργανωμένη διεθνής συνεργασία αυτόνομων διασυνδεδεμένων δικτύων, υποστηρίζει την επικοινωνία υποδοχής με κεντρικό υπολογιστή μέσω της εθελοντικής τήρησης των ανοιχτών πρωτοκόλλων και διαδικασιών που καθορίζονται από τα πρότυπα του Διαδικτύου. Υπάρχουν επίσης πολλά απομονωμένα διασυνδεδεμένα δίκτυα, τα οποία δεν συνδέονται με το παγκόσμιο Internet αλλά χρησιμοποιούν τα πρότυπα του Διαδικτύου.

Με βάση αυτόν τον ορισμό, η υποδομή διαδικτύου αποτελείται από ένα ευρύ φάσμα περιουσιακών στοιχείων που διαμένουν σε διαφορετικά φυσικά και λογικά επίπεδα, τα οποία είναι κρίσιμα για τη σωστή λειτουργία της. Το πεδίο αυτής της μελέτης επικεντρώνεται στις απειλές που εφαρμόζονται σε αυτά τα φυσικά και λογικά περιουσιακά στοιχεία, όπως παρουσιάζονται στο Σχήμα 1 .



Σχήμα 1 - Εστίαση του τοπίου απειλών και οδηγός ορθής πρακτικής για την υποδομή Internet

Η μελέτη αυτή προτείνει ένα απειλητικό τοπίο, το οποίο αποτελεί μια επισκόπηση των τρεχουσών απειλών που ισχύουν για την Υποδομή Διαδικτύου και τις σχετικές τάσεις. Ο στόχος είναι να ενισχυθεί η ασφάλεια της υποδομής του Διαδικτύου, περιγράφοντας μια λίστα με καλές πρακτικές και συστάσεις για σημαντικές συγκεκριμένες απειλές.

1.2. Δομή αυτής της μελέτης

Η υπόλοιπη μελέτη οργανώνεται ως εξής:

Το Κεφάλαιο 2 δίνει μια εικόνα για τη μεθοδολογία που ακολουθήθηκε κατά την εκτέλεση αυτής της μελέτης.

Το Κεφάλαιο 3 παρουσιάζει όλους τους σχετικούς τύπους περιουσιακών στοιχείων υποδομής Διαδικτύου Μια επισκόπηση των περιουσιακών στοιχείων και των εξαρτήσεων τους απεικονίζεται σε ένα χάρτη μυαλού.

Στο Κεφάλαιο 4 αναπτύσσονται οι τύποι απειλών που εκτίθενται στα στοιχεία ενεργητικού που έχουν οριστεί προηγουμένως. Η ανεπτυγμένη ταξινόμηση παρουσιάζεται ως χαρτογράφος και οι πιο σχετικές απειλές συγκεντρώνονται σε σημαντικές ειδικές ομάδες απειλών και οι τάσεις τους υποδεικνύονται.

Το Κεφάλαιο 5 ασχολείται με την έκθεση των προσδιορισμένων περιουσιακών στοιχείων στις απειλές του κυβερνοχώρου.

Το Κεφάλαιο 6 εισάγει τους παράγοντες κινδύνου και τους χαρτογραφεί σε σχέση με τους τύπους απειλών.

Το Κεφάλαιο 7 απαριθμεί και συνοψίζει τα διαθέσιμα μέτρα ασφάλειας υποδομής του Διαδικτύου που μετριάζουν τις σημαντικές συγκεκριμένες απειλές. Τα περιουσιακά στοιχεία που δεν καλύπτονται προσδιορίζονται και περιγράφονται οι λόγοι.

Το Κεφάλαιο 8 βασίζεται στα διδάγματα που αντλήθηκαν κατά τη διάρκεια της μελέτης και συνοψίζει τις εμπειρίες που αποκτήθηκαν σε τεχνικές και οργανωτικές συστάσεις.

Το κεφάλαιο 9 καταλήγει στο συμπέρασμα.

Το υλικό που αναφέρεται σε μια διεύθυνση URL στις υποσημειώσεις διατίθεται την ημέρα της δημοσίευσης αυτής της μελέτης. Αξίζει επίσης να σημειωθεί ότι για να διατηρηθεί το μέγεθος αυτής της μελέτης εύχρηστο, παρέχεται λεπτομερές υλικό μέσω παραρτημάτων. Αυτά υποστηρίζουν τους ιδιοκτήτες περιουσιακών στοιχείων υποδομής του Διαδικτύου για την εκτίμηση κινδύνου.

2. Μεθοδολογία

Προκειμένου να προσδιοριστούν τα απαιτούμενα επίπεδα προστασίας για πολύτιμα περιουσιακά στοιχεία, είναι σύνηθες να διενεργείται εκτίμηση κινδύνου. Στη συνέχεια, πρέπει να θεσπιστούν μέτρα ασφαλείας για την επίτευξη εκτιμημένων επιπέδων προστασίας με τον μετριασμό (μέρους) των εκτιμώμενων κινδύνων. Μπορούν να μεταφερθούν ή να γίνουν δεκτοί και άλλοι Όπως αναλύεται στη συνέχεια, οι απειλές αποτελούν σημαντικό στοιχείο για την εκτίμηση των κινδύνων.

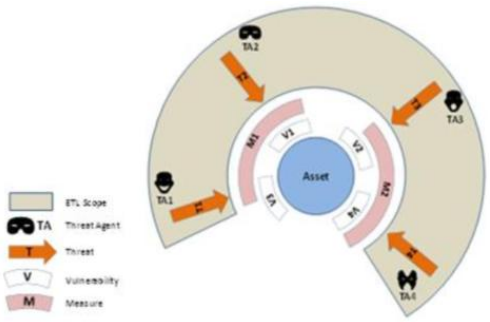
Σε αυτή την ενότητα παρουσιάζεται η μεθοδολογία που ακολουθείται στο IITL. Αποτελείται από διάφορες απειλές στις οποίες εκτίθενται τα περιουσιακά στοιχεία της υποδομής Διαδικτύου. Ως εκ τούτου, το παρουσιαζόμενο IITL είναι ένα σημαντικό εργαλείο για όσους θέλουν να αξιολογήσουν τους κινδύνους σε ένα περιβάλλον πληροφορικής οποιασδήποτε πολυπλοκότητας. Με βάση αυτούς τους κινδύνους, μπορούν να επιλεγούν κατάλληλα μέτρα ασφαλείας για την επίτευξη μετριασμού του κινδύνου. Οι αναγνωρισμένες ορθές πρακτικές μπορούν να χρησιμοποιηθούν ως κατευθυντήρια γραμμή για την επίτευξη αυτού του στόχου.

Ο ρόλος των απειλών στις εξισώσεις αξιολόγησης κινδύνων γίνεται εμφανής όταν εξετάζουμε τα συστατικά των κινδύνων. Σύμφωνα με τον ευρέως αποδεκτό ορισμό του ISO 27005, οι κίνδυνοι αναδύονται όταν: " *Απειλείται η ευπάθεια των περιουσιακών στοιχείων από την κατάχρηση για να προκληθεί βλάβη στον οργανισμό* ". Σε πιο λεπτομερείς όρους, ο κίνδυνος θεωρείται ότι λαμβάνει υπόψη τα ακόλουθα στοιχεία:

> ***Περιουσιακά στοιχεία*** *(Ευπάθειες, Έλεγχοι),* ***Απειλή*** *(Προφίλ απειλητικού παράγοντα, Πιθανότητα) και* ***Αντίκτυπος***

Η μελέτη αυτή δεν προϋποθέτει τη χρήση οποιουδήποτε συγκεκριμένου εξοπλισμού υποδομής Διαδικτύου ή δικτύου ή των επιχειρησιακών διαδικασιών ή υπηρεσιών. Ως εκ τούτου, είναι αδύνατο να προβούμε σε έγκυρες υποθέσεις σχετικά με τις επιπτώσεις και τις ευπάθειες των περιουσιακών στοιχείων. Αυτές είναι δραστηριότητες που μπορούν να εκτελεστούν αποκλειστικά από τον ιδιοκτήτη του περιουσιακού στοιχείου. Ως εκ τούτου, η ανάγκη υποστήριξης εργαλείων για την εκτίμηση των κινδύνων γίνεται προφανής και απαραίτητη για τον ιδιοκτήτη του περιουσιακού στοιχείου σε αυτό το πολύπλοκο περιβάλλον.

Τα στοιχεία κινδύνων απεικονίζονται γραφικά στο παρακάτω σχήμα 2 :



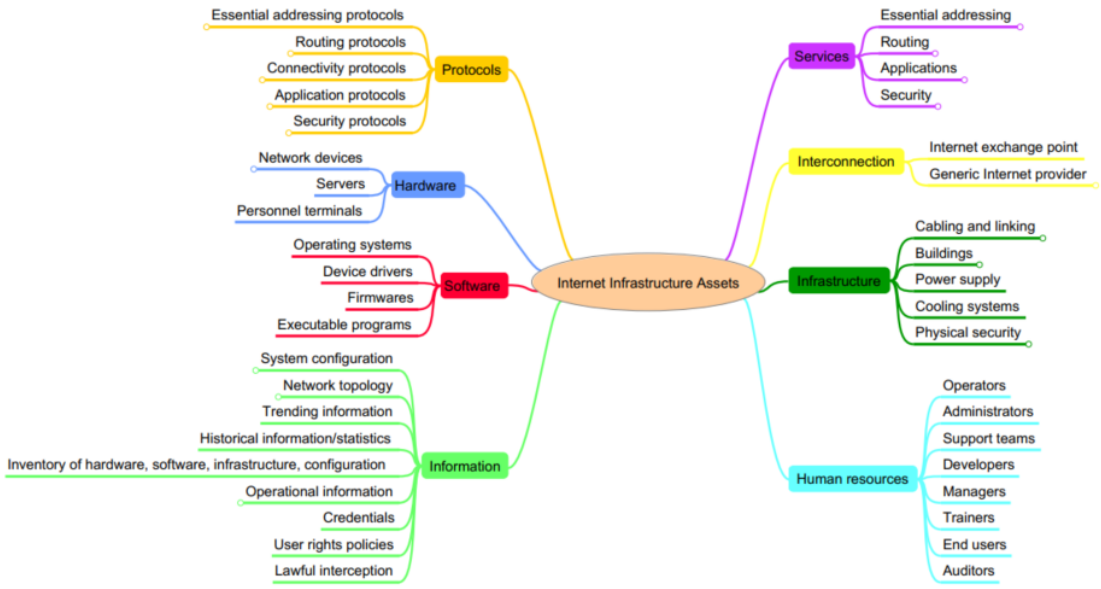
Εικόνα 2 - Απειλές που στοχεύουν ένα περιουσιακό στοιχείο προσπαθώντας να εκμεταλλευτούν τις ευπάθειές του

Το ποσοστό αυτό έχει εγκριθεί από την ISO 13335-4 και δείχνει πως μέσα απειλή (βλ κεφάλαιο 6), αναπτύσσοντας απειλές (Τ), προσπαθήστε να εκμεταλλευτείτε τα ευάλωτα περιουσιακά στοιχεία (V), προκειμένου να βλάψετε / να αναλάβετε το περιουσιακό στοιχείο. Ο κύριος του ενεργητικού έχει εφαρμόσει μέτρα ασφαλείας (Μ) για την προστασία του περιουσιακού στοιχείου, δηλαδή για την εξάλειψη ή τη σημαντική μείωση των τρωτών σημείων. Ο αντίκτυπος που επιτυγχάνεται με την πιθανή υλοποίηση μιας απειλής είναι το τελικό στοιχείο για την αξιολόγηση του κινδύνου ενός περιουσιακού στοιχείου (βλ. Επίσης τον ορισμό του κινδύνου παραπάνω).

3. Περιουσιακά στοιχεία υποδομής διαδικτύου

Σύμφωνα με την *κατευθυντήρια γραμμή* του ENISA *για τις απειλές και τα περιουσιακά στοιχεία που* δημοσιεύθηκε στο πλαίσιο του *πλαισίου ασφαλείας* του ENISA *για τα άρθρα 4 και 13 μια* πρόταση, ένα περιουσιακό στοιχείο ορίζεται *ως "... οτιδήποτε αξίας. Τα περιουσιακά στοιχεία μπορούν να είναι αφηρημένα περιουσιακά στοιχεία (όπως διαδικασίες ή φήμη), εικονικά περιουσιακά στοιχεία (για παράδειγμα, δεδομένα), φυσικά περιουσιακά στοιχεία (καλώδια, εξοπλισμός), ανθρώπινοι πόροι, χρήματα »* . Ωστόσο, για λόγους ασφάλειας των πληροφοριών, αυτή η μελέτη επικεντρώνεται σε στοιχεία ενεργητικού που σχετίζονται κυρίως με την τεχνολογία της πληροφορίας και της επικοινωνίας (ΤΠΕ) στο πλαίσιο της υποδομής του Διαδικτύου.

Τα περιουσιακά στοιχεία της υποδομής Διαδικτύου εξασφαλίζουν τη συνδεσιμότητα των δικτύων από φυσική και λογική άποψη. Παρουσιάζεται μια ταξινόμηση περιουσιακών στοιχείων για τη διάρθρωση όλων των σχετικών περιουσιακών στοιχείων, όπως απεικονίζεται στο σχήμα 3 . Λόγω της πολυπλοκότητας της υποδομής του Διαδικτύου, τα περιουσιακά στοιχεία ομαδοποιούνται σε τύπους περιουσιακών στοιχείων διαφορετικής περιεκτικότητας και εμβέλειας. Για παράδειγμα, η λειτουργία ενός δρομολογητή απαιτεί το υλικό που μπορεί να βρεθεί σε μια φυσική θέση, μια διαμόρφωση, λογισμικό που παράγει τη διαμόρφωση, βασικές υπηρεσίες διευθυνσιοδότησης για διασύνδεση που ορίζονται από ένα σύνολο πρωτοκόλλων και ένας χειριστής για την παρακολούθηση της τρέχουσας κατάστασής του. Ως εκ τούτου, η διακριτότητα των τύπων περιουσιακών στοιχείων, ακόμα και αν είναι διατεταγμένα στο ίδιο επίπεδο της ταξινόμησης, μπορεί να διαφέρει. Εκτός από τα περιουσιακά στοιχεία των ΤΠΕ, εντοπίζονται διάφορα περιουσιακά στοιχεία εκτός της πληροφορικής. Αυτά εξαρτώνται έντονα από τις ΤΠΕ και είναι κεντρικά για την ορθή λειτουργία του Διαδικτύου. Για παράδειγμα, κτίρια, τροφοδοτικά, συστήματα ψύξης ή ανθρώπινοι πόροι. Λεπτομερής περιγραφή αυτών των στοιχείων ενεργητικού περιλαμβάνεται στο παράρτημα Α.



Εικόνα 3 - Περιουσιακά στοιχεία της υποδομής Διαδικτύου (επίπεδα 1 και 2 - βλέπε παράρτημα Β για τον εκτεταμένο χάρτη μυαλού)

Ο χάρτης μυαλού που παρουσιάζεται στο σχήμα 3 δίνει μια επισκόπηση όλων των στοιχείων που προσδιορίζονται και είναι δομημένη σε τύπους περιουσιακών στοιχείων ανάλογα με τη χρήση τους. Ωστόσο, ένα περιουσιακό στοιχείο δεν είναι αναγκαστικά αποκλειστικό μέλος μόνο ενός τύπου περιουσιακού στοιχείου. Για λόγους αναγνωσιμότητας, οι λεπτομέρειες του χάρτη μυαλού περιορίζονται στο δευτεροβάθμιο επίπεδο. Μια εκτεταμένη έκδοση παρουσιάζεται στο παράρτημα Β . Στη συνέχεια παρουσιάζονται οι τύποι περιουσιακών στοιχείων για το πρώτο επίπεδο του χάρτη μυαλού:

Τα **υλικά** , το **λογισμικό** , οι **πληροφορίες** και οι **ανθρώπινοι πόροι** των περιουσιακών στοιχείων περιλαμβάνουν τα ίδια περιουσιακά στοιχεία όπως και στις προηγούμενες μελέτες και μπορεί να θεωρηθεί ως διαισθητικά σαφής. Επιπλέον, τα ακόλουθα ισχύουν ιδιαίτερα για την υποδομή του Διαδικτύου:

- Ένα **πρωτόκολλο** είναι ένα σύνολο ψηφιακών κανόνων για την ανταλλαγή δεδομένων εντός ή μεταξύ συστημάτων υπολογιστών. Τα πρωτόκολλα είναι πολύτιμα περιουσιακά στοιχεία για την υποδομή του Διαδικτύου επειδή επιτρέπουν την ουσιαστική επικοινωνία μεταξύ διαφορετικών συστημάτων υπολογιστών.

- Μια **υπηρεσία** , όσον αφορά την υποδομή του Διαδικτύου, αναφέρεται σε έναν αφηρημένο συνδυασμό άλλων λειτουργιών που χρησιμοποιούν άλλα περιουσιακά στοιχεία για να εκπληρώσουν μια καθορισμένη εργασία. Οι υπηρεσίες είναι σημαντικές, καθώς το Διαδίκτυο είναι χτισμένο γύρω από τις υπηρεσίες.

- **Η διασύνδεση** καλύπτει τις οργανώσεις που δημιουργούν και εκτελούν μεγάλα δίκτυα υπολογιστών. Δεδομένου ότι το Διαδίκτυο είναι ένα δίκτυο διαφορετικών μεγάλων δικτύων υπολογιστών, τα περιουσιακά στοιχεία που παρέχουν τη δυνατότητα διασύνδεσης είναι πολύτιμα.

- Ο όρος **υποδομή** υποδηλώνει τις βασικές φυσικές δομές και εγκαταστάσεις (π.χ. κτίρια και καλώδια) που απαιτούνται για τη λειτουργία του Διαδικτύου. Προκειμένου να δημιουργηθεί ένα παγκόσμιο δίκτυο δικτύων, το λεγόμενο Διαδίκτυο, η υποστηρικτική υποδομή είναι ζωτικής σημασίας.

Η ταξινόμηση του περιουσιακού στοιχείου που παρουσιάζεται πρέπει να θεωρείται ως στιγμιότυπο της σύνθετης γκάμας περιουσιακών στοιχείων του Διαδικτύου και δεν μπορεί να είναι εξαντλητική.

4. Απειλές της υποδομής του Διαδικτύου

4.1. Τύποι απειλών

Σύμφωνα με το Γλωσσάρι του ENISA, απειλή είναι *"κάθε περιστατικό ή γεγονός με πιθανότητα να επηρεάσει αρνητικά ένα περιουσιακό στοιχείο μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης δεδομένων ή / και άρνησης παροχής υπηρεσίας"* .

Με βάση τα αναγνωρισμένα περιουσιακά στοιχεία του προηγούμενου κεφαλαίου, αναπτύσσεται ταξινόμηση σχετικών απειλών που παρεμποδίζουν την υποδομή του Διαδικτύου ή τουλάχιστον σημαντικά τμήματα.

Δεδομένου ότι η μελέτη αυτή επικεντρώνεται στην ασφάλεια των πληροφοριών, η ταξινόμηση απειλών που παρουσιάζεται αφορά κυρίως απειλές για την ασφάλεια στον κυβερνοχώρο. Ωστόσο, για την άψογη λειτουργία απαιτούνται επίσης φυσικά περιουσιακά στοιχεία και ως εκ τούτου λαμβάνονται διάφορες συγκεκριμένες απειλές εκτός της πληροφορικής. Οι απειλές που εντοπίστηκαν είναι η ενοποίηση των εκδόσεων ENISA Threat Landscape 2013 , το τοπίο απειλής έξυπνου δικτύου και ο οδηγός ορθής πρακτικής το Πλαίσιο Ασφαλείας για την πρόταση των άρθρων 4 και 13α και η *κατευθυντήρια γραμμή* του ENISA *για τις απειλές και τα περιουσιακά στοιχεία* . Συνεπώς, παρουσιάζεται το πρώτο επίπεδο της ταξινόμησης απειλών και παρέχονται ορισμένες περιπτώσεις συναφών απειλών.

Οι απειλές έχουν ανασυγκροτηθεί με τους τύπους απειλών, με κάθε τύπο απειλής να αντιπροσωπεύει την πηγή αιτία μιας απειλής. Είναι τα εξής:

- **Οι φυσικές επιθέσεις** είναι εκ προθέσεως επιθετικές ενέργειες που αποσκοπούν στην καταστροφή, έκθεση, αλλαγή, απενεργοποίηση, κλοπή ή απόκτηση μη εξουσιοδοτημένης πρόσβασης σε φυσικά περιουσιακά στοιχεία όπως υποδομή, υλικό ή διασύνδεση. Αυτός ο τύπος απειλής βασικά ισχύει για κάθε είδους υποδομή εν γένει, και επίσης για την υποδομή του Διαδικτύου. Περιπτώσεις, μεταξύ άλλων, είναι ο βανδαλισμός, η κλοπή, το σαμποτάζ, η διαρροή πληροφοριών και οι βομβιστικές επιθέσεις.

- Μια **καταστροφή** είναι μια σοβαρή διατάραξη της λειτουργίας μιας κοινωνίας και μπορεί να διαιρεθεί σε φυσικές καταστροφές που δεν προκαλούνται άμεσα από τον άνθρωπο και περιβαλλοντικές καταστροφές που προκαλούνται άμεσα από τον άνθρωπο. Αυτές οι απειλές ισχύουν για οποιοδήποτε είδος περιουσιακού στοιχείου εν γένει, και επομένως και για την υποδομή του Διαδικτύου. Τυπικές απειλές αυτής της τάξης είναι οι σεισμοί, οι πλημμύρες, οι πυρκαγιές και η ρύπανση, η σκόνη ή η διάβρωση.

- Η κατάσταση μη λειτουργίας ή ανεπαρκούς λειτουργίας οποιουδήποτε στοιχείου υποδομής διαδικτύου ορίζεται ως **βλάβη ή δυσλειτουργία** . Για παράδειγμα, βλάβες ή διαταραχές συσκευών δικτύου ή συστημάτων, σφάλματα λογισμικού ή σφάλματα διαμόρφωσης.

- **Οι διακοπές** είναι απροσδόκητες διακοπές λειτουργίας ή μείωση της ποιότητας κάτω από ένα απαιτούμενο επίπεδο. Αυτό περιλαμβάνει όλα τα είδη περιουσιακών στοιχείων, ακόμη και τους ανθρώπινους πόρους. Οι διακοπές μπορεί να έχουν πολλούς λόγους, μεταξύ των οποίων, μεταξύ άλλων, η έλλειψη πόρων, εξαντλήσεων, υπερβολικές τάσεις ή ανθρώπινοι παράγοντες όπως η απουσία προσωπικού.

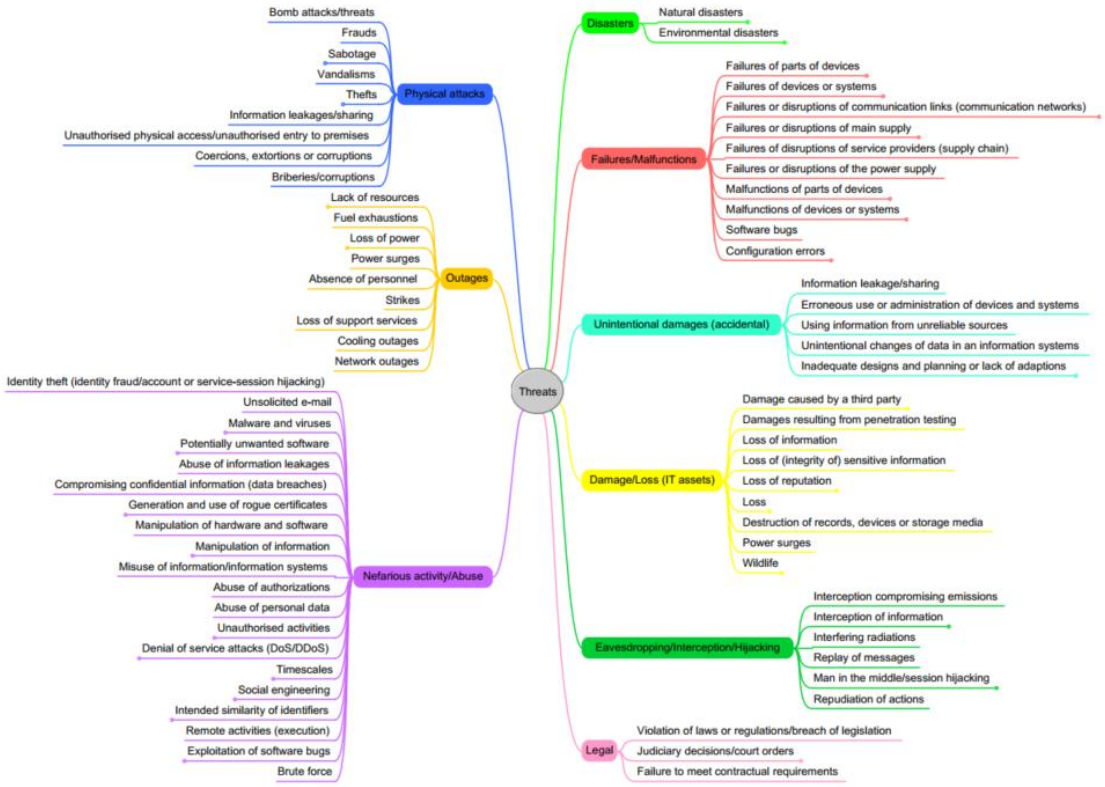
- **Οι ακούσιες ζημιές** αφορούν καταστροφή, βλάβη ή τραυματισμό σε ακίνητα ή πρόσωπα κατά λάθος. Οι ζημιές περιλαμβάνουν φυσικές ζημιές καθώς και διαρροές πληροφοριών, αλλοιώσεις συστημάτων, ανεπαρκή σχέδια ή έλλειψη προσαρμογής.

- **Η ζημιά** αναφέρεται σε καταστροφή, βλάβη ή τραυματισμό περιουσίας ή προσώπων και έχει ως αποτέλεσμα την αποτυχία ή τη μείωση της χρησιμότητας. Οι συγκεκριμένες απειλές είναι παρόμοιες με τις ακούσιες ζημιές, αλλά επικεντρώνονται κυρίως στα περιουσιακά στοιχεία πληροφορικής και συνεπάγονται πρόθεση. Σημαντικοί εκπρόσωποι είναι οι απειλές όπως η απώλεια πληροφοριών, η απώλεια φήμης και η απώλεια υλικού.

- **Οι άσχετες δραστηριότητες και η κατάχρηση** προορίζονται για δράσεις που στοχεύουν συστήματα, υποδομές και / ή δίκτυα ΤΠΕ μέσω κακόβουλων πράξεων με στόχο είτε να κλέψουν, να αλλάξουν ή να καταστρέψουν έναν καθορισμένο στόχο. Αυτή η τάξη της ταξινόμησης οργανώνει κοινές απειλές γενικά αναφερόμενες ως επιθέσεις στον κυβερνοχώρο και συναφείς ενέργειες όπως spam, κακόβουλο λογισμικό, χειραγώγηση υλικού και λογισμικού, διανομή DDoS, μη εξουσιοδοτημένη χρήση, κοινωνική μηχανική ή εκμετάλλευση σφαλμάτων λογισμικού.

- **Υποκλοπής / Υποκλοπής / Αποκάλυψη** αναφέρεται σε μια κατηγορία ενεργειών που αποσκοπούν στην ακρόαση, διακοπή ή κατάσχεση του ελέγχου μιας επικοινωνίας τρίτου μέρους χωρίς τη συναίνεση.

- **Οι νομικές** απειλές μπορούν να προβλεφθούν, να επιδιωχθούν ή να συνεχιστούν δικαστικές ενέργειες τρίτων (αναθέτοντες ή μη), προκειμένου να απαγορευθούν οι ενέργειες ή να αποκατασταθεί η ζημία βάσει του εφαρμοστέου δικαίου. Τέτοιες νομικές απειλές περιλαμβάνουν παραβίαση νόμων, δικαστικές εντολές και αδυναμία εκπλήρωσης των συμβατικών απαιτήσεων που εκτελούνται από ή παραχωρούνται σε παρόχους υπηρεσιών των δικαιούχων της υποδομής δικτύου.



Σχήμα 4 - Ταξινόμηση της απειλής της υποδομής του Διαδικτύου (επίπεδα 1 και 2 - βλ. Παράρτημα Γ για τον εκτεταμένο χάρτη μυαλού)

Ο χάρτης μυαλού που παρουσιάζεται στο σχήμα 4 κατασκευάζει όλους τους προσδιορισμένους τύπους απειλών και τις συγκεκριμένες συναφείς απειλές. Για λόγους αναγνωσιμότητας, ο χάρτης μυαλού περιγράφει μόνο τα δύο πρώτα επίπεδα. Μια εκτεταμένη έκδοση παρουσιάζεται στο παράρτημα Γ .

Πρέπει να σημειωθεί ότι τα στοιχεία που παρουσιάζονται αντικατοπτρίζουν την τρέχουσα κατάσταση των προαναφερθεισών αναφορών. Ωστόσο, υπόκεινται σε αλλαγές σε περίπτωση νέων εξελίξεων και θα πρέπει να θεωρούνται ως ζωντανά έγγραφα που αντικατοπτρίζουν δυναμικές αλλαγές στο περιβάλλον απειλής στον κυβερνοχώρο.

4.2. Σημαντικές συγκεκριμένες απειλές της υποδομής Διαδικτύου

Σε αυτό το κεφάλαιο εντοπίζονται απειλές ειδικά για την υποδομή του Internet. Όπως αναφέρθηκε προηγουμένως, το Διαδίκτυο αποτελεί τη ραχοκοκαλιά της σύγχρονης κοινωνίας των πληροφοριών μας και, ως εκ τούτου, τα τρωτά σημεία αυτής της κρίσιμης υποδομής δεν περιορίζονται σε μεμονωμένες εταιρείες ή σε ορισμένους τελικούς χρήστες, αλλά μπορούν να θέσουν σε κίνδυνο σημαντικό τμήμα του Διαδικτύου. Αυτό απειλεί την καθημερινή ζωή χιλιάδων χρηστών. Το παρελθόν αναπτύχθηκε απειλή ταξινόμησης (βλ κεφάλαιο 4) περιλαμβάνει αρκετές απειλές που ισχύουν γενικά για την τεχνολογία της πληροφορίας και των τηλεπικοινωνιών και συνεπώς πρέπει να ληφθούν υπόψη και για την υποδομή του Διαδικτύου. Ωστόσο, για να ληφθεί υπόψη το πεδίο εφαρμογής της μελέτης, συνιστάται η εξέταση των απειλών αποκλειστικά από την υποδομή του Διαδικτύου για μια βαθύτερη ανάλυση. Παραδέχεται μια βαθύτερη κατανόηση των λεπτομερειών των απειλών

και επιτρέπει τη συγκέντρωση στην προστασία των σχετικών περιουσιακών στοιχείων κατά τη διάρκεια της απογραφής των ορθών πρακτικών στο Κεφάλαιο 7 παρακάτω.

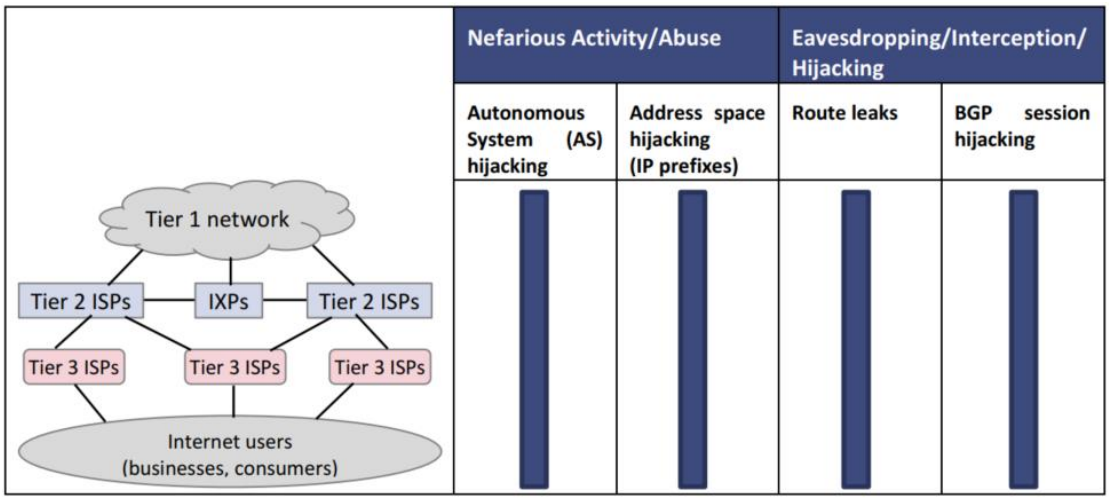
Για να εντοπίσει σημαντικές συγκεκριμένες απειλές, αυτή η μελέτη καταγράφει έγκυρες αναφορές απειλών. Το υλικό που αναλύθηκε έχει δημοσιευθεί από ιδιωτικούς και δημόσιους οργανισμούς και κοινότητες . Για κάθε απειλή, η σημασία ανάλογα με τη συχνότητα της εμφάνισης, δίνοντας μια εκτίμηση αν δεν υπήρχαν έγκυρα δεδομένα και αξιολογούνται οι εκτιμήσεις των εμπειρογνωμόνων.

Η καταληκτική λίστα συγκεντρώνεται σε **ομάδες απειλών** σύμφωνα με τα εκτεθειμένα περιουσιακά στοιχεία. Κάθε ομάδα απειλών συγκεντρώνει τις απειλές που απειλούν έναν συγκεκριμένο τεχνικό τομέα ή / και τεχνολογία, χωρίς διακρίσεις όσον αφορά τον τύπο απειλής τους. Οι κύριες ομάδες απειλή είναι **δρομολόγησης απειλές, οι απειλές DNS, DDoS απειλές** και **γενικές απειλές** που δεν αφορούν ειδικά την υποδομή του Διαδικτύου, όπως υποδηλώνεται παραπάνω. Έτσι, οι απειλές και οι ομάδες απειλών που παρουσιάζονται σε αυτό το τμήμα αντικατοπτρίζουν την τρέχουσα κατάσταση, αλλά δεν είναι και δεν θα είναι ποτέ εξαντλητικές. Ωστόσο, μπορεί κανείς να υποστηρίξει ότι το δεδομένο σύνολο απειλών εξακολουθεί να έχει μεγάλη σημασία και πρέπει να λαμβάνεται υπόψη στις αξιολογήσεις κινδύνου που διενεργούν οι ιδιοκτήτες περιουσιακών στοιχείων.

Στη συνέχεια παρουσιάζονται οι ομάδες απειλών και οι απειλές τους. Για κάθε ομάδα απειλών αναφέρεται ο σχετικός τύπος απειλής στην παρουσιαζόμενη ταξινόμηση, ακολουθούμενη από περιγραφή όλων των υποδεέστερων συγκεκριμένων σημαντικών απειλών. Το επίπεδο λεπτομέρειας περιορίζεται σε κάποιο βαθμό για να διατηρηθεί η αναγνωσιμότητα. Για να καταδείξει τη σημασία της απειλής, συμπληρώνεται με ένα παράδειγμα πρόσφατου περιστατικού. Σημειώστε ότι ο κατάλογος δεν έχει προτεραιότητα, αλλά οι τάσεις για τις ομάδες απειλών παρέχονται έτσι ώστε οι ιδιοκτήτες περιουσιακών στοιχείων να μπορούν να αξιολογήσουν τις προτεραιότητές τους μετά από αξιολόγηση κινδύνου.

4.2.1. Απειλές δρομολόγησης

Η δρομολόγηση υπόκειται σε επιθέσεις που μπορούν να βλάψουν τη διασύνδεση των δικτύων καθώς και τη λειτουργία μεμονωμένων δικτύων. Η ομαλή λειτουργία της υποδομής δρομολόγησης είναι ζωτικής σημασίας για την ευρωστία του Διαδικτύου. Οι περισσότερες απειλές καταστρέφουν τις λειτουργίες δρομολόγησης με αεροπειρατεία, κατάχρηση, εσφαλμένη ρύθμιση ή παρεμπόδιση αριθμών, διευθύνσεων ή χώρων ονόματος. Η τρέχουσα τάση δείχνει ότι η απειλή αυτή αυξάνεται.



Πίνακας 1 - Εφαρμογή σημαντικής συγκεκριμένης απειλής στη δρομολόγηση

Ο Πίνακας 1 υπογραμμίζει την εφαρμογή σημαντικών ειδικών απειλών για την υποδομή δρομολόγησης, για δίκτυα Tier 1, ISPs Tier 2 και IXPs, Tier 3 ISPs και τελικούς χρήστες. Η έκταση μιας απειλής αντιπροσωπεύεται από μια έγχρωμη ράβδο, η οποία υποδηλώνει τον τρόπο με τον οποίο η απειλή ισχύει για τα στρώματα που απεικονίζονται στο αριστερό πλάνο. Οι απειλές δρομολόγησης ισχύουν για όλα τα επίπεδα της Υποδομής Διαδικτύου.

Αυτές οι σημαντικές ειδικές απειλές είναι τώρα λεπτομερείς και παρουσιάζονται οι τάσεις τους.

Τύπος απειλής: Φανερή Δραστηριότητα / Κατάχρηση

Τάση: Αύξηση

Απειλή: Κλοπή του αυτόνομου συστήματος (AS)

Καθώς οι επιθέσεις αεροπειρατείας αποσκοπούν στην απομίμηση της οργάνωσης του θύματος. Το κίνητρο για αυτό το είδος επίθεσης είναι κακόβουλο: οι δραστηριότητες που διεξάγονται με το αεροπειρατειακό δίκτυο αποκρύπτονται και φαίνεται να εκτελούνται εξ ονόματος του ίδιου του θύματος. Τέτοιες επιθέσεις χαρακτηρίζονται από έναν εισβολέα που ανακοινώνει τα προθέματα του θύματος που προέρχονται από το θύμα ΟΠΩΣ ΚΑΙ.

Παράδειγμα:

- Μια εγκληματολογική μελέτη περί της πειρατείας του AS: η προοπτική του εισβολέα

Απειλή: Αποσύνδεση χώρου διευθύνσεων (προθέματα IP)

Αυτή η απειλή εμφανίζεται όταν ένας αδίστακτος συνεργάτης του BGP ανακοινώνει κακόβουλα τα προθέματα ενός θύματος σε μια προσπάθεια να ανακατευθύνει κάποια ή όλη την κίνηση μέσω των δικών του δικτύων για δυσάρεστους σκοπούς (για παράδειγμα, για να δείτε τα περιεχόμενα της κίνησης που διαφορετικά δεν θα μπορούσε να διαβάσει ο δρομολογητής).

Παραδείγματα:

- Ο χάκερ ανακατευθύνει την κίνηση από 19 παροχείς Internet για να κλέψει bitcoins
- Hijack από AS4761 - Indosat, ένα γρήγορο repo rt
- Η νέα απειλή: στοχευμένη κακή μετακίνηση του Internet
- Κοιτάζοντας το Spamhaus DDoS από την άποψη του BGP
- Το Πακιστάν πειράζει το YouTube

Τύπος απειλής: Υποκλοπή / Παρακολούθηση /

Τάση της πειρατείας: Αύξηση

Απειλή: Διαρροές διαδρομής

Μια διαρροή διαδρομής λέγεται ότι συμβαίνει όταν το AS *A* διαφημίζει τις διαδρομές BGP που έχει λάβει από το AS *B* στους γείτονές του, αλλά το AS *A* δεν θεωρείται παροχέας διαμετακόμισης για τα ανακοινωθέντα προθέματα.

Παραδείγματα:

- Hijack από AS4761 - Indosat, μια γρήγορη αναφορά
- Πώς το Internet στην Αυστραλία κατέβηκε κάτω
- Μεγάλες διαρροές διαδρομής

Απειλή: Απόπειρα χειραγώγησης της σύσκεψης BGP

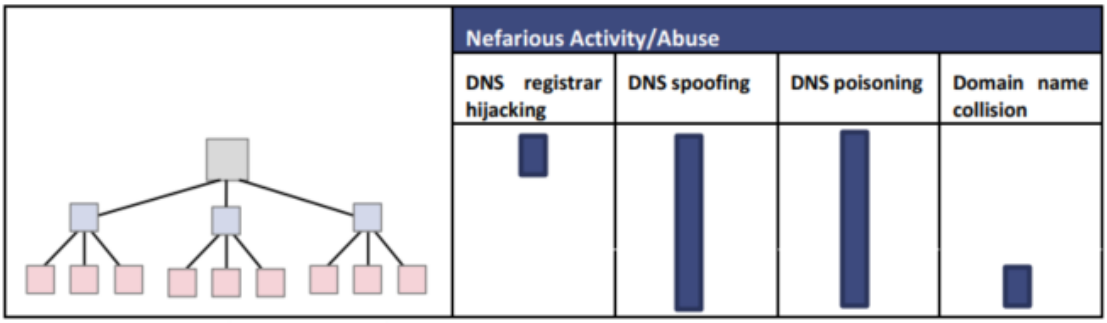
Η αεροπειρατεία της συνόδου BGP υποδηλώνει μια μεταβολή του περιεχομένου του πίνακα δρομολόγησης BGP από μια κακόβουλη συσκευή, η οποία μπορεί, μεταξύ άλλων επιπτώσεων, να εμποδίσει την κυκλοφορία να φτάσει στον προορισμό χωρίς να λάβει γνώση ή ειδοποίηση.

Παράδειγμα:

- Κλοπή συνόδου μικρού βίου BGP
- *Μέτρηση και ανάλυση της επίδρασης της επίθεσης κατά της BGP Session Hijack*

4.2.2. Απειλές DNS

Το σύστημα **DNS** εκτίθεται σε απειλές που αποσκοπούν στην αποδυνάμωση ενός κεντρικού χαρακτηριστικού, το οποίο επιτρέπει βολική περιήγηση στο web για μη τεχνικούς χρήστες και επιτρέπει ευέλικτη διεύθυνση για αυτοματοποιημένα συστήματα. Χωρίς την επίλυση ονομάτων τομέα σε διευθύνσεις IP, το Internet είναι απρόσιτο για το ευρύ κοινό. Οι επιθέσεις προσπαθούν να αλλάξουν τα αρχεία DNS για να ανακατευθύνουν την κίνηση, να διακόψουν τη λειτουργία ή να εισαγάγουν λογοκρισία. Οι τελευταίες τάσεις δείχνουν μείωση για αυτό το είδος απειλής. Ωστόσο, αυτό δεν μειώνει τη σημασία του.



Πίνακας 2 - Εφαρμογή σημαντικής συγκεκριμένης απειλής στο DNS

Ο Πίνακας 2 υπογραμμίζει την εφαρμογή σημαντικών ειδικών απειλών στην υποδομή DNS. Η υποδομή DNS αντιπροσωπεύεται από ένα αφηρημένο (απλοποιημένο) δέντρο, το οποίο δείχνει έναν συνδυασμό αρκετών τυπικών στρωμάτων. Η έκταση μιας απειλής αντιπροσωπεύεται από μια έγχρωμη ράβδο, η οποία υποδηλώνει τον τρόπο με τον οποίο η απειλή ισχύει για τα στρώματα που απεικονίζονται στο αριστερό πλάνο. Σημαντικές συγκεκριμένες απειλές για το DNS ισχύουν σε διαφορετικές εκτάσεις για την Υποδομή Διαδικτύου.

Αυτές οι σημαντικές ειδικές απειλές είναι τώρα λεπτομερείς και παρουσιάζονται οι τάσεις τους.

Τύπος απειλής: Δραστική δραστηριότητα / Κατάχρηση

Τάση: Μείωση

Απειλή: DNS registrar hijacking

Εάν ένας καταχωρητής DNS έχει πειραματιστεί, όλα τα πεδία υπό τον έλεγχό του διακυβεύονται: οι πληροφορίες εγγραφής τομέα μπορούν να τροποποιηθούν, πράγμα που μπορεί να οδηγήσει σε μεταφορά του τομέα σε άλλο καταχωρητή ή να οδηγήσει σε κλοπή ταυτότητας. Μόλις γίνει αυτό, ο αεροπειρατής έχει τον πλήρη έλεγχο όλων των τομέων και μπορεί να τα χρησιμοποιήσει ή να τα πουλήσει σε τρίτους.

Παράδειγμα:

- Ο δημοφιλής καταχωρητής Namecheap διορθώνει το σφάλμα DNS

Απειλή: υποκλοπή DNS

Η υποκλοπή DNS αναφέρεται στην ευρεία κατηγορία επιθέσεων που καταγράφουν τα αρχεία DNS. Υπάρχουν πολλοί διαφορετικοί τρόποι για να κάνετε το spoofing του DNS: να συμβιβαστείτε με έναν διακομιστή DNS, να συνδέσετε μια επίθεση δηλητηρίασης DNS cache, να βάλετε μια επίθεση στον άνθρωπο στη μέση, να μαντέψετε έναν αριθμό ακολουθίας και πολλά άλλα.

Παράδειγμα:

- Υποβιβασμός του αλγόριθμου SRTT του BIND για αποδιαμόρφωση της επιλογής NS

Απειλή: δηλητηρίαση DNS

Η δηλητηρίαση DNS (cache) είναι μια τεχνική επίθεσης που επιτρέπει σε έναν εισβολέα να εισάγει πλαστές πληροφορίες DNS στην κρυφή μνήμη ενός διακομιστή ονομάτων χώρου αποθήκευσης cache. Υπάρχουν δημοσιευμένα άρθρα που περιγράφουν έναν αριθμό εγγενών ελλείψεων στο πρωτόκολλο DNS και ελαττώματα στις κοινές υλοποιήσεις DNS που διευκολύνουν τη δηλητηρίαση DNS cache.

Παραδείγματα:

- Κατάχρηση μηχανισμών αντι-DDoS για την εκτέλεση δηλητηρίασης DNS cache
- Ο κατακερματισμός θεωρείται δηλητηριώδης

Απειλή: Σύγκρουση ονόματος τομέα

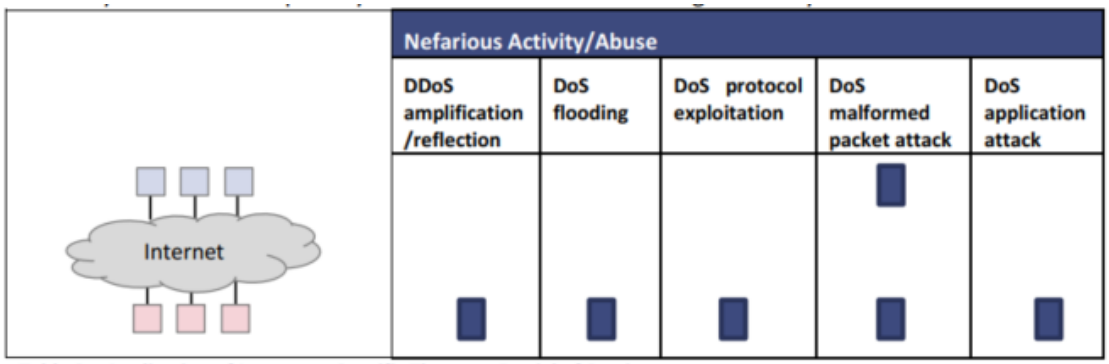
Μια σύγκρουση ονομάτων αναφέρεται σε μια προσπάθεια επίλυσης ενός ονόματος που χρησιμοποιείται σε ένα ιδιωτικό χώρο ονομάτων (π.χ. μη εξουσιοδοτημένος τομέας ανωτάτου επιπέδου ή σύντομο όνομα), με αποτέλεσμα ένα ερώτημα DNS στο δημόσιο DNS και ένα όνομα που ταιριάζει μπορεί να ανακτηθεί. Στις περισσότερες περιπτώσεις, η αιτία είναι μια κακή διαμόρφωση και αγνοεί τις συστάσεις του ICANN. Τα συμβάντα σύγκρουσης ονομάτων δεν είναι καινούργια και έχουν ιστορικά παρατηρηθεί και αναφερθεί ως ερωτήματα που περιέχουν μη εξουσιοδοτημένα TLD στο επίπεδο ρίζας του DNS. Έχουν λάβει νέα προσοχή επειδή πολλοί υπέβαλαν αίτηση για νέες σειρές TLD που είναι ταυτόσημες με τις ετικέτες χώρου ονομάτων που χρησιμοποιούνται σε ιδιωτικά δίκτυα.

Παραδείγματα:

- Κοιτάζοντας στο corp.com ως πληρεξούσιο για το .corp
- Έχουν δημοσιευθεί αναφορές για εναλλακτική πορεία προς την εξουσιοδότηση

4.2.3. Άρνηση παροχής υπηρεσίας (DoS / Distributed DoS (DDoS)) Απειλές

Οι επιθέσεις άρνησης παροχής υπηρεσιών προσπαθούν να καταστήσουν ένα μηχανογραφικό σύστημα ή δίκτυο μη διαθέσιμο στους χρήστες τους. Βασικά, κάθε σύστημα μπορεί να στοχεύεται από το DoS που κυμαίνεται από έναν απλό οικιακό υπολογιστή σε ένα σημαντικό αγρόκτημα διακομιστή ιστού. Υπάρχουν πολλές διαφορετικές προσεγγίσεις που ενισχύουν την ένταση μιας επίθεσης. Ιδιαίτερα αυτό το είδος επίθεσης αυξάνεται αυτές τις μέρες.



Πίνακας 3 - Εφαρμογή σημαντικής συγκεκριμένης απειλής στην άρνηση παροχής υπηρεσίας

Ο Πίνακας 3 υπογραμμίζει την εφαρμογή σημαντικών συγκεκριμένων απειλών σχετικά με την άρνηση παροχής υπηρεσιών. Η αρχιτεκτονική του Διαδικτύου που παρουσιάζεται στην εικόνα απλοποιείται και αφαιρείται για να δείξει τα σημαντικά μέρη σε σχέση με το DoS. Η έκταση μιας απειλής αντιπροσωπεύεται από μια έγχρωμη ράβδο, η οποία υποδηλώνει τον τρόπο με τον οποίο η απειλή ισχύει για τα στρώματα που απεικονίζονται στο αριστερό πλάνο. Σημαντικές συγκεκριμένες απειλές για το DoS ισχύουν σε διαφορετική έκταση για την υποδομή του Διαδικτύου.

Αυτές οι σημαντικές ειδικές απειλές είναι τώρα λεπτομερείς και παρουσιάζονται οι τάσεις τους.

Τύπος απειλής: Φανερή Δραστηριότητα / Κατάχρηση

Τάση: Αύξηση

Απειλή: ενίσχυση / αντανάκλαση DDoS

Σε μια επίθεση DDoS αντανάκλασης, ο επιτιθέμενος παραβιάζει τη διεύθυνση IP του θύματος και στέλνει αίτημα για πληροφορίες μέσω του UDP σε διακομιστές που είναι γνωστοί ότι ανταποκρίνονται σε αυτόν τον τύπο αίτησης. Οι διακομιστές απαντούν στο αίτημα και στέλνουν την απάντηση στη διεύθυνση IP του θύματος. Όλα τα δεδομένα από αυτούς τους διακομιστές προσθέτουν ένα σημαντικό εύρος ζώνης, αρκετό για να συγκλίνει η σύνδεση στο Internet του στόχου. Με το μέγιστο εύρος ζώνης, η κανονική κυκλοφορία δεν μπορεί να εξυπηρετηθεί και οι νόμιμοι πελάτες δεν μπορούν να συνδεθούν.

Παραδείγματα:

- Οι τεχνικές λεπτομέρειες πίσω από μια επίθεση DDoS ενίσχυσης NTP 400 Gbps
- Βαθιά μέσα σε μια επίθεση DDoS ενίσχυσης DNS
- Το DDoS που χτύπησε το Spamhaus εκτός σύνδεσης (και πώς το μετριάσαμε)

Απειλή: πλημμύρες DoS

Μια πλημμύρα είναι μια απλή επίθεση άρνησης εξυπηρέτησης όπου ο επιτιθέμενος συντρίβει το θύμα με πακέτα (π.χ. πακέτα ping ICMP). Είναι πιο επιτυχημένη αν ο εισβολέας έχει μεγαλύτερο εύρος ζώνης από το θύμα (για παράδειγμα, ένας εισβολέας με γραμμή DSL και το θύμα σε ένα τηλεφωνικό μόντεμ). Ο επιτιθέμενος μπορεί να ελπίζει ότι το θύμα θα ανταποκριθεί στα πακέτα του (π.χ. ICMP echo reply packets), καταναλώνοντας έτσι τόσο το εξερχόμενο εύρος ζώνης όσο και το εισερχόμενο εύρος ζώνης.

Παραδείγματα:

- Χαμηλή Orbit Ion Canon
- Ανώνυμος δηλώνει τον πόλεμο στον κυβερνοχώρο στο Ισραήλ, την περιοχή Downs Mossad, πολλούς άλλους

Απειλή: εκμετάλλευση πρωτοκόλλου DoS

Η χρήση πρωτοκόλλου (π.χ. TCP-SYN) είναι μια μορφή επίθεσης άρνησης εξυπηρέτησης στην οποία ένας εισβολέας στέλνει μια σειρά αιτημάτων σε ένα σύστημα στόχου σε μια προσπάθεια να καταναλώσει αρκετούς πόρους διακομιστή (π.χ. θύρες TCP) για να μην ανταποκρίνεται στο σύστημα νόμιμη κυκλοφορία.

Παραδείγματα:

- Οι επιθέσεις DDoS που εκμεταλλεύονται ευπάθεια στο πρωτόκολλο χρόνου δικτύου, καλέστε το γιατρό
- Η επίθεση Sloworis DoS, γνωστή και ως "αργή και χαμηλή"

Απειλή: DoS εσφαλμένη επίθεση πακέτων

Επιθέσεις που σχεδιάστηκαν για τη συντριβή της στοίβας δικτύου του λειτουργικού συστήματος, παρέχοντας ανεπαρκή πληροφορίες κεφαλίδας ή ωφέλιμο φορτίο.

Παραδείγματα:

- Μαζική επίθεση 300 Gbps DDoS στην εταιρία μέσων μαζικής ενημέρωσης που τροφοδοτείται από ανεπιθύμητη αδυναμία διακομιστή
- Το θέμα ευπάθειας στο ICMPv6 θα μπορούσε να επιτρέψει την άρνηση παροχής υπηρεσίας

Απειλή: επίθεση εφαρμογής DoS

Γνωστοί περιορισμοί λογικής εφαρμογής, ατέλειες και ευπάθειες εκμεταλλεύονται, με αποτέλεσμα μια συγκεκριμένη αποτυχία εφαρμογής ή καταστροφή δεδομένων.

Παραδείγματα:

- Η Gartner αναφέρει ότι το 25% των κατανεμημένων επιθέσεων άρνησης παροχής υπηρεσιών το 2013 θα βασίζεται σε εφαρμογές
- Η επίθεση DDoS χρησιμοποίησε προγράμματα περιήγησης «χωρίς κεφάλια» σε πολιορκία 150 ωρών

4.2.4. Γενικές απειλές

Όλες οι απειλές που αναφέρονται στην κατηγορία γενικών απειλών ισχύουν για όλα τα συστήματα ηλεκτρονικών υπολογιστών εν γένει, και συνεπώς για συστήματα της υποδομής Διαδικτύου. Πρόκειται για μια περίληψη των σημαντικών απειλών παρά μιας πλήρους λίστας και πρέπει να ευαισθητοποιήσει ότι ακόμη και πολύ κοινές επιθέσεις μπορεί να βλάψουν την υποδομή του Διαδικτύου.

Τύπος απειλής: Φυσική επίθεση

Τάση: Δεν είναι διαθέσιμο

Μια φυσική επίθεση μπορεί να αποτελέσει απειλή για έναν οργανισμό, ορισμένες περιοχές του οργανισμού ή άτομα. Οι τεχνικές δυνατότητες διάπραξης μιας επίθεσης είναι πολλές: ρίψη τούβλων, εκρήξεις από εκρηκτικά, χρήση πυροβόλων όπλων ή εμπρησμοί.

Τύπος απειλής: ζημιές

Τάση: Αύξηση

Κάθε περιστατικό όπου α) ένα περιουσιακό στοιχείο (π.χ. καλώδιο θαλάσσης, συσκευή, πληροφορίες) έχει υποστεί βλάβη τυχαία ή κακόπιστα ή β) λείπει ένα περιουσιακό στοιχείο (π.χ. μέσα αποθήκευσης, έγγραφα), είτε λόγω κακής τοποθέτησης είτε λόγω κακής χρήσης.

Τύπος απειλής: Αποτυχίες / Δυσλειτουργίες

Τάση: Αύξηση

Απειλή: Αποτυχία συσκευών ή συστημάτων

Λόγω των εξαρτήσεων της τεχνικής υποδομής, οι μεμονωμένες βλάβες μεμονωμένων εξαρτημάτων, όπως οι εγκαταστάσεις κλιματισμού ή τροφοδοσίας, μπορεί να συμβάλλουν στην αποτυχία μιας συσκευής ή ακόμα και ολόκληρου του συστήματος. Συγκεκριμένα, βασικά στοιχεία ενός συστήματος ΤΠ (για παράδειγμα, διακομιστές και στοιχεία σύζευξης δικτύου) είναι πιθανό να προκαλέσουν τέτοιες αποτυχίες.

Απειλή: Σφάλματα διαμόρφωσης

Οι επιθέσεις σφάλματος διαμόρφωσης εκμεταλλεύονται τις αδυναμίες διαμόρφωσης που εντοπίζονται στο λογισμικό. Το λογισμικό μπορεί να έρθει με περιττές και μη ασφαλείς λειτουργίες, όπως οι δυνατότητες εντοπισμού σφαλμάτων και QA, ενεργοποιημένες από προεπιλογή. Αυτά τα χαρακτηριστικά μπορεί να παρέχουν ένα μέσο για έναν εισβολέα να παρακάμπτει τις μεθόδους ελέγχου ταυτότητας και να αποκτά πρόσβαση σε ευαίσθητες πληροφορίες, ίσως με αυξημένα προνόμια. Ομοίως, οι προεπιλεγμένες εγκαταστάσεις ενδέχεται να περιλαμβάνουν πολύ γνωστά ονόματα χρήστη και κωδικούς πρόσβασης, σκληρούς κωδικούς λογαριασμούς backdoor, μηχανισμούς ειδικής πρόσβασης και εσφαλμένα δικαιώματα που έχουν οριστεί για αρχεία που είναι προσβάσιμα μέσω διακομιστών ιστού. Τα προεπιλεγμένα δείγματα μπορεί να είναι προσβάσιμα σε περιβάλλοντα παραγωγής. Τα αρχεία διαμόρφωσης που δεν είναι σωστά κλειδωμένα ενδέχεται να αποκαλύπτουν συμβολοσειρές με σαφή σύνδεση κειμένου στη βάση δεδομένων και οι προεπιλεγμένες ρυθμίσεις στα αρχεία ρυθμίσεων ενδέχεται να μην έχουν ρυθμιστεί με γνώμονα την ασφάλεια.Όλες αυτές οι εσφαλμένες ρυθμίσεις μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες.

Τύπος απειλής: Αφηρημένη δραστηριότητα / Κατάχρηση

Τάση: Αύξηση

Απειλή: Malware και ιούς

Το κακόβουλο λογισμικό, συντομογραφία για κακόβουλο λογισμικό, είναι ένας γενικός όρος για οποιοδήποτε πρόγραμμα με σκοπό να διαταράξει τη λειτουργία του υπολογιστή, να συλλέξει ευαίσθητες πληροφορίες ή να αποκτήσει πρόσβαση σε ιδιωτικά συστήματα υπολογιστών. Περιλαμβάνει, μεταξύ άλλων, ιούς, σκουλήκια, trojans, rootkits, botnets, spyware, scareware ή rogueware.

Απειλή: Brute force

Οι επιθέσεις βίαιης δύναμης χρησιμοποιούνται συχνά για την αποτροπή ενός κρυπτογραφικού σχεδίου, όπως αυτές που εξασφαλίζονται με κωδικούς πρόσβασης. Οι χάκερ χρησιμοποιούν προγράμματα υπολογιστών για να δοκιμάσουν έναν πολύ μεγάλο αριθμό κωδικών πρόσβασης για να αποκρυπτογραφήσουν το μήνυμα ή να αποκτήσουν πρόσβαση στο σύστημα.

Απειλή: Κοινωνική μηχανική

Η κοινωνική μηχανική είναι ο ψυχολογικός χειρισμός της ανθρώπινης συμπεριφοράς για την παραβίαση της ασφάλειας, χωρίς οι συμμετέχοντες (ή τα θύματα) να συνειδητοποιούν ότι έχουν χειραγωγηθεί. Υπάρχουν δύο βασικές κατηγορίες στις οποίες θα μπορούσαν να ταξινομηθούν όλες οι προσπάθειες κοινωνικής μηχανικής - η εξαπάτηση που βασίζεται σε υπολογιστή ή τεχνολογία και η εξαπάτηση με βάση τον άνθρωπο. Η προσέγγιση που βασίζεται στην τεχνολογία είναι να εξαπατήσει τον χρήστη να πιστέψει ότι αλληλοεπιδρά με το «πραγματικό» σύστημα ηλεκτρονικών υπολογιστών και να τον πάρει για να παρέχει εμπιστευτικές πληροφορίες. Η ανθρώπινη προσέγγιση γίνεται με εξαπάτηση, εκμεταλλευόμενος την άγνοια του θύματος και τη φυσική ανθρώπινη διάθεση να είναι χρήσιμη και άρεσε.

Απειλή: Παραβίαση δεδομένων

Μια παραβίαση δεδομένων αναφέρεται στην εξάτμιση δεδομένων από ένα σύστημα χωρίς τη γνώση ή τη συναίνεση του ιδιοκτήτη του. Αυτά τα δεδομένα βρίσκονται στα συστήματα ή τα δίκτυα του στοχευμένου οργανισμού και είναι ιδιοκτησιακά ή ευαίσθητα. Τα στοιχεία ιδιοκτησίας μπορεί να είναι πολύτιμα ή εμπιστευτικά σε έναν οργανισμό. Η απόκτηση από εξωτερικά μέρη μπορεί να προκαλέσει βλάβη. Αυτά τα δεδομένα μπορούν να περιλαμβάνουν προσωπικά αναγνωρίσιμες πληροφορίες, δεδομένα πελατών, εμπορικά μυστικά και τα παρόμοια.

Τύπος απειλής: Υποκλοπή / Παρακολούθηση

Τάση της πειρατείας : Αύξηση

Απειλή: Κατασκοπεία

Η κατασκοπεία είναι μια διαδικασία που περιλαμβάνει ανθρώπινες πηγές ή τεχνικά μέσα για τη λήψη πληροφοριών που κανονικά δεν είναι διαθέσιμες στο κοινό.

4.3. Περίληψη των τάσεων των απειλών

Αυτή η ενότητα συνοψίζει τις τάσεις για κάθε τύπο απειλής που παρουσιάστηκε στην προηγούμενη ενότητα. Η γενική τάση υποδηλώνει αύξηση για την πλειονότητα των απειλών, όπως παρουσιάζεται στον Πίνακα 4 .

Ωστόσο, αυτό το αποτέλεσμα θα μετριαστεί για ορισμένους σημαντικούς ειδικούς κινδύνους από τον πραγματικό αριθμό επιθέσεων που χρησιμοποιούν αυτή την απειλή. Μια αυξανόμενη τάση υποδηλώνει μεγαλύτερο αριθμό εμφανίσεων φέτος σε σύγκριση με το προηγούμενο έτος, παρόλο που ο αριθμός των επιθέσεων μπορεί να είναι χαμηλός. Μια αυξανόμενη τάση για αυτή τη συλλογή απειλών θα πρέπει να αποτελέσει κίνητρο για την παρακολούθηση πιθανών επιθέσεων στο μέλλον.

Από την άλλη πλευρά, μια πτωτική τάση για Σημαντική Ειδική Απειλή δεν μειώνει τη σημασία αυτής της απειλής. Στον πίνακα, η απειλή DNS μειώνεται. Ωστόσο, ο αριθμός των επιθέσεων στον κυβερνοχώρο που στοχεύουν το DNS παραμένει σημαντικός σε σχέση με τον συνολικό αριθμό των επιθέσεων. Αυτή η πτωτική τάση θα υποδηλώνει μόνο μια μείωση του DNS ως διάνυσμα επίθεσης από παράγοντες απειλής.

Ομάδες απειλών	Τύποι απειλών	Τάσεις
Απειλές δρομολόγησης	Εξαφανής Δραστηριότητα / Κατάχρηση	Αύξηση ⇑
	Υποκλοπή / Παρακολούθηση / αεροπειρατεία	Αύξηση ⇑
Απειλές DNS	Εξαφανής Δραστηριότητα / Κατάχρηση	Μείωση ⇒
Άρνηση παροχής υπηρεσίας	Εξαφανής Δραστηριότητα / Κατάχρηση	Αύξηση ⇑
Γενικές απειλές	Φυσική επίθεση	N / A
	Ζημιά / Απώλεια	Αύξηση ⇑
	Βλάβες / Βλάβες	Αύξηση ⇑
	Αφηρημένη δραστηριότητα / Κατάχρηση	Αύξηση ⇑
	Υποκλοπή / Παρακολούθηση / αεροπειρατεία	Αύξηση ⇑

Πίνακας 4 - Περίληψη τάσεων ανά τύπο απειλής για κάθε ομάδα απειλών

5. Περιουσιακά στοιχεία υποδομής διαδικτύου Έκθεση σε απειλές του κυβερνοχώρου

Σε αυτή την ενότητα παρουσιάζεται η απειλή έκθεσης της υποδομής Internet. Η συσχέτιση μεταξύ των περιουσιακών στοιχείων από το Σχήμα 3 και των απειλών από το Σχήμα 4 καθορίζεται για κάθε τύπο απειλής. Ένας ενδιαφερόμενος αναγνώστης μπορεί να εντοπίσει σχετικές απειλές με βάση τα αναπτυγμένα περιουσιακά του στοιχεία. Ο Πίνακας 5 αντιστοιχεί σε μια σειρά συγκεκριμένων απειλών με τους εμπλεκόμενους τύπους περιουσιακών στοιχείων. Το παράρτημα Δ προτείνει έναν πιο εξαντλητικό κατάλογο των απειλών και των σχετικών περιουσιακών τους στοιχείων.

Οι πληροφορίες που απεικονίζονται στον πίνακα είναι διατεταγμένες ως εξής:

- **Τύποι απειλών** : Στη στήλη αυτή αναφέρονται οι τύποι απειλών.
- **Απειλές** : Αυτό το πεδίο περιέχει πιο λεπτομερείς απειλές που ανήκουν στους διαφορετικούς τύπους απειλών.
- **Τύποι περιουσιακών στοιχείων** : Αυτό το πεδίο καθορίζεται από τους τύπους περιουσιακών στοιχείων που εμφανίζονται στους τύπους απειλών και απειλών.

Τύποι απειλών	Απειλές	Τύποι περιουσιακών στοιχείων
Φυσικές επιθέσεις		
	Σαμποτάζ	Υλικό, Υποδομή
	Μη εξουσιοδοτημένη φυσική πρόσβαση / μη εξουσιοδοτημένες καταχωρήσεις σε χώρους	Υλικό, Υποδομή
Καταστροφές		
	Φυσικές καταστροφές	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες, Διασύνδεση, Υποδομές, Ανθρώπινοι πόροι
	Περιβαλλοντικές καταστροφές	*Ομοια*
Βλάβες / Βλάβες		
	Αποτυχίες μερών συσκευών	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Σφάλματα διαμόρφωσης	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες

Διακοπές		
	Ελλειψη πηγών	Hardware, Λογισμικό, Πληροφορίες, Υπηρεσίες, Διασύνδεση, Υποδομή, Ανθρώπινο πόροι
	Διακοπές δικτύου	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες
Αθέλητες ζημιές (τυχαίες)		
	Διαρροή πληροφοριών / κοινή χρήση	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες, διασύνδεση
	Μη ακούσια αλλαγή δεδομένων σε ένα σύστημα πληροφοριών	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
Ζημιές / Απώλειες (στοιχεία ενεργητικού)		
	Ζημία που προκλήθηκε από τρίτους	Hardware, Λογισμικό, Πληροφορίες, Υπηρεσίες, Διασύνδεση, Υποδομή, Ανθρώπινο πόροι
	Απώλεια φήμης	Διασύνδεση, Ανθρώπινοι πόροι
Αφηρημένη δραστηριότητα / Κατάχρηση		
	Χειρισμός υλικού και λογισμικού	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Επιθέσεις άρνησης εξυπηρέτησης (DoS / DDoS)	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες
Υποκλοπή / Παρακολούθηση / αεροπειρατεία		
	Υποκλοπή συμβιβασμού εκπομπών	Πρωτόκολλα, λογισμικό, πληροφορίες, υπηρεσίες

	Άνθρωπος στη μεσολάβηση / απόπειρα αεροπειρατεία	Λογισμικό, πληροφορίες, υπηρεσίες
Νομικός		
	Παραβιάσεις νόμων ή κανονιστικών ρυθμίσεων / παραβιάσεις της νομοθεσίας	Λογισμικό, Πληροφορίες, Διασύνδεση, Ανθρώπινοι πόροι
	Μη τήρηση των συμβατικών απαιτήσεων	*Ομοια*

Πίνακας 5 - Σύνδεση μεταξύ απειλών και περιουσιακών στοιχείων (απόσπασμα, βλέπε παράρτημα Δ για τον εξαντλητικό κατάλογο)

6. Απειλείς πράκτορες

Σύμφωνα με το ENISA Threat Landscape 2013 , ένας παράγοντας απειλής είναι *"κάποιος ή κάτι με αξιοπρεπείς δυνατότητες, μια σαφής πρόθεση να εκδηλώσει απειλή και ένα ιστορικό παλαιών δραστηριοτήτων από αυτή την άποψη"* . Για άλλη μια φορά, η μελέτη αυτή δίνει μόνο μια γενική επισκόπηση λόγω της έλλειψης συγκεκριμένης εφαρμογής. Για τους ιδιοκτήτες περιουσιακών στοιχείων υποδομής του Διαδικτύου, είναι σημαντικό να γνωρίζετε ποιες απειλές προκύπτουν από την ομάδα των απειλητικών παραγόντων. Ο πίνακας 6 παρουσιάζει μια τέτοια επισκόπηση.

Ωστόσο, αυτή η μελέτη δεν αναπτύσσει νέο γλωσσάριο για τους παράγοντες απειλής στο πλαίσιο του IITL, αλλά μάλλον χρησιμοποιεί την ενοποίηση αρκετών δημοσιεύσεων του ENISA Threat Landscape 2013. Οι ενδιαφερόμενοι αναγνώστες μπορούν να βρουν μια λεπτομερή περιγραφή στο τοπίο απειλής του ENISA 2013 . Η ταξινόμηση των παραγόντων απειλής έχει ως εξής:

- *Εταιρείες*
- *Hacktivists*
- *Ηλεκτρονικοί εγκληματίες*
- *Κυβερνητικοί τρομοκράτες*
- *Script kiddies*
- *Online κοινωνικοί χάκερ*
- *Υπαλλήλους*
- *Κράτη μέλη*

Με βάση τους παράγοντες απειλής, οι απειλές αποδίδονται σε σχετικούς τύπους απειλών (βλ. Πίνακα 6). Λεπτομερής επισκόπηση που καλύπτει όχι μόνο τους τύπους απειλών περιλαμβάνεται στο παράρτημα Ε .

	Εταιρείες	Hacktivists	Ηλεκτρονικοί εγκληματίες	Κυβερνητικοί τρομοκράτες	Script kiddies	Online κοινωνικοί χάκερ	Υπαλλήλους	Τα εθνικά κράτη
Φυσικές επιθέσεις	√	-	√	√	-	-	√	√
Καταστροφές	N / A	N / A	N / A	N / A	N / A	N / A	N / A	N / A
Βλάβες / Βλάβες	√	-	-	-	-	-	√	-
Διακοπές	√	√	√	√	√	√	√	√

Αθέλητες ζημιές	√	-	-	-	-	-	√	-
Ζημιά / Απώλεια	√	√	√	√	√	√	√	√
Αφηρημένη δραστηριότητα / Κατάχρηση	√	√	√	√	√	√	√	√
Υποκλοπή / Υποκλοπή / αεροπειρατεία	√	√	√	√	√	√	√	√
Νομικός	√	√	√	√	√	√	√	√

Πίνακας 6 - Συμμετοχή παραγόντων απειλής σε απειλές

7. Καλές πρακτικές

Αυτό το τμήμα καταγράφει τα διαθέσιμα στο κοινό μέτρα ασφάλειας για την προστασία των περιουσιακών στοιχείων της υποδομής του Διαδικτύου και ως εκ τούτου υποστηρίζει την ανθεκτικότητα του οικοσυστήματος του Διαδικτύου. Συνεπώς, εξετάζονται, συνοψίζονται και χαρτογραφούνται διαφορετικές πηγές με συστάσεις και ορθές πρακτικές που δημοσιεύονται από σημαντικά ινστιτούτα ή ομάδες εργασίας του Internet όπως το ICANN, το IETF, το RIPE, το Euro-IX και η κοινωνία του Διαδικτύου στις αντίστοιχες σημαντικές συγκεκριμένες απειλές. Αυτό το εργαλείο επιτρέπει στους ιδιοκτήτες περιουσιακών στοιχείων να αναλύουν προσεκτικά την υποδομή τους και να υιοθετούν κατάλληλες ορθές πρακτικές. Ολόκληρος ο κατάλογος που περιλαμβάνει όλες τις αναφορές μπορεί να βρεθεί στο παράρτημα ΣΤ.

Μια κεντρική αρχή σχεδιασμού του Διαδικτύου, ως συλλογή δικτύων, αποτελεί κοινή ευθύνη. Κάθε συμμετέχων θα πρέπει να συνειδητοποιήσει ότι η δική του ασφάλεια εξαρτάται επίσης από την ασφάλεια των γειτονικών δικτύων. Ως εκ τούτου, είναι συλλογική ευθύνη να εφαρμόζουν ορθές πρακτικές όταν θεωρούνται χρήσιμες για τη δική τους ασφάλεια και για την ασφάλεια των άλλων μερών, όταν ισχύει. Ένα παράδειγμα είναι ανεπαρκώς διαμορφωμένοι διακομιστές DNS ή NTP που χρησιμοποιούνται από τους αντιπάλους για την ενίσχυση των επιθέσεων DDoS.

Ο Πίνακας 7 περιέχει τις αναγνωρισμένες ορθές πρακτικές και παρέχει περισσότερες λεπτομέρειες σχετικά με την ανάλυση των κενών. Δεν παρουσιάζει καλές πρακτικές για τις "γενικές απειλές" οι οποίες, όπως υποδηλώνει το όνομά τους, είναι υπερβολικά γενικές ώστε να αντιμετωπίζονται με συγκεκριμένες ορθές πρακτικές. Ο πίνακας είναι δομημένος ως εξής:

- **Σημαντικές συγκεκριμένες ομάδες απειλών:** Μια γραμμή με γκρίζο φόντο που περιέχει τις σημαντικές ειδικές ομάδες απειλών που ορίζονται στην ενότητα 4.2.

- **Απειλές:** Ακολουθούν οι συγκεκριμένες απειλές, ομαδοποιημένες σύμφωνα με την προηγούμενη στήλη, οι οποίες υποδηλώνουν τις πραγματικές απειλές που πρέπει να αντιμετωπιστούν εφαρμόζοντας τις ορθές πρακτικές.

- **Καλές πρακτικές:** Οι πραγματικές ορθές πρακτικές για την απειλή στην ίδια σειρά. Η περιγραφή είναι μια περίληψη των διαφόρων πηγών που αναφέρονται στο παράρτημα ΣΤ .

- **Περιουσιακά στοιχεία, περιουσιακά στοιχεία που καλύπτονται:** Όλα τα στοιχεία ενεργητικού που σχετίζονται με μια σημαντική ομάδα ειδικών απειλών εκτυπώνονται με μαύρο χρώμα Στις σειρές των συγκεκριμένων απειλών, όλα τα περιουσιακά στοιχεία που καλύπτονται από ένα τουλάχιστον μέτρο εκτυπώνονται με πράσινο χρώμα.

- **Κενό (περιουσιακά στοιχεία που δεν καλύπτονται):** Αυτή η στήλη περιέχει τα περιουσιακά στοιχεία που σχετίζονται με μια απειλή που δεν καλύπτονται από τη σχετική ορθή πρακτική, τυπωμένη με μαύρο χρώμα. Εάν

ένα περιουσιακό στοιχείο δεν καλύπτεται από τουλάχιστον μία καλή πρακτική εντός της διακεκριμένης ομάδας απειλών, το στοιχείο αυτό τυπώνεται με κόκκινο χρώμα για να το επισημάνει ως κενό για τον τύπο απειλής.

Απειλές	Καλές πρακτικές	Περιουσιακά στοιχεία, καλύπτονται στοιχεία ενεργητικού	Κενά (περιουσιακά στοιχεία που δεν καλύπτονται)
Απειλές δρομολόγησης			
Ως αεροπειρατεία		Διεύθυνση πρωτοκόλλου Internet, Πρωτόκολλα δρομολόγησης, Διαχειριστές	Διαχειριστές
	Χρησιμοποιήστε την πιστοποίηση πόρων (RPKI) για την επικύρωση της προέλευσης AS. Ο αναγνώστης πρέπει να γνωρίζει ότι στο τη στιγμή της γραφής, δεν είναι δυνατό να ανιχνεύσουμε αυτόματα την πειρατεία AS.	Διεύθυνση πρωτοκόλλου Internet, Πρωτόκολλα δρομολόγησης	Διαχειριστές
Διέλευση χώρου διευθύνσεων (προθέματα IP)		Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	-
	Χρησιμοποιήστε την πιστοποίηση πόρων (RPKI) για την επικύρωση της προέλευσης AS.	Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	
	Καθορίστε μια πολιτική κατάλληλης χρήσης (AUP) όπως εξηγείται στο BCP 46, το οποίο προωθεί τους κανόνες που πρέπει να τηρούνται peering.	Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	
	Καθιέρωση φίλτρου εισόδου από την περιοχή	Δρομολόγηση, διευθυνσιοδότηση	Ρυθμίσεις συστήματος,

	άκρη στο Internet.	πρωτοκόλλου Διαδικτύου	Τοπολογία δικτύου
	Καθιέρωση προώθησης Unicast Reverse Path για επιβεβαίωση της εγκυρότητας μιας διεύθυνσης IP προέλευσης.	Δρομολόγηση, διαμόρφωση συστήματος, τοπολογία δικτύου	Διεύθυνση πρωτοκόλλου Internet
	Δημιουργήστε φιλτράρισμα εξόδου στο οριακό δρομολογητή για να φιλτράρετε προορατικά όλη την κίνηση που πηγαίνει στον πελάτη που έχει διεύθυνση προέλευσης οποιασδήποτε από τις διευθύνσεις που έχουν εκχωρηθεί σε αυτό πελάτης.	Δρομολόγηση, διευθυνσιοδότηση πρωτοκόλλου Διαδικτύου	Ρυθμίσεις συστήματος, Τοπολογία δικτύου
	Φιλτράρετε τις ανακοινώσεις δρομολόγησης και εφαρμόστε τεχνικές που μειώνουν τον κίνδυνο υπερβολικής φόρτωσης στη δρομολόγηση που παράγεται από παράνομες ενημερώσεις / ανακοινώσεις διαδρομών. Για παράδειγμα, η απόσβεση των λασπών διαδρομής (RFD) με ένα καλά καθορισμένο κατώφλι μπορεί να συμβάλει στη μείωση του δρομολογητή Χρόνος επεξεργασίας.	Δρομολόγηση, Τοπολογία δικτύου	Διεύθυνση πρωτοκόλλου Internet, Διαμόρφωση συστήματος
	Οι βάσεις δεδομένων μητρώου όπως IRR, APNIC, ARIN και RIPE πρέπει να υπόκεινται σε συνεχείς συντήρηση. Αυτό θα επιτρέψει τη χρήση επικαιροποιημένων	Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, διαμόρφωση συστήματος	Τοπολογία δικτύου

	πληροφοριών για την εξασφάλιση της ανταλλαγής κίνησης. Για παράδειγμα, το πεδίο "Αντικείμενο διαδρομής" μπορεί να βοηθήσει στην επικύρωση δρομολογίων που λαμβάνονται από συνομηλίκους.		
	Οι ενημερώσεις διαμόρφωσης για την υποδομή δρομολόγησης μπορούν να εκτελούνται μόνο από μια ορισμένη αρχή χρησιμοποιώντας ισχυρό έλεγχο ταυτότητας.	Δρομολόγηση, διαμόρφωση συστήματος, τοπολογία δικτύου	Διεύθυνση πρωτοκόλλου Internet
	Παρακολουθήστε την κατάσταση του BGP για να ανιχνεύσετε ασυνήθιστη συμπεριφορά, όπως αλλαγές διαδρομής ή ασυνήθιστες συμπεριφορές ανακοίνωση.	Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	
Διαρροές διαδρομής		Δρομολόγηση, Τοπολογία δικτύου	-
	Διαμορφώστε το *μέγιστο πρόθεμα* BGP *για* να διασφαλίσετε την εγκυρότητα των δρομολογίων που ανακοινώθηκαν. Εάν υπάρχουν περισσότερα προθέματα παραληφθεί, είναι σημάδι λανθασμένης συμπεριφοράς και η περίοδος BGP τερματίζεται.	Δρομολόγηση, Τοπολογία δικτύου	
	Χρησιμοποιήστε την πιστοποίηση πόρων (RPKI) για την επικύρωση της προέλευσης AS.	Δρομολόγηση, Τοπολογία δικτύου	

Απόπειρα συνόδου BGP		Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	-
	Καθιέρωση φίλτρου προθέματος και αυτοματοποίηση φίλτρων πρόθεμα.	Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	
	Χρησιμοποιήστε φιλτράρισμα μονοπατιού AS.	Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	
	Χρησιμοποιήστε το TCP-AO (επιλογή TCP-Authentication Option) για να εξασφαλίσετε τον έλεγχο ταυτότητας BGP για να αντικαταστήσετε το TCP-MD5. Το TCP-AO απλοποιεί την ανταλλαγή πλήκτρων.	Δρομολόγηση, διεύθυνση πρωτοκόλλου Internet, σύστημα διαμορφώσεις, Τοπολογία δικτύου	
Απειλές DNS			
DNS καταχωρητής αεροπειρατεία		Σύστημα ονομάτων τομέα, Διευθυνσιοδότηση μονάδων, Εφαρμογές, διαπιστευτήρια, διαχειριστές	-
	Οι καταχωρίζοντες πρέπει να προστατεύουν τα διαπιστευτήρια λογαριασμού και να ορίζουν εξουσιοδοτημένους χρήστες, ενώ οι καταχωρητές πρέπει να παρέχει μια ασφαλή διαδικασία επαλήθευσης ταυτότητας.	Αντιμετώπιση μονάδων, διαπιστευτηρίων, διαχειριστών	Σύστημα ονομάτων τομέα, Εφαρμογές
	Οι καταχωρίζοντες θα πρέπει να επωφεληθούν από την τακτική	Αντιμετώπιση μονάδων, Εφαρμογές	Σύστημα ονομάτων τομέα,

	αλληλογραφία από τον καταχωρητή, όπως αλλαγή ειδοποίηση, πληροφορίες χρέωσης ή εγγραφές WHOIS. Ως εκ τούτου, οι καταχωρητές πρέπει να παρέχουν αυτές τις πληροφορίες.		διαπιστευτήρια, Διαχειριστές
	Οι καταχωρίζοντες πρέπει να τηρούν τεκμηρίωση για να "αποδείξουν την καταχώριση"	Αντιμετώπιση μονάδων, Εφαρμογές	Σύστημα ονομάτων τομέα, διαπιστευτήρια, Διαχειριστές
	Οι καταχωρίζοντες πρέπει να χρησιμοποιούν ξεχωριστές ταυτότητες για τον καταχωρίζοντα, τις τεχνικές, τις διοικητικές και τη χρέωσηεπαφές. Έτσι, οι καταχωρητές πρέπει να επιτρέψουν μια πιο σύνθετη διαχείριση δικαιωμάτων των χρηστών.	Πιστοποιητικά, Διαχειριστές	Σύστημα ονομάτων τομέα, Διευθυνσιοδότηση μονάδων, Εφαρμογές
	Οι καταχωρητές πρέπει να καθιερώσουν αποτελεσματική διαχείριση δεδομένων ζώνης.	Σύστημα ονόματος τομέα, Διεύθυνση μονάδων, Εφαρμογές	Πιστοποιητικά, Διαχειριστές
	Οι καταχωρητές πρέπει να εξετάσουν το ενδεχόμενο υποστήριξης του DNSSEC.	Σύστημα ονόματος τομέα, Διεύθυνση μονάδων, Εφαρμογές	Πιστοποιητικά, Διαχειριστές
	Οι καταχωρητές μπορούν να παρακολουθούν τις δραστηριότητες αλλαγής DNS.	Αντιμετώπιση μονάδων, Εφαρμογές, Διαχειριστές	Σύστημα ονόματος τομέα, διαπιστευτήρια
Υποκλοπή DNS		Σύστημα ονομάτων τομέα, Διευθυνσιοδότηση μονάδων, Εφαρμογές, Ρυθμίσεις συστήματος, Βασικά πρωτόκολλα	Διαχειριστές

		διευθυνσιοδότησης - DNS, Διαχειριστές	
	Η ανάπτυξη του DNSSEC στοχεύει στην εξασφάλιση της αυθεντικότητας των δεδομένων DNS των εξυπηρετητών DNS (resolvers), της αυθεντικής άρνησης ύπαρξης και της ακεραιότητας των δεδομένων.	Σύστημα ονομάτων τομέα, διευθύνσεις μονάδων, Εφαρμογές, Διαμόρφωση Συστήματος, Βασική διεύθυνση πρωτόκολλα - DNS	Διαχειριστές
DNS δηλητηρίαση		Σύστημα ονομάτων τομέα, Διευθυνσιοδότηση μονάδων, Εφαρμογές, διαμορφώσεις συστήματος, εκτελέσιμο προγράμματα, βασικά πρωτόκολλα διευθυνσιοδότησης - DNS, διαχειριστές, χειριστές	Διαχειριστές, χειριστές
	Η ανάπτυξη του DNSSEC στοχεύει στην εξασφάλιση της ταυτότητας των DNS πελατών (resolvers) προέλευσης των δεδομένων DNS, την αυθεντική άρνηση ύπαρξης και την ακεραιότητα των δεδομένων.	Σύστημα ονομάτων τομέα, Διευθυνσιοδότηση μονάδων, Εφαρμογές, διαμορφώσεις συστήματος, εκτελέσιμα προγράμματα, πρωτόκολλα βασικής διεύθυνσης - DNS	Διαχειριστές, χειριστές
	Περιορίστε τις μεταφορές ζώνης για να μειώσετε το φορτίο σε συστήματα και δίκτυο.	Εφαρμογές, Εκτελέσιμα προγράμματα	Σύστημα ονομάτων τομέα, Διευθυνσιοδότηση μονάδων, Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης - DNS, Διαχειριστές,

			χειριστές
	Περιορίστε δυναμικές ενημερώσεις μόνο σε εξουσιοδοτημένες πηγές, για να αποφύγετε την κατάχρηση. Αυτή η κακή χρήση περιλαμβάνει η κατάχρηση ενός διακομιστή DNS ως ενισχυτή, δηλητηρίαση DNS cache ...	Αντιμετώπιση μονάδων, εφαρμογών, συστήματος διαμορφώσεις, εκτελέσιμα προγράμματα	Σύστημα ονόματος τομέα, Βασικές διευθύνσεις πρωτόκολλα - DNS, διαχειριστές, χειριστές
	Ρυθμίστε τον κύριο διακομιστή ονομάτων ως μη επαναλαμβανόμενο. Ξεχωριστοί αναδρομικοί διακομιστές ονομάτων από τον έγκυρο διακομιστή ονομάτων.	Σύστημα ονομάτων τομέα, Μονάδα διευθύνσεων, Εφαρμογές, Εκτελέσιμα προγράμματα	Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης - DNS, Διαχειριστές, χειριστές
	Να επιτρέπεται η μεταφορά DNS μέσω του TCP για την υποστήριξη μη τυποποιημένων ερωτημάτων. Επιπλέον, ενδέχεται να είναι απαραίτητο το TCP για το DNSSEC.	Αντιμετώπιση μονάδων, Εφαρμογές, Σύστημα διαμορφώσεις, εκτελέσιμα προγράμματα	Σύστημα ονόματος τομέα, Βασικές διευθύνσεις πρωτόκολλα - DNS, διαχειριστές, χειριστές
Όνομα τομέα σύγκρουση		Σύστημα ονομάτων τομέα, Εφαρμογές	-
	Μην χρησιμοποιείτε τυχαία ονόματα τομέα που δεν είστε ιδιοκτήτες για την εσωτερική υποδομή σας. Για παράδειγμα, δεν θεωρούν το ιδιωτικό όνομα τομέα ως τομέα ανώτατου επιπέδου.	Σύστημα ονομάτων τομέα, Εφαρμογές	
	Αποτρέψτε την αίτηση DNS για εσωτερικούς χώρους ονομάτων να διαρρεύσουν	Εφαρμογές	Σύστημα ονομάτων

	στο Internet εφαρμόζοντας τείχος προστασίας πολιτικές.		τομέα
	Χρησιμοποιήστε αποκλειστικά TLD όπως .test, .example, .invalid ή .localhost.	Σύστημα ονομάτων τομέα, Εφαρμογές	
Άρνηση παροχής υπηρεσίας			
Ενίσχυση / αντανάκλαση		Εφαρμογές, ασφάλεια, γενικός πάροχος Διαδικτύου, υλικό, εκτελέσιμα προγράμματα, διαμόρφωση συστήματος, πρωτόκολλα εφαρμογών, διαχειριστές, Χειριστές	Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, διαχειριστές, χειριστές
	Υιοθετήστε την επαλήθευση διεύθυνσης IP πηγής στην άκρη της υποδομής Internet (κοντά στην προέλευση της κίνησης) για να αποτρέψετε την πλαστογράφηση διεύθυνσης δικτύου μέσω του φιλτραρίσματος εισόδου και εξόδου.	Εφαρμογές, ασφάλεια, γενικός πάροχος Διαδικτύου, υλικό, εκτελέσιμα προγράμματα, εφαρμογή πρωτόκολλα	Διαμόρφωση συστήματος, διαχειριστές, χειριστές
	Οι χειριστές του αυθεντικού φορέα εξυπηρετητή ονομάτων θα πρέπει να εφαρμόσουν το RRL (Limit Rate Response).	Εφαρμογές, Ασφάλεια, Γενικός πάροχος Διαδικτύου, Hardware, Εκτελέσιμα προγράμματα	Διαμόρφωση συστήματος, Εφαρμογή πρωτόκολλα, διαχειριστές, χειριστές
	Οι χειριστές διακομιστών ονομάτων DNS και οι ISP πρέπει να απενεργοποιήσουν την ανοικτή αναδρομή σε διακομιστές ονομάτων και μπορούν μόνο να δέχονται ερωτήματα DNS από	Εφαρμογές, Ασφάλεια, Γενικός πάροχος Διαδικτύου, Hardware, Εκτελέσιμα προγράμματα	Διαμόρφωση συστήματος , Εφαρμογή πρωτόκολλα, διαχειριστές, χειριστές

	αξιόπιστες πηγές.		
Πλημμύρα		Εφαρμογές, Ασφάλεια, Γενικοί πάροχοι Διαδικτύου, Hardware, εκτελέσιμα προγράμματα, διαμόρφωση συστήματος, βασικά πρωτόκολλα διευθύνσεων, διαχειριστές, χειριστές	Διαμόρφωση συστήματος , Βασικές διαχείριση πρωτόκολλων, διαχειριστές, χειριστές
	Οι κατασκευαστές και οι διαμορφωτές του εξοπλισμού δικτύου πρέπει να λάβουν μέτρα για να εξασφαλίσουν όλες τις συσκευές. Μια πιθανότητα είναι να τα διατηρήσετε ενημερωμένα με την επιδιόρθωση ελαττωμάτων.	Εφαρμογές, Ασφάλεια, Γενικοί πάροχοι Διαδικτύου, Hardware, Εκτελέσιμα προγράμματα	Διαμόρφωση συστήματος , Βασικές διαχείριση πρωτόκολλων, διαχειριστές, χειριστές
Εκμετάλλευση πρωτοκόλλου	-	Εφαρμογές, ασφάλεια, γενικοί παροχείς Διαδικτύου, υλικό, εκτελέσιμα προγράμματα, διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, Διαχειριστές, χειριστές	-
Δύσμορφος επίθεση πακέτων	-	Εφαρμογές, Ασφάλεια, Γενικοί πάροχοι Διαδικτύου, Hardware, εκτελέσιμα προγράμματα, διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, Διαχειριστές, χειριστές	-
Εφαρμογή	-	Εφαρμογές, Ασφάλεια, Γενικός πάροχος Διαδικτύου, Hardware, εκτελέσιμα προγράμματα, διαμόρφωση συστήματος, πρωτόκολλα εφαρμογών, διαχειριστές, χειριστές	-

Πίνακας 7 - Απειλές με καλές πρακτικές για μετριασμό και κάλυψη περιουσιακών στοιχείων

7.1. Ανάλυση κενού

Κατά συνέπεια, τα περιουσιακά στοιχεία που καλύπτονται από μία τουλάχιστον ορθή πρακτική συγκρίνονται με τον πλήρη κατάλογο όλων των περιουσιακών στοιχείων (βλέπε κεφάλαιο 3) που απειλούνται από συγκεκριμένη σημαντική απειλή. Αυτή η ανάλυση κενών περιγράφει με σαφήνεια τις υπάρχουσες ελλείψεις αυτής της μελέτης, οι οποίες αντιμετωπίζονται με συστάσεις (βλ. Κεφάλαιο 8).

Τα συνοπτικά αποτελέσματα της ανάλυσης κενών που παρουσιάζεται στον Πίνακα 7 είναι ότι για τις πιο σημαντικές συγκεκριμένες απειλές υπάρχουν διαθέσιμες στο κοινό ορθές πρακτικές. Τα κενά που βρέθηκαν για κάθε ομάδα απειλών είναι τα εξής:

Απειλές δρομολόγησης

- **Ως αεροπειρατεία**

Διαφορά βρέθηκε: Διαχειριστές

Οι διαχειριστές είναι υπεύθυνοι για τον καθορισμό των κανόνων δρομολόγησης και των επιπέδων ασφαλείας. Για παράδειγμα, καθορίζουν τα φίλτρα που εφαρμόζονται στις ανακοινώσεις BGP και παρακολουθούν την κατάσταση του BGP. Οι διαχειριστές μιας υποδομής Διαδικτύου είναι συνήθως σε άμεση σχέση με τους διαχειριστές άλλων δικτύων (peer) και συνεργάζονται στενά μαζί τους.

Οι διαθέσιμες ορθές πρακτικές για τη δρομολόγηση καλύπτουν τεχνικές πτυχές που σχετίζονται με το φιλτράρισμα και την παρακολούθηση. Ωστόσο, δεν υπάρχει σήμερα καμία καλή πρακτική που εμποδίζει έναν διαχειριστή να καθορίζει κανόνες που επηρεάζουν τη δρομολόγηση με κακό τρόπο, είτε σε τοπική είτε σε παγκόσμια κλίμακα.

Επιπλέον, οι διαχειριστές διασφαλίζουν την ασφάλεια της δρομολόγησης παρακολουθώντας την κατάσταση του χρησιμοποιούμενου συστήματος δρομολόγησης (π.χ. BGP) και καθορίζοντας τις ενέργειες που πρέπει να λάβουν σε περίπτωση συμβάντος. Ωστόσο, επί του παρόντος δεν υπάρχουν διαθέσιμες καλές πρακτικές που να εστιάζουν σαφώς στον τρόπο αντιμετώπισης περιστατικών δρομολόγησης μεταξύ διαφορετικών δικτύων. Πράγματι, τέτοια περιστατικά συχνά επιλύονται επικοινωνώντας με άλλους διαχειριστές σε ad-hoc βάση.

Αυτό το χάσμα απαιτεί την ανάπτυξη ορθών πρακτικών που θα ενισχύσουν τη συνεργασία μεταξύ των διαχειριστών, με στόχο την εξασφάλιση δρομολόγησης και χειρισμού περιστατικών.

Απειλές DNS

- **DNS Spoofing**

Διαφορά βρέθηκε: Διαχειριστές

Ομοίως με τη δρομολόγηση, οι διαχειριστές είναι υπεύθυνοι για την ασφάλεια DNS. Ωστόσο, η υποκλοπή μπορεί να γίνει όταν οι διαχειριστές αποτυγχάνουν στην εξασφάλιση

ορισμένων ευπαθών στοιχείων (π.χ., διαμορφώστε έναν διακομιστή DNS με ασφαλή τρόπο) στην υποδομή τους. Για το σκοπό αυτό, οι διαχειριστές ενδέχεται να χρειαστεί να κάνουν μια επισκόπηση του τρέχοντος επιπέδου ασφαλείας τους και να αξιολογήσουν τα περιουσιακά στοιχεία για να καλύψουν τις καλές πρακτικές.

Όπως και στο παρελθόν, υπάρχει ανάγκη συνεργασίας στην κοινότητα, ειδικά επειδή το DNS είναι κατανεμημένο σύστημα με πολλούς διαφορετικούς οργανισμούς που εμπλέκονται. Πράγματι, η πλαστογράφηση μπορεί να μετριαστεί όταν οι διαχειριστές της ανταλλαγής υποδομών Διαδικτύου με τους συνομηλίκους τους για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών.

- **Δηλητηρίαση DNS**

Διαφορά βρέθηκε: Διαχειριστές

Αυτό το κενό είναι ίδιο με αυτό που εντοπίστηκε για το διαχειριστή στην απειλή "DNS Spoofing". Τα συμπεράσματα είναι πανομοιότυπα.

Βρήκε κενό: Χειριστές

Οι φορείς εκμετάλλευσης των υποδομών DNS είναι υπεύθυνοι για την ανάπτυξη κανόνων ασφαλείας που μπορούν να εφαρμόσουν οι διαχειριστές στα στοιχεία υποδομής του Διαδικτύου. Ωστόσο, οι άνθρωποι δεν είναι ανοσοποιημένοι σε λάθη. Επιπλέον, η επίδραση κάποιου τεχνικού κανόνα ασφαλείας ενδέχεται να διαφέρει ανάλογα με τις ιδιαιτερότητες μιας δεδομένης υποδομής Διαδικτύου.

Αυτό το χάσμα μπορεί να μετριαστεί με την αξιολόγηση της εφαρμογής καλών πρακτικών στην προστασία της υποδομής του Διαδικτύου. Οι φορείς εκμετάλλευσης μπορούν επίσης να υποβάλουν έκθεση σχετικά με την εφαρμογή ορθών πρακτικών στην ιδιαίτερη υποδομή τους, προκειμένου να ωφελήσουν την κοινότητα.

- **Άρνηση παροχής υπηρεσιών / πλημμύρες**

Βρήκε κενό: ***Διαμόρφωση συστήματος***

Η διαμόρφωση του συστήματος πρέπει να διασφαλίζει την εφαρμογή μιας πολιτικής ασφαλείας. Ωστόσο, ανάλογα με τις τιμές ορισμένων παραμέτρων και τις ιδιαιτερότητες της υποδομής διαδικτύου, μπορεί να οδηγήσει σε διαφορετικά αποτελέσματα.

Καμία καλή πρακτική δεν υπάρχει σήμερα για να διασφαλιστεί η προστασία από την άρνηση παροχής υπηρεσιών / πλημμύρας καθορίζοντας μια διαμόρφωση συστήματος για ένα συγκεκριμένο στοιχείο υποδομής του Διαδικτύου.

Προκειμένου να επικυρωθεί η καλή χρήση της διαμόρφωσης του συστήματος και να βελτιωθεί η ασφάλεια, η κοινότητα μπορεί να μοιραστεί εμπειρίες σχετικά με τη διαμόρφωση που χρησιμοποιείται για να εξασφαλίσει την υποδομή του στο Διαδίκτυο, εστιάζοντας σε συγκεκριμένες περιπτώσεις χρήσης.

Διαφορά βρέθηκε: Βασικά πρωτόκολλα διευθύνσεων

Στην πλειονότητα των περιπτώσεων άρνησης παροχής υπηρεσιών / πλημμύρας, τα βασικά πρωτόκολλα διευθυνσιοδότησης παραβιάζονται όταν το επιτρέπει το πρωτόκολλο (π.χ. διευθύνσεις προέλευσης IP σε πακέτα UDP). Επίσης, εάν τα βασικά πρωτόκολλα διευθυνσιοδότησης δεν είναι ψευδή, η διαφορά από τις πλημμύρες και ένας υψηλός ρυθμός τακτικών αιτήσεων είναι δύσκολο να καταγραφούν για τα μηχανήματα, καθώς απαιτεί κατανόηση του σκοπού. Από την άποψη αυτή, δεν υπάρχει καμία ορθή πρακτική για την πρόληψη αυτού του διαρθρωτικού ζητήματος.

Αυτό το κενό μπορεί να καλυφθεί με την αξιολόγηση συγκεκριμένων μέτρων ασφαλείας για την προστασία των συνδεδεμένων συσκευών. Επιπλέον, η μετάβαση προς ασφαλέστερα πρωτόκολλα μπορεί να μετριάσει αυτήν την απειλή σε κάποιο βαθμό.

Διαφορά βρέθηκε: Διαχειριστές

Αυτό το κενό είναι ίδιο με αυτό που εντοπίστηκε στις ομάδες απειλών "Δρομολόγηση" και "DNS". Τα συμπεράσματα είναι πανομοιότυπα.

Βρήκε κενό: Χειριστές

Αυτό το κενό είναι ίδιο με το κενό που βρέθηκε για τις ομάδες απειλών "Δρομολόγηση" και "DNS". Τα συμπεράσματα είναι πανομοιότυπα.

Για κάθε ομάδα απειλών, οι τύποι περιουσιακών στοιχείων ανθρώπινου δυναμικού καλύπτονται ανεπαρκώς. Αυτό πιθανώς οφείλεται στην τεχνική εστίαση του αναθεωρημένου υλικού. Ως εκ τούτου, είναι σκόπιμο οι ιδιοκτήτες περιουσιακών στοιχείων να εξετάσουν τον ανθρώπινο παράγοντα, εκτός από τις τεχνικές καλές πρακτικές, στη στρατηγική ασφαλείας τους.

Επιπλέον, οι καλές πρακτικές δεν καλύπτουν τις πλημμύρες απειλή για τη περιουσιακών στοιχείων *διαμόρφωσης του συστήματος* και *πρωτόκολλα εφαρμογής* . Αυτό προκύπτει από ένα πιο διαρθρωτικό ζήτημα. Οι πλημμύρες εκμεταλλεύονται τον όγκο των δεδομένων για να διαταράξουν ένα σύστημα ή μια υπηρεσία, οπότε τα λανθασμένα διαμορφωμένα ή παρωχημένα πρωτόκολλα δεν είναι αναγκαστικά προϋπόθεση. Έτσι, οι καλές πρακτικές που θεωρούνται δεν περιγράφουν τα αντίμετρα.

8. Συστάσεις

Με βάση τις γνώσεις που αποκτήθηκαν στο πλαίσιο αυτής της μελέτης, παρατίθενται σε αυτό το κεφάλαιο συστάσεις για κατανόηση και βελτίωση της ασφάλειας της υποδομής του Διαδικτύου. Επομένως, τα αποθέματα που λαμβάνονται και οι απειλές συμπυκνώνονται σε σημαντικές ειδικές ομάδες απειλών της υποδομής Διαδικτύου. Με βάση τα παραπάνω, συλλέχθηκαν και συνοψίστηκαν συμπληρωματικές πληροφορίες εμπειρογνωμόνων σχετικά με τις ορθές πρακτικές.

Η ακόλουθη ανάλυση κενού αποδίδει έναν αριθμό περιουσιακών στοιχείων που δεν μπορούν να καλυφθούν από τουλάχιστον μία καλή πρακτική. Προκειμένου να παρέχονται πληροφορίες για την προστασία μη επαρκώς καλυμμένων περιουσιακών στοιχείων, έχει αναπτυχθεί ένα σύνολο συστάσεων.

Ο κατάλογος των συστάσεων χωρίζεται σε τεχνικές (ενότητα 8.1) και οργανωτικές (ενότητα 8.2) οδηγίες για να απευθύνονται σε συγκεκριμένο κοινό-στόχο. Μπορούν να εξεταστούν από τους ενδιαφερόμενους φορείς όπως είναι οι οργανισμοί τυποποίησης (π.χ. IETF, ICANN), η βιομηχανία και ο ακαδημαϊκός τομέας.

Πρέπει κανείς να γνωρίζει το γεγονός ότι κανένας κατάλογος καλών πρακτικών και συστάσεων δεν μπορεί να είναι εξαντλητικός ούτε είναι εφικτό να διατηρηθεί ένας κατάλογος όλων των πιθανών μέτρων προστασίας. Είναι σημαντικό να ανεβάσετε την μπάρα αρκετά υψηλή ώστε να εξασφαλίσετε τουλάχιστον μια βασική ασφάλεια.

Το αντικείμενο της μελέτης αυτής είναι η υποδομή του Διαδικτύου. η μελέτη αυτή υποστηρίζει έντονα ότι εξαρτάται από τις βασικές επιχειρηματικές δραστηριότητες μιας επιχείρησης, την εφαρμογή και προσαρμογή των ορθών πρακτικών δρομολόγησης, DNS και μετριασμού των DDoS που αναφέρονται στο Κεφάλαιο 7 . Επιπλέον, θα πρέπει να έχουμε κατά νου ότι οι προμηθευτές υλικού για τις βασικές διατάξεις του Διαδικτύου, όπως δρομολογητές ή διακόπτες συχνά απελευθερώνουν τις κατευθυντήριες γραμμές για την ασφαλή και υγιή διαμόρφωσή τους (βλέπε έγγραφα που αναφέρονται στο Κεφάλαιο 7).

8.1. Τεχνικές συστάσεις

Οι συστάσεις που παρουσιάζονται σε αυτό το υποτμήμα πρέπει να θεωρούνται ως καθοδήγηση στο τεχνικό προσωπικό, όπως οι φορείς εκμετάλλευσης ή οι διαχειριστές. Η εφαρμογή των απαριθμούμενων μέτρων θα πρέπει να αποδίδεται κατά προτεραιότητα στα αποτελέσματα των αξιολογήσεων κινδύνου.

Σύσταση 1: Για τους ιδιοκτήτες υποδομών του Διαδικτύου και για τους ρυθμιστικούς οργανισμούς δικτύων ηλεκτρονικών επικοινωνιών, να αξιολογήσετε το σημερινό επίπεδο ασφάλειας, κατανοώντας τα περιουσιακά στοιχεία που καλύπτονται (και δεν καλύπτονται) από τα υφιστάμενα μέτρα ασφαλείας.

Έχοντας μια ολιστική άποψη για τα περιουσιακά στοιχεία που πρέπει να εξασφαλιστούν είναι η βάση για να διασφαλιστεί ότι τα μέτρα ασφαλείας εφαρμόζονται αποτελεσματικά. Έτσι, το πρώτο βήμα για κάθε ιδιοκτήτη υποδομής Διαδικτύου και ρυθμιστικό δίκτυο ηλεκτρονικών επικοινωνιών θα αρχίσει με μια ανάλυση των υφιστάμενων (και

προγραμματισμένων) περιουσιακών στοιχείων προκειμένου να κατανοηθούν οι υφιστάμενες ή πιθανές απειλές.

Οι ιδιοκτήτες υποδομών του Ίντερνετ θα πρέπει να αξιολογούν τον τρόπο με τον οποίο τα τρέχοντα μέτρα ασφαλείας μετριάζουν τις απειλές που εφαρμόζονται σε αυτά τα στοιχεία. Συγκεκριμένα, θα μπορούσαν να επικεντρωθούν σε Σημαντικές Ειδικές Απειλές που συνδέονται με τη Δρομολόγηση, το DNS και την Άρνηση Υπηρεσίας.

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση παροχής υπηρεσιών / πλημμύρες: *Διαχειριστές, χειριστές*

Σύσταση 2: Για τους ιδιοκτήτες υποδομών του Διαδικτύου, να αξιολογηθεί η εφαρμογή προσαρμοσμένων ορθών πρακτικών κατά τρόπο εστιασμένο.

Οι ιδιοκτήτες υποδομών του Ίντερνετ θα πρέπει γενικά να εξετάσουν τη χρήση συστάσεων από οργανισμούς ανοικτού κώδικα, όπως η IETF, η κοινωνία του Διαδικτύου, η Euro-IX ή η RIPE. Θα πρέπει επίσης να λαμβάνουν υπόψη τις συστάσεις που αφορούν συγκεκριμένους πωλητές για να εξασφαλίσουν την υποδομή υλικού και λογισμικού του οργανισμού καθ 'όλη τη διάρκεια του κύκλου ζωής του.

Οι ιδιοκτήτες υποδομών του διαδικτύου πρέπει να καθορίσουν τα μέτρα που πρέπει να εφαρμόσουν και πώς να τα χρησιμοποιήσουν, προκειμένου να βελτιώσουν την ασφάλεια των επιμέρους περιουσιακών στοιχείων και του συνόλου του συστήματος τους. Για παράδειγμα, θα μπορούσαν να δώσουν προτεραιότητα σε συγκεκριμένα μέτρα ασφαλείας δίνοντας μεγαλύτερη προσοχή στις απειλές που αντιμετωπίζουν. Για το σκοπό αυτό, μπορούν να βασίζονται στην παρακολούθηση για παράδειγμα.

Αυτό ισχύει για συστάσεις για τεχνικές λεπτομέρειες, όπως διαμόρφωση συσκευών ή ανάπτυξη λογισμικού, καθώς και για οργανωτικές δομές όπως η εξασφάλιση επιχειρηματικών διαδικασιών και η εκτίμηση κινδύνου.

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση παροχής υπηρεσιών / Πλημμύρες: *Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, διαχειριστές, χειριστές*

Σύσταση 3: Για τους ιδιοκτήτες υποδομών Διαδικτύου, συνεργάζονται με την κοινότητα για την ανταλλαγή πληροφοριών σχετικά με τις απειλές και για την προώθηση της εφαρμογής ορθών πρακτικών ως μέτρα άμβλυνσης.

Οι ιδιοκτήτες υποδομών διαδικτύου πρέπει να καθιερώσουν καλύτερο συντονισμό στον τομέα της ασφάλειας των υποδομών του Διαδικτύου. Οι διαδικασίες και τα μέτρα ασφάλειας σε τοπικό αλλά και σε ευρύτερο κλίμα απαιτούν συντονισμό για αποτελεσματικό μετριασμό σε τεχνικό και επιχειρησιακό επίπεδο. Περιλαμβάνει επίσης την ανάθεση υπεύθυνου προσωπικού και τη δημιουργία περιφερειακών, εθνικών και πολυεθνικών κοινοτήτων πλατφορμών εμπιστοσύνης και ανταλλαγής πληροφοριών.

Μπορεί να υπάρξει ανταλλαγή εμπιστευτικών πληροφοριών:

- Με βάση την εμπιστοσύνη. δεδομένου ότι η αποκάλυψη συμβάντων μπορεί να έχει αρνητικό αντίκτυπο στη φήμη.
- Μέσω ρυθμίσεων και νομικών υποχρεώσεων, όπως προβλέπεται στο άρθρο 13α της οδηγίας 2009/140 / ΕΚ της ΕΕ.
- Μέσω Κέντρων Ανταλλαγής Πληροφοριών και Ανάλυσης (ISAC).

Είναι επίσης σημαντικό να δεσμευθεί να συμμετάσχει, αυτό εξασφαλίζει ότι άλλες οργανώσεις βιώνουν την εφαρμογή στην πράξη και μπορεί να ακολουθήσουν το παράδειγμα.

Επιπλέον, μια τέτοια συνεργασία είναι επωφελής για την ενίσχυση του επιπέδου ασφαλείας του Διαδικτύου. Θα βοηθήσει στην κατανόηση των προαπαιτήσεων και των προκλήσεων που συνδέονται με την ανάπτυξη ορθών πρακτικών από τους ιδιοκτήτες υποδομών του Διαδικτύου. Μπορεί επίσης να οδηγήσει στην ανάπτυξη νέων ορθών πρακτικών (που βασίζονται στην κοινότητα) για την κάλυψη αναδυόμενων απειλών.

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση παροχής υπηρεσιών / Πλημμύρες: *Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, διαχειριστές, χειριστές*

Σύσταση 4: Για τους χρήστες που χρησιμοποιούν οδηγούς καλών πρακτικών, αναφέρετε τις υλοποιήσεις τους, τα περιουσιακά στοιχεία που καλύπτονται και τα κενά που βρέθηκαν.

Για οργανισμούς που επιθυμούν να εφαρμόσουν τις υπάρχουσες καλές πρακτικές, είναι πολύ χρήσιμο αν οι οδηγοί ορθής πρακτικής δείχνουν μια λίστα επιτυχημένων εφαρμογών. Εάν ο κατάλογος αυτός περιέχει γνωστά ονόματα, τονίζεται η σημασία των ορθών πρακτικών. Επίσης, ο οργανισμός που πρόκειται να εφαρμόσει τα μέτρα ασφαλείας που περιγράφονται στις ορθές πρακτικές μπορεί να έρθει σε επαφή με τις άλλες οργανώσεις

που έχουν ήδη εφαρμόσει επιτυχώς τα μέτρα ασφαλείας προκειμένου να συζητήσουν ανοιχτές ερωτήσεις.

Για το σκοπό αυτό, συνιστάται οι οργανισμοί που χρησιμοποιούν ορθές πρακτικές να αναφέρουν στις αντιφάσεις των δημιουργών τους, για παράδειγμα περιπτώσεις όπου η ορθή πρακτική δεν είναι άμεσα εφαρμόσιμη λόγω μιας πολύ συγκεκριμένης υποδομής Διαδικτύου. Σε σχέση με τη σύσταση 3, αυτή η ανταλλαγή πληροφοριών μπορεί να πραγματοποιηθεί μέσω μιας πλατφόρμας με γνώμονα την κοινότητα.

Επιπλέον, οι υπεύθυνοι ανάπτυξης καλών πρακτικών θα μπορούσαν επίσης να τονίσουν τα περιουσιακά στοιχεία που καλύπτονται από τα μέτρα ασφαλείας που περιγράφονται και τα κενά που εξακολουθούν να υπάρχουν. Αυτό βοηθά τους οργανισμούς που εφαρμόζουν τα μέτρα ασφαλείας που περιγράφονται στον οδηγό ορθής πρακτικής να κατανοούν εύκολα ποια περιουσιακά στοιχεία καλύπτονται και ποια περιουσιακά στοιχεία παραμένουν ανέγγιχτα.

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση παροχής υπηρεσιών / Πλημμύρες: *Διαμόρφωση συστήματος, διαχειριστές, χειριστές*

Σύσταση 5: Οι λέξεις έχουν σημασία: Εξασφαλίστε τη σωστή χρήση όρων και ορισμών.

Για μια κοινότητα που ανήκει στον ίδιο τομέα, συνιστάται να χρησιμοποιείτε την ίδια ορολογία. Αυτό θα βελτιώσει την κατανόηση του γραπτού υλικού και θα βοηθήσει στη συζήτηση σχετικών θεμάτων. Μεταξύ άλλων, το RFC 4949 παρέχει ένα σύνολο όρων ασφαλείας και ορισμών.

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση παροχής υπηρεσιών / πλημμύρες: *Διαχειριστές, χειριστές*

8.2. Οργανωτικές συστάσεις

Οι οργανωτικές συστάσεις πρέπει να κατανοούνται και να εφαρμόζονται από υπεύθυνο διοικητικό προσωπικό και να επικεντρώνονται στον καθορισμό διαδικασιών και διαδικασιών λειτουργίας.

Σύσταση 6: Για τους ιδιοκτήτες υποδομών Διαδικτύου, χρησιμοποιήστε τις κατάλληλες μεθόδους αξιολόγησης κινδύνου για να κατανοήσετε τα ευπαθή περιουσιακά στοιχεία στην υποδομή σας στο Internet και να δώσετε προτεραιότητα στις ενέργειες προστασίας σας.

Είναι σκόπιμο οι ιδιοκτήτες υποδομών Διαδικτύου να δώσουν προτεραιότητα σε ενέργειες για την προστασία της υποδομής τους στο Διαδίκτυο. Ωστόσο, μόνο μια αξιολόγηση κινδύνου θα εκθέσει αξιόπιστα στοιχεία σχετικά με την πιθανότητα πιθανής απώλειας, που επίσης χαρακτηρίζεται ως κίνδυνος. Τα εντοπισμένα κενά μπορούν να καλυφθούν από τα μέτρα εφαρμογής που παρουσιάζονται στο κεφάλαιο για τις ορθές πρακτικές (βλέπε τμήμα 7).

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση υπηρεσίας / Πλημμύρες: *Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, διαχειριστές, χειριστές, διαχειριστές, χειριστές*

Σύσταση 7: Δημιουργία ενός προγράμματος ευαισθητοποίησης και κατάρτισης στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών.

Ένα εκπαιδευτικό πρόγραμμα ΤΠΕ είναι ζωτικής σημασίας για την ασφάλεια της υποδομής του Διαδικτύου σε κάθε επιχείρηση. Το περιεχόμενο και το πεδίο εφαρμογής του προγράμματος πρέπει να συνδέονται με τις υφιστάμενες οδηγίες για την ασφάλεια και τις καθιερωμένες πολιτικές. Επιπλέον, πρέπει να καλύπτει όλες τις θέσεις μιας επιχείρησης και να διακρίνει μεταξύ γενικής κατάρτισης στον τομέα της ασφάλειας για την ευαισθητοποίηση και ειδικά προγράμματα προσαρμοσμένα στους συγκεκριμένους ρόλους των εμπειρογνωμόνων. Μια βασική κατανόηση της ασφάλειας μπορεί να επιτευχθεί με ένα ολοκληρωμένο σύστημα πιστοποίησης. Ωστόσο, είναι σημαντικό να δηλωθεί ότι παρόλο που η πιστοποίηση αποτελεί πολύτιμο δομικό στοιχείο, δεν είναι πράγματι λύση για να στηριχθεί κανείς απολύτως. Οι συχνές δραστηριότητες εξασφαλίζουν την ετοιμότητα της πρακτικής και πρέπει να περιλαμβάνουν εκτεταμένες συνεδριάσεις ενημέρωσης για να συζητηθούν τα διδάγματα που αντλήθηκαν.

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*

- Άρνηση παροχής υπηρεσιών / Πλημμύρες: *Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, διαχειριστές, χειριστές*

Σύσταση 8: Οι ιδιοκτήτες υποδομών διαδικτύου υποχρεώνουν τους τρίτους προμηθευτές να εφαρμόζουν μέτρα ασφαλείας.

Οι ιδιοκτήτες υποδομών διαδικτύου θα πρέπει να συστήσουν ότι ο πωλητής ακολουθεί ορισμένους κανόνες, συστάσεις ή πιστοποιήσεις σύμφωνα με την αρχιτεκτονική ή το επιχειρηματικό μοντέλο τους. Αυτοί οι κανόνες θα πρέπει να ορίζονται ως μέρος της εκτίμησης κινδύνου του ιδιοκτήτη του περιουσιακού στοιχείου υπό την εποπτεία του προσωπικού ασφαλείας της εταιρείας. Αυτό εξασφαλίζει εκτεταμένο αντίκτυπο των συστάσεων και θα βελτιώσει τη βιωσιμότητα της ασφάλειας.

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση παροχής υπηρεσιών / Πλημμύρες: *Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, διαχειριστές, χειριστές*

Σύσταση 9: Μείνετε ενημερωμένοι για τυχόν ενημερώσεις.

Μείνετε ενημερωμένοι σχετικά με τα πρωτόκολλα και τις ενημερώσεις προδιαγραφών και αξιολογείτε την έγκαιρη υλοποίηση μέσα στις δικές σας υποδομές και συστήματα. Αυτό μπορεί να επιτευχθεί με τη συμμετοχή σε συνέδρια και εργαστήρια ή απλά με την εγγραφή σε καταλόγους ή περιοδικά. Η πρακτική εμπειρία δείχνει ότι σε πολλές περιπτώσεις είναι διαθέσιμα ενημερωμένα πρωτόκολλα ή προδιαγραφές, αλλά απλά δεν εφαρμόζονται ή εφαρμόζονται ανεπαρκώς.

Η παρούσα σύσταση αποσκοπεί να καλύψει τα ακόλουθα κενά:

- Απειλές δρομολόγησης: *Διαχειριστές*
- DNS Spoofing: *Διαχειριστές*
- DNS δηλητηρίαση: *Διαχειριστές, χειριστές*
- Άρνηση παροχής υπηρεσιών / Πλημμύρες: *Διαμόρφωση συστήματος, πρωτόκολλα βασικής διεύθυνσης, διαχειριστές, χειριστές*

9. Συμπεράσματα

Αυτός ο Τοπικός Οδηγός Απειλών και Καλών Πρακτικών για την Υποδομή Διαδικτύου θα επιτρέπουν στους κατόχους υποδομών Διαδικτύου να εξασφαλίζουν τα περιουσιακά τους στοιχεία ενάντια σε σημαντικές και αναδυόμενες απειλές.

Για το σκοπό αυτό, η μελέτη αυτή έχει κατατάξει στοιχεία και απειλές της υποδομής του Διαδικτύου στους χάρτες μυαλού. Έχει υπογραμμίσει τα περιουσιακά στοιχεία που εμπλέκονται σε σημαντικές συγκεκριμένες απειλές, οι οποίες περιλαμβάνουν απειλές δρομολόγησης, απειλές DNS, άρνηση παροχής υπηρεσιών και γενικές απειλές. Επιπλέον, οι πράκτορες απειλών, οι οποίοι αποτελούν την αιτία της απειλής, έχουν επίσης χαρτογραφήσει για κάθε τύπο απειλής.

Για κάθε σημαντική συγκεκριμένη απειλή, αξιολογούνται οι τάσεις, με βάση τις δημόσιες πληροφορίες: το επίπεδο απειλής αυξάνεται παγκοσμίως, με εξαίρεση τις απειλές DNS, σε μείωση (αν και ο αριθμός των επιθέσεων παραμένει αυξημένος).

Για κάθε Σημαντική Ειδική Απειλή, η μελέτη περιγράφει μια λίστα με τις υπάρχουσες καλές πρακτικές που στοχεύουν στην άμβλυνση αυτών των απειλών. Οι καλές πρακτικές συνδέονται με τον κατάλογο των περιουσιακών στοιχείων που καλύπτονται και εκείνων που αποκαλύπτονται.

Με βάση τον κατάλογο των ακάλυπτων περιουσιακών στοιχείων, πραγματοποιήθηκε μια ανάλυση κενού. Ενισχύει την έλλειψη ορθών πρακτικών για την αντιμετώπιση των απειλών που συνδέονται με τους ανθρώπινους πόρους (διαχειριστές και φορείς εκμετάλλευσης), τη διαμόρφωση του συστήματος και τα βασικά πρωτόκολλα αντιμετώπισης.

Τέλος, προτείνεται ένας κατάλογος με πέντε τεχνικές και τέσσερις οργανωτικές συστάσεις για τη βελτίωση της ασφάλειας της υποδομής του Διαδικτύου. Επιπλέον, οι ιδιοκτήτες υποδομών του Διαδικτύου μπορούν να επαναχρησιμοποιήσουν ή να προσαρμόσουν τα εργαλεία που προτείνονται σε αυτή τη μελέτη (π.χ. χάρτες μυαλού, απειλές και περιουσιακά στοιχεία που συνδέουν το πλέγμα, απειλές που συνδέονται με μήτρα και παράγοντες απειλής) για να αξιολογήσουν το επίπεδο έκθεσής τους στις τρέχουσες απειλές. Μπορούν επίσης να αξιολογήσουν (ή να βελτιώσουν) τα τρέχοντα μέτρα ασφαλείας για κάθε περιουσιακό στοιχείο που συνδέεται με αυτές τις απειλές.

Βιβλιογραφία

[1] "A Forensic Case Study on AS Hijacking: The Attacker's Perspective", http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf

[2] "Anatomy of a Data Breach", http://about-threats.trendmicro.com/us/webattack/110/Anatomy+of+a+Data+Breach

[3] "Application Misconfiguration", http://projects.webappsec.org/w/page/13246914/Application%20Misconfiguration

[4] "Article 13a of EU Directive 2009/140/EC", https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20 NO%20CROPS.pdf

[5] "Beware of BGP Attacks", http://www.cc.gatech.edu/~dovrolis/Papers/ccr-bgp.pdf

[6] "Beware of BGP Attacks", http://www.cc.gatech.edu/~dovrolis/Papers/ccr-bgp.pdf

[7] "Brute force attack", http://www.sophos.com/en-us/threat-center/threat-analyses/threatsaurus/a-to-z-of- threats/b/brute-force-attack.aspx

[8] "BSI Threats Catalogue", Federal Office for Information Security, 2012, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf? b lob=publicationFile

[9] "ENISA Threat Landscape 2013", https://www.enisa.europa.eu/activities/risk-management/evolving-threat- environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

[10] "ENISA Work Programme 2014", http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 , in particular, p. 16.

[11] "ENISA Annual Incident Reports 2013", http://www.enisa.europa.eu/activities/Resilience-and- CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport

[12] "Financial Services Information Sharing and Anlysis Center", https://www.fsisac.com

[13] "IBM Security Services Cyber Security Intelligence Index", IBM, 2013, https://www- 935.ibm.com/services/multimedia/Cyber_security_Index.pdf

[14] "Measuring and Analyzing on Effection of BGP Session Hijack Attack", http://www.wseas.us/e- library/conferences/2013/Rhodes/CIRCOM/CIRCOM-13.pdf

[15] "Multiple DNS implementations vulnerable to cache poisoning", http://www.kb.cert.org/vuls/id/800113

[16] "Name Collision in the DNS",

https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf
[17] "Popular Registrar Namecheap Fixes DNS Hijack Bug", http://threatpost.com/popular-registrar-namecheap- fixes-dns-hijack-bug
[18] "Protecting Border Gateway Protocol for the Enterprise", http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html
[19] "Protecting Border Gateway Protocol for the Enterprise", http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html
[20] "Reflection DDoS Attacks: How They Work and What You Can Do", http://www.ddosattacks.biz/attacks/reflection-ddos-attacks-how-they-work-and-what-you-can-do/
[21] "The Threat of Social Engineering and Your Defense Against It", http://www.sans.org/reading- room/whitepapers/engineering/threat-social-engineering-defense-1232
[22] "Threat Model for BGP Path Security", http://tools.ietf.org/html/rfc7132
[23] "Threat Model for BGP Path Security", http://tools.ietf.org/html/rfc7132
[24] "Threat Model for BGP Path Security": http://tools.ietf.org/html/rfc7132
[25] "Threats Catalogue – Elementary Threats", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf
[26] "Threats Catalogue – Elementary Threats", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf? b lob=publicationFile
[27] "What is Espionage", https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html
[28] ENISA Glossary, https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management- inventory/glossary
[29] ENISA, "Security Framework for Article 4 and 13a proposal", http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security- framework-for-articles-4-and-13a
[30] ENISA, "Smart Grid Threat Landscape", https://www.enisa.europa.eu/activities/risk-management/evolving- threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide
[31] ENISA, "Understanding the Importance of the Internet Infrastructure in Europe", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter- x/guidelines-for-enhancing-the-resilience-of-ecommunication-networks
[32] Hackmaggedon Analysis, http://hackmageddon.com/2013-cyber-attacks-statistics/
[33] http://arxiv.org/abs/1205.4011
[34] http://blackbag.gawker.com/anonymous-declares-cyber-war-on-israel-downs-mossad-si-1615500861

[35] http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack
[36] http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack
[37] http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho
[38] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online- freedom-and-opportunity-cyber-security
[39] http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon
[40] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF
[41] http://namecollisions.net/downloads/wpnc14_slides_strutt_looking_at_corp com.pdf
[42] http://newgtlds.icann.org/en/announcements-and-media/announcement-2-17nov13-en
[43] http://nrl.cs.arizona.edu/projects/lsrl-events-from-2003-to-2009/
[44] http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf
[45] http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf
[46] http://threatpost.com/popular-registrar-namecheap-fixes-dns-hijack-bug
[47] http://tools.ietf.org/html/rfc4949
[48] http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf
[49] http://www.bgpmon.net/hijack-by-as4761-indosat-a-quick-report
[50] http://www.bgpmon.net/how-the-internet-in-australia-went-down-under/
[51] http://www.bgpmon.net/looking-at-the-spamhouse-ddos-from-a-bgp-perspective/
[52] http://www.computerworld.in/news/massive-300gbps-ddos-attack-on-media-firm-fuelled-by-unpatched- server-flaw
[53] http://www.darkreading.com/attacks-breaches/ddos-attack-used-headless-browsers-in-150-hour- siege/d/d-id/1140696?
[54] http://www.ddosattacks.biz/attacks/slowloris-ddos-attack-aka-slow-and-low/
[55] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security- framework-for-articles-4-and-13a/at_download/fullReport
[56] http://www.freedomfromfearmagazine.org/index.php?option=com_content &view=article&id=302:hackers- profiling-who-are-the-attackers&catid=50:issue-7&Itemid=187
[57] http://www.gartner.com/newsroom/id/2344217
[58] http://www.itcsecure.com/2014/01/ddos-attacks-exploiting-vulnerability-in-network-time-protocol-call-the- doctor/

[59] http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/global-profiles-of-the- fraudster/Documents/global-profiles-of-the-fraudster-v2.pdf
[60] http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/
[61] http://www.renesys.com/2013/11/mitm-internet-hijacking/
[62] http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit
[63] http://www.ssi.gouv.fr/en/the-anssi/publications-109/scientific-publications/conference/abusing-anti-ddos- mechanisms-to-perform-dns-cache-poisoning.html
[64] http://www.terena.org/news/fullstory.php?news_id=2666
[65] http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background
[66] http://www.verizonenterprise.com/DBIR/2013/
[67] https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_T op_Threats_in_2013.pdf
[68] https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/guideline-on-threats-and-assets/at_download/file
[69] https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/guideline-on-threats-and-
[70] https://resilience.enisa.europa.eu/internet-infrastructure-security-and-resilience-reference-group
[71] https://technet.microsoft.com/library/security/ms13-065
[72] https://www.ncsc.nl/english/current-topics/news/cyber-security-assesment-netherlands.html
[73] https://www.usenix.org/conference/woot13/workshop-program/presentation/hay
[74] https://www.usenix.org/publications/login/december-2006-volume-31-number-6/homeless-vikings-short- lived-bgp-session-hijacki
[75] Joanna RUTKOWSKA, “Introducing stealth malware taxonomy”, COSEINC Advanced Malware Labs, 2006, S. 1-9
[76] RFC 2026, http://www.ietf.org/rfc/rfc2026.txt
[77] Verizon, “2014 Data Breach Investigations Report”, 2014, http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf 14 “Cloud Computing Top Threats in 2013”, Cloud Security Alliance, 2013,
[78] Y. ROBIAH et al., “A new generic taxonomy on hybrid malware detection technique”, arXiv preprint, http://arxiv.org/abs/0909.4860

Παραρτήματα

Παράρτημα Α Περιγραφή περιουσιακών στοιχείων υποδομής διαδικτύου

Αυτή η ενότητα περιγράφει τις διάφορες ομάδες της ταξινόμησης "Περιουσιακά στοιχεία υποδομής διαδικτύου", που αντιπροσωπεύεται από τον χάρτη μυαλού στο σχήμα 3 και περιγράφεται λεπτομερώς στο παράρτημα Β . Η περιγραφή δεν καλύπτει τον πλήρη χάρτη του νου, καθώς αυτό θα ξεπερνούσε το σκοπό αυτής της μελέτης. Αυτή η μελέτη επικεντρώνεται στα περιουσιακά στοιχεία του χάρτη του νου τα οποία παρουσιάζουν ιδιαίτερο ενδιαφέρον για την ανάλυση απειλών και την καλύτερη κάλυψη κοινών πρακτικών.

Πρωτόκολλα

Ένα πρωτόκολλο είναι ένα σύνολο ψηφιακών κανόνων για την ανταλλαγή δεδομένων εντός ή μεταξύ συστημάτων υπολογιστών. Τα πρωτόκολλα είναι πολύτιμα περιουσιακά στοιχεία για την υποδομή του Διαδικτύου επειδή επιτρέπουν την ουσιαστική επικοινωνία μεταξύ διαφορετικών συστημάτων υπολογιστών:

- *Βασικά πρωτόκολλα διευθύνσεων:* Βασικά πρωτόκολλα διευθύνσεων (π.χ. ARP, IPv4, IPv6, DNS) χρησιμοποιούνται για την αντιμετώπιση μιας ή μιας ομάδας συστημάτων υπολογιστών σε ένα δίκτυο. Ένα άλλο σύνολο βασικών πρωτοκόλλων διευθυνσιοδότησης, όπως το TCP και το UDP, επιτρέπουν τη διευθυνσιοδότηση συγκεκριμένου εκτελέσιμου προγράμματος που εκτελείται σε ένα μόνο σύστημα υπολογιστή.

- *Πρωτόκολλα δρομολόγησης:* Ένα πρωτόκολλο δρομολόγησης είναι ένα σύνολο κανόνων που χρησιμοποιούνται από τους δρομολογητές για να καθορίσουν τις καταλληλότερες διαδρομές στις οποίες πρέπει να προωθούν τα πακέτα προς τους τελικούς προορισμούς τους. Για τη δρομολόγηση δεδομένων μέσα στα πρωτόκολλα δικτύου ενός παρόχου Διαδικτύου όπως το RIP, το MPLS ή το OSPF χρησιμοποιούνται συνήθως. Μεταξύ διαφορετικών παροχέων Διαδικτύου το BGP πρωτόκολλο δρομολόγησης συνήθως χρησιμοποιείται για την ανταλλαγή διαδρομών δρομολόγησης. Τα πρωτόκολλα δρομολόγησης βασίζονται σε βασικά πρωτόκολλα διευθυνσιοδότησης.

- *Πρωτόκολλα σύνδεσης:* Αν χρησιμοποιηθούν διαφορετικά βασικά πρωτόκολλα διευθυνσιοδότησης και πρέπει να υπάρξει επικοινωνία μεταξύ αυτών των διαφορετικών κόσμων, μπορούν να εφαρμοστούν πρωτόκολλα συνδεσιμότητας. Για παράδειγμα, για να ενεργοποιηθεί η επικοινωνία που βασίζεται στο IPv6 σε ένα δίκτυο IPv4, μπορεί να χρησιμοποιηθεί το πρωτόκολλο 6to4. Ένα άλλο παράδειγμα είναι το NAT, το οποίο επιτρέπει την απόκρυψη ενός δικτύου διευθύνσεων IPv4 που δεν μπορεί να διαλυθεί πίσω από μια ενιαία διεύθυνση IP και τη δυνατότητα περιορισμένης σύνδεσης στο Internet.

- *Πρωτόκολλα εφαρμογής: Τα* εκτελέσιμα προγράμματα ορίζουν τα δικά τους πρωτόκολλα που εξαρτώνται από την εργασία (π.χ. HTTP, FTP ή SMTP) για την ανταλλαγή δεδομένων.

▪Πρωτόκολλα ασφαλείας: Τα πρωτόκολλα ασφαλείας είναι ένα συγκεκριμένο σύνολο ψηφιακών κανόνων που εξασφαλίζουν την προστασία των δεδομένων με την εφαρμογή κρυπτογραφικών πρωτογενών στοιχείων όπως η υπογραφή και η κρυπτογράφηση. Τα πρωτόκολλα ασφαλείας τυπικά τυλίγουν τα υπάρχοντα πρωτόκολλα εφαρμογών (π.χ. HTTPS, FTPS, IMAPS) ή ενισχύουν υπάρχοντα πρωτόκολλα (π.χ. IPsec, DNSSec).

Υπηρεσίες

Μια υπηρεσία, όσον αφορά την υποδομή του Διαδικτύου, αναφέρεται σε έναν αφηρημένο συνδυασμό άλλων λειτουργιών που χρησιμοποιούν άλλα περιουσιακά στοιχεία για να εκπληρώσουν μια καθορισμένη εργασία. Οι υπηρεσίες είναι σημαντικές, καθώς χωρίς υπηρεσίες η έννοια του Internet δεν έχει καμία χρησιμότητα. Οι υπηρεσίες μπορούν να δομηθούν ως εξής:

- *Βασική διεύθυνση:* Για τα διαφορετικά επίπεδα του πρωτοκόλλου Internet υπάρχουν έννοιες διευθυνσιοδότησης στοίβας που περιγράφονται στην παρακάτω ενότητα:

o Διευθυνσιοδότηση στρώματος συνδέσμου: Για το στρώμα συνδέσεων χρησιμοποιείται συνήθως το πρωτόκολλο Ethernet το οποίο βασίζεται στις λεγόμενες διευθύνσεις MAC. Οι διευθύνσεις MAC είναι διαφορετικοί αριθμοί που αντιστοιχίζονται σε συσκευές υλικού δικτύου. Οι σειρές αριθμών διοικούνται και εκχωρούνται σε κατασκευαστές υλικού από το IEEE.

o Διεύθυνση ηλεκτρονικού πρωτοκόλλου: Το πρωτόκολλο Internet είναι το κύριο πρωτόκολλο επικοινωνίας του Internet. Μια μοναδική διεύθυνση εκχωρείται σε οποιονδήποτε συμμετέχοντα στην επικοινωνία προκειμένου να μεταδίδει πληροφορίες μέσω ολόκληρου του Διαδικτύου σε έναν καθορισμένο προορισμό. Ο χώρος διευθύνσεων διατηρείται από το IANA, το οποίο δίνει χώρο στις διάφορες "Περιφερειακές Μητρώες Διαδικτύου" (RIR) (βλ. Routing). Τα ίδια τα RIR διαχωρίζουν τους δικούς τους χώρους διευθύνσεων και τα διανέμουν στα "Τοπικά Μητρώα Διαδικτύου" (LIRs). Οι LIR κατανέμουν στους πελάτες τους (π.χ. τελικούς χρήστες ή εταιρείες) τον συγκεκριμένο χώρο διευθύνσεων στο Internet.

o Διεύθυνση πρωτοκόλλου μεταφοράς: Τα πρωτόκολλα μεταφοράς παρέχουν υπηρεσίες επικοινωνίας από άκρο σε άκρο σε προγράμματα λογισμικού διαφορετικών υπολογιστών. Προσθέτει ένα στρώμα

αφαίρεσης στο πρωτόκολλο Internet που απευθύνεται και διακρίνει μεταξύ διαφορετικών εφαρμογών στον ίδιο κεντρικό υπολογιστή, αναθέτοντας μοναδικούς αριθμούς, τις αποκαλούμενες θύρες. Αυτοί οι αριθμοί θυρών διατηρούνται από το IANA. Σημαντικά πρωτόκολλα είναι TCP και UDP.

- Σύστημα ονομάτων τομέα: Το σύστημα ονομάτων τομέα είναι υπεύθυνο για τη μετάφραση εύκολα ονόματων ονομάτων τομέα (π.χ. enisa.europa.eu) στις αριθμητικές διευθύνσεις πρωτοκόλλου Internet. Τα ονόματα τομέων διαχειρίζονται καταχωρητές ονομάτων τομέα, οι οποίοι οργανώνονται υπό ιεραρχία με επικεφαλής τον IANA.

- Μονάδα αντιμετώπισης: Γενικά, για την αντιμετώπιση πόρων στο Διαδίκτυο, χρησιμοποιούνται οι αποκαλούμενοι Ενιαίοι Δείκτες Πόρων (URI). Η σύνταξη των URIs έχει ως εξής: Αρχίζει με ένα πρωτόκολλο για τον τρόπο πρόσβασης στον πόρο, ακολουθούμενο από ένα παχύ έντερο και δύο πτέρυγες, ακολουθούμενη από μια διεύθυνση πρωτοκόλλου Internet ή ένα όνομα τομέα, ακολουθούμενη από προαιρετικό αριθμό κόλον και θύρας και τελειώνει με την πλήρη πορεία προς τον πόρο. Για παράδειγμα: http://www.enisa.europa.eu/@@search?SearchableText=enisa

- *Δρομολόγηση* : Η δρομολόγηση είναι η διαδικασία επιλογής καλύτερων διαδρομών μεταξύ δύο σημείων επικοινωνίας σε ένα δίκτυο. Οι διοικητικές περιγραφές της υπηρεσίας δρομολόγησης, οι οποίες αποκαλούνται συχνά "περιφερειακά μητρώα διαδικτύου" (π.χ. RIPE NCC, LACNIC, APNIC, ARIN, AfriNIC), οι λεγόμενοι αυτόνομα αριθμοί συστημάτων, σε οργανισμούς (π.χ.) που συμμετέχουν στο Διαδίκτυο.

- *Εφαρμογές: Η* επικοινωνία με εφαρμογές, όπως η ηλεκτρονική αλληλογραφία ή η μεταφορά αρχείων, βασίζεται σε πρωτόκολλα που υλοποιούνται από λογισμικό (π.χ. εκτελέσιμα προγράμματα) προκειμένου να παρέχουν μια υπηρεσία στους τελικούς χρήστες ή μηχανές.

- *Ασφάλεια:* Οι υπηρεσίες ασφαλείας αποσκοπούν στη διατήρηση της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας, της αυθεντικότητας και της μη αποθάρρυνσης.

Σκεύη, εξαρτήματα

Το υλικό ορίζεται ως φυσικά συστατικά των συστημάτων πληροφορικής, όπως μηχανές ή καλωδιώσεις. Χωρίς υλικό δεν μπορεί να εκτελεστεί λογισμικό ή να αποθηκευτούν πληροφορίες, επομένως το υλικό είναι ένα πολύτιμο στοιχείο. Για την υποδομή του Διαδικτύου ομαδοποιούνται σε τρεις κατηγορίες:

- *Συσκευές δικτύου: Ο* εξοπλισμός που διευκολύνει τη χρήση δικτύων υπολογιστών ονομάζεται συσκευές δικτύου. Για παράδειγμα, μετατρέπει τα πλαίσια προς τα εμπρός βάσει των διευθύνσεων του επιπέδου 2, οι δρομολογητές χρησιμοποιούν τις διευθύνσεις των επιπέδων 3 για την προώθηση των πακέτων, τα firewalls φιλτράρουν τα δεδομένα δικτύου βάσει προκαθορισμένων κανόνων και οι γέφυρες συνδυάζουν διαφορετικά τμήματα δικτύου.

- *Σέρβερ:* Ένας διακομιστής είναι ένα σύστημα υπολογιστή που παρέχει υπηρεσίες σε άλλους υπολογιστές ή χρήστες, εκτελώντας εκτελέσιμα προγράμματα.

- *Προσωπικά τερματικά:* Ένα προσωπικό τερματικό είναι μια ηλεκτρονική συσκευή υλικού που χρησιμοποιείται για την επικοινωνία με άλλα συστήματα υπολογιστών.

Ενδοσύνδεση

Δεδομένου ότι το Διαδίκτυο είναι ένα δίκτυο διαφορετικών μεγάλων δικτύων υπολογιστών, τα περιουσιακά στοιχεία που παρέχουν τη δυνατότητα διασύνδεσης είναι πολύτιμα. Δύο διαφορετικά είδη οργανώσεων μπορούν να οριστούν:

- *Γενικός πάροχος Διαδικτύου:* Ένας γενικός πάροχος Διαδικτύου είναι ένας οργανισμός που παρέχει υπηρεσίες για πρόσβαση στο Διαδίκτυο. Οι γενικοί πάροχοι Διαδικτύου μπορούν να οργανώνονται σε διάφορες μορφές, όπως εμπορικά, κοινοτικά, μη κερδοσκοπικά ή άλλως ιδιωτικά. Οι πάροχοι Διαδικτύου ειδικεύονται στο είδος των υπηρεσιών που παρέχουν: Οι χειριστές των κέντρων δεδομένων και οι παροχείς διακομιστών εκτελούν κέντρα δεδομένων και ενοικιάζουν χώρο ή διακομιστές αντίστοιχα. Οι πάροχοι πρόσβασης στο διαδίκτυο χρησιμοποιούν μια σειρά τεχνολογιών (π.χ. Wi-Fi, καλώδια από χαλκό ή ίνες) για τη σύνδεση χρηστών στο δίκτυό τους. Οι πάροχοι βάσεων δεδομένων συνήθως εκτελούν ένα μεγαλύτερο δίκτυο και παρέχουν σύνδεση στο Διαδίκτυο με παρόχους πρόσβασης στο διαδίκτυο, κέντρα δεδομένων και παρόχους διακομιστών.

- *Σημείο ανταλλαγής μέσω Διαδικτύου:* Ένα σημείο ανταλλαγής μέσω Διαδικτύου αποτελείται κατά κύριο λόγο από έναν ή περισσότερους διακόπτες για τη διασύνδεση διαφόρων παρόχων Διαδικτύου, προκειμένου να ανταλλάσσεται η διαδικτυακή κυκλοφορία μεταξύ των δικτύων τους.

Λογισμικό

Το λογισμικό είναι ένας γενικός όρος για συλλογές δεδομένων και οδηγιών ηλεκτρονικών υπολογιστών, προκειμένου να διαχειρίζεται πληροφορίες και να αποθηκεύει νέες

πληροφορίες, να παρέχει πρόσβαση σε πληροφορίες και να τις επεξεργάζεται. Το λογισμικό έχει ιδιαίτερη σημασία επειδή το υλικό είναι συχνά άχρηστο χωρίς λογισμικό και οι υπηρεσίες είναι χτισμένες πάνω από το λογισμικό. Το λογισμικό μπορεί να δομηθεί ως εξής:

- *Λειτουργικά συστήματα: Τα* λειτουργικά συστήματα παρέχουν τη βασική συνάρτηση των υπολογιστών που δεν σχετίζεται με τις εργασίες. Τα λειτουργικά συστήματα είναι υπεύθυνα για τον έλεγχο, την ενοποίηση και τη διαχείριση των επιμέρους στοιχείων υλικού ενός συστήματος υπολογιστών χρησιμοποιώντας τα προγράμματα οδήγησης συσκευών και το υλικολογισμικό, έτσι ώστε άλλα λογισμικά και χρήστες να μπορούν εύκολα να αλληλεπιδράσουν με το σύστημα.

- Οδηγός *συσκευών:* Ένα πρόγραμμα οδήγησης συσκευής είναι ένα πρόγραμμα υπολογιστή που λειτουργεί ή ελέγχει έναν συγκεκριμένο τύπο συσκευής που είναι συνδεδεμένος ή ενσωματωμένος σε έναν υπολογιστή, μιλώντας στο υλικολογισμικό της συσκευής. Τα προγράμματα οδήγησης συσκευών θεωρούνται συχνά ως μέρος ενός λειτουργικού συστήματος επειδή αλληλεπιδρούν στενά με αυτό.

- *Firmware:* Ο όρος firmware περιγράφει ένα συνδυασμό μόνιμης μνήμης, κωδικού προγράμματος και δεδομένων που είναι αποθηκευμένα μέσα σε αυτό. Η μόνιμη μνήμη είναι μέρος ενός συγκεκριμένου εξαρτήματος υλικού (π.χ. μια κάρτα γραμμής ενός δρομολογητή). Ένας οδηγός συσκευής συνήθως επικοινωνεί με το υλικολογισμικό μιας συγκεκριμένης συνιστώσας υλικού προκειμένου να τον ελέγχει ή να το διαχειρίζεται.

- *Εκτελέσιμα προγράμματα:* Ένα κομμάτι λογισμικού που έχει σχεδιαστεί για να εκπληρώσει έναν συγκεκριμένο σκοπό ονομάζεται εκτελέσιμο πρόγραμμα. Τα εκτελέσιμα προγράμματα απαιτούν ένα λειτουργικό σύστημα για να εκτελεστούν.

Υποδομή

Ο όρος υποδομή υποδηλώνει τις βασικές φυσικές δομές και εγκαταστάσεις (π.χ. κτίρια και καλώδια) που απαιτούνται για τη λειτουργία του Διαδικτύου. Προκειμένου να δημιουργηθεί ένα παγκόσμιο δίκτυο δικτύων, το λεγόμενο Διαδίκτυο, η υποστηρικτική υποδομή είναι ζωτικής σημασίας. Μπορεί να ομαδοποιηθεί ως εξής:

- *Καλωδίωση και σύνδεση: Τα* καλώδια και άλλοι σύνδεσμοι χρησιμοποιούνται για τη διασύνδεση συσκευών δικτύωσης ή δικτύων. Συνήθως, αυτές οι συνδέσεις είναι ενσύρματες ή ασύρματες συνδέσεις.

Διαφορετικοί τύποι συνδέσμων καλωδίων όπως ο χαλκός ή οι ίνες χρησιμοποιούνται ανάλογα με το εύρος ζώνης του δικτύου, το μέγεθος ή τις απαιτήσεις επιδόσεων και εξαρτώνται από περιβαλλοντικούς περιορισμούς όπως υποθαλάσσια καλώδια, υπόγεια

καλώδια ή καλώδια υπεράνω. Εάν η ανάπτυξη φυσικών συνδέσεων δεν είναι εφικτή ή αναποτελεσματική, μπορούν να χρησιμοποιηθούν ασύρματες συνδέσεις. Τέτοιες τεχνολογίες περιλαμβάνουν Wi-Fi, WiMAX ή LTE.

- *Κτίρια: Τα* κτίρια είναι εγκαταστάσεις που φιλοξενούν περιουσιακά στοιχεία όπως υλικό, λογισμικό και διασύνδεση. Αυτό κυμαίνεται από εγκαταστάσεις ειδικού σκοπού, όπως τα σημεία προσγείωσης όπου υποθαλάσσια καλώδια προσγειώνονται στην ξηρά, σε κέντρα δεδομένων πολλαπλών χρήσεων που χρησιμοποιούνται για την στέγαση όλων των ειδών υλικού και υποδομής.

- *Τροφοδοσία ρεύματος:* Ένα τροφοδοτικό είναι ένα σύστημα που τροφοδοτεί ηλεκτρική ενέργεια.

- *Συστήματα ψύξης:* Το σύστημα ψύξης ρυθμίζει τις ιδιότητες θερμοκρασίας και υγρασίας του αέρα, προκειμένου να διασφαλιστεί η σωστή λειτουργία των συστημάτων πληροφορικής.

- *Φυσική ασφάλεια: Η* φυσική ασφάλεια αναφέρεται σε μέτρα που απαγορεύουν την άνευ αδείας πρόσβαση στην υποδομή. Αυτά τα μέτρα περιλαμβάνουν αλλά δεν περιορίζονται σε φράχτες, τοίχους και πόρτες.

Πληροφορίες

Οι πληροφορίες είναι η αντίληψη που προκύπτει από τη συλλογή δεδομένων. Οι πληροφορίες αποτελούν πολύτιμο περιουσιακό στοιχείο, διότι τα συστήματα (π.χ. λογισμικό, υλικό, υπηρεσίες) και οι ανθρώπινοι πόροι εξαρτώνται από αυτό για τη λήψη λογικών αποφάσεων. Τα αναγνωρισμένα στοιχεία ενεργητικού ταξινομούνται ως εξής:

- *Απογραφή υλισμικού, λογισμικού, υποδομής, πληροφοριών:* μια λίστα αναλυτικών πληροφοριών σχετικά με το υλικό, το λογισμικό, τα στοιχεία της υποδομής και τις σημαντικές πληροφορίες, όπως διαμορφώσεις. Οι λεπτομερείς πληροφορίες ενδέχεται να περιέχουν την έκδοση του στοιχείου, τον τόπο στον οποίο βρίσκεται και τα τιμολόγια, αλλά δεν περιορίζονται σε αυτό.

- *Ιστορικές πληροφορίες / στατιστικές:* Ιστορικές πληροφορίες είναι πληροφορίες που συλλέχθηκαν στο παρελθόν και είναι προσβάσιμες στο παρόν. Ορισμένα είδη ιστορικών πληροφοριών μπορούν να συλλέγονται μόνο σύμφωνα με το νόμο, συλλέγονται και άλλα είδη προκειμένου να δημιουργηθούν στατιστικά στοιχεία σχετικά με θέματα όπως η χρήση ή ποιος έχει πρόσβαση στον πόρο.

- *Προσαρμοσμένες πληροφορίες: Η* προσπάθεια προσδιορισμού των τάσεων στις πληροφορίες που συλλέγονται συχνά χρησιμοποιείται για την πρόβλεψη του μέλλοντος με βάση παρελθόντα γεγονότα ή συμπεριφορές.

- *Τοπολογία δικτύου:* Η τοπολογία δικτύου είναι η διάταξη διαφόρων εξαρτημάτων (π.χ. δρομολογητές, διακόπτες, τείχη προστασίας, διακομιστές) ενός δικτύου υπολογιστών. Τέτοιες λεπτομέρειες μπορούν να κατατεθούν ως χάρτες δικτύου ή πίνακες δρομολόγησης.

- *Διαμόρφωση συστήματος:* Η διαμόρφωση συστήματος περιγράφει τον τρόπο διαμόρφωσης, σύνδεσης και διαλειτουργικότητας διαφόρων στοιχείων (π.χ. λογισμικού, υλικού) ενός συστήματος (π.χ. λογισμικό, υλικό, υπηρεσίες) προκειμένου να επιτευχθεί συγκεκριμένος στόχος. Για παράδειγμα, οι διευθύνσεις MAC και IP του δρομολογητή ρυθμίζουν το υποσύστημα δικτύου.

- *Λειτουργικές πληροφορίες: Οι* πληροφορίες που απαιτούνται για τη λειτουργία ενός συστήματος ονομάζονται λειτουργικές πληροφορίες. Οι λειτουργικές πληροφορίες περιλαμβάνουν την κατάσταση ενός συστήματος, τα μέτρα για ορισμένες μετρήσεις, τα γεγονότα όταν αλλάζει η κατάσταση ενός συστήματος, προειδοποιούνται όταν επιτυγχάνεται συγκεκριμένο όριο για συγκεκριμένη μέτρηση και πληροφορίες σχετικά με ελλείψεις ή διαταραχές.

- *Πιστοποιητικά:* Μια πιστοποίηση είναι μια βεβαίωση εξουσιοδότησης που εκδίδεται σε μια μηχανή ή ένα άτομο από τρίτο μέρος. Μπορεί να είναι φυσικά, όπως κλειδιά και διαβατήρια, ή εικονικά (π.χ. ονόματα χρήστη και κωδικοί πρόσβασης, PIN).

- *Πολιτικές δικαιωμάτων χρήστη:* Οι πολιτικές δικαιωμάτων χρήστη καθορίζουν τα δικαιώματα των ομάδων χρηστών (π.χ. διαχειριστές, χειριστές) σε ορισμένες πληροφορίες (όπως συστήματα υπολογιστών, εκτελέσιμα προγράμματα, πληροφορίες).

- *Νόμιμη παρακολούθηση: Η* νόμιμη παρακολούθηση επιτυγχάνει πρόσβαση σε δεδομένα δικτύου επικοινωνιών σύμφωνα με νόμιμη εξουσιοδότηση για σκοπούς ανάλυσης, αποδείξεων ή επιτήρησης.

Ανθρώπινο δυναμικό

Αυτή η ενότητα ορίζει το προσωπικό που θεωρείται σημαντικό πλεονέκτημα της υποδομής του Διαδικτύου όσον αφορά τις δεξιότητες και τις ικανότητες.

- *Διαχειριστές:* Ένα άτομο που είναι υπεύθυνο για τη ρύθμιση, τη διαμόρφωση, την παρακολούθηση και τη συντήρηση ενός συστήματος (π.χ. διακομιστή, δρομολογητή).

- *Χειριστές:* Ένα άτομο ή μια εταιρεία που τρέχει λογισμικό, μηχανήματα ή συστήματα.

- *Ομάδα υποστήριξης* : Ένα άτομο ή μια ομάδα που παρέχει βοήθεια σχετικά με τη χρήση, τη διαμόρφωση ή την ανίχνευση σφαλμάτων ενός συστήματος ή μιας υπηρεσίας.

- *Προγραμματιστές:* Πρόσωπο που ασχολείται με την έρευνα, το σχεδιασμό, την υλοποίηση και τη δοκιμή συστημάτων ή λογισμικού.

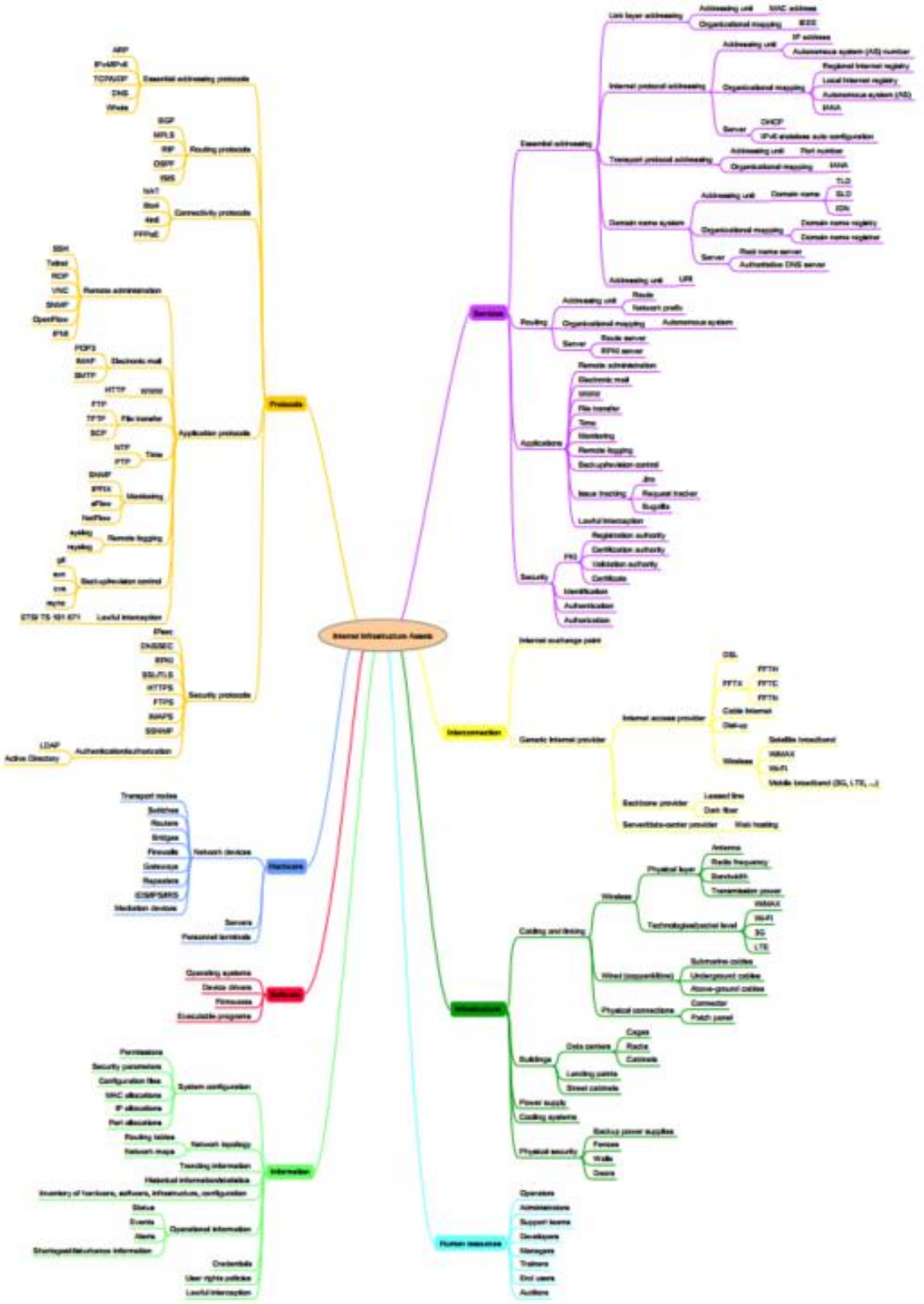
- *Διαχειριστές:* Ένα άτομο που είναι υπεύθυνο για τον έλεγχο ή τη διοίκηση ενός οργανισμού ή μιας ομάδας προσωπικού (π.χ. διαχειριστές, φορείς εκμετάλλευσης, προγραμματιστές).

- *Εκπαιδευτές:* Πρόσωπο που εκπαιδεύει άλλο άτομο σε συγκεκριμένο θέμα.

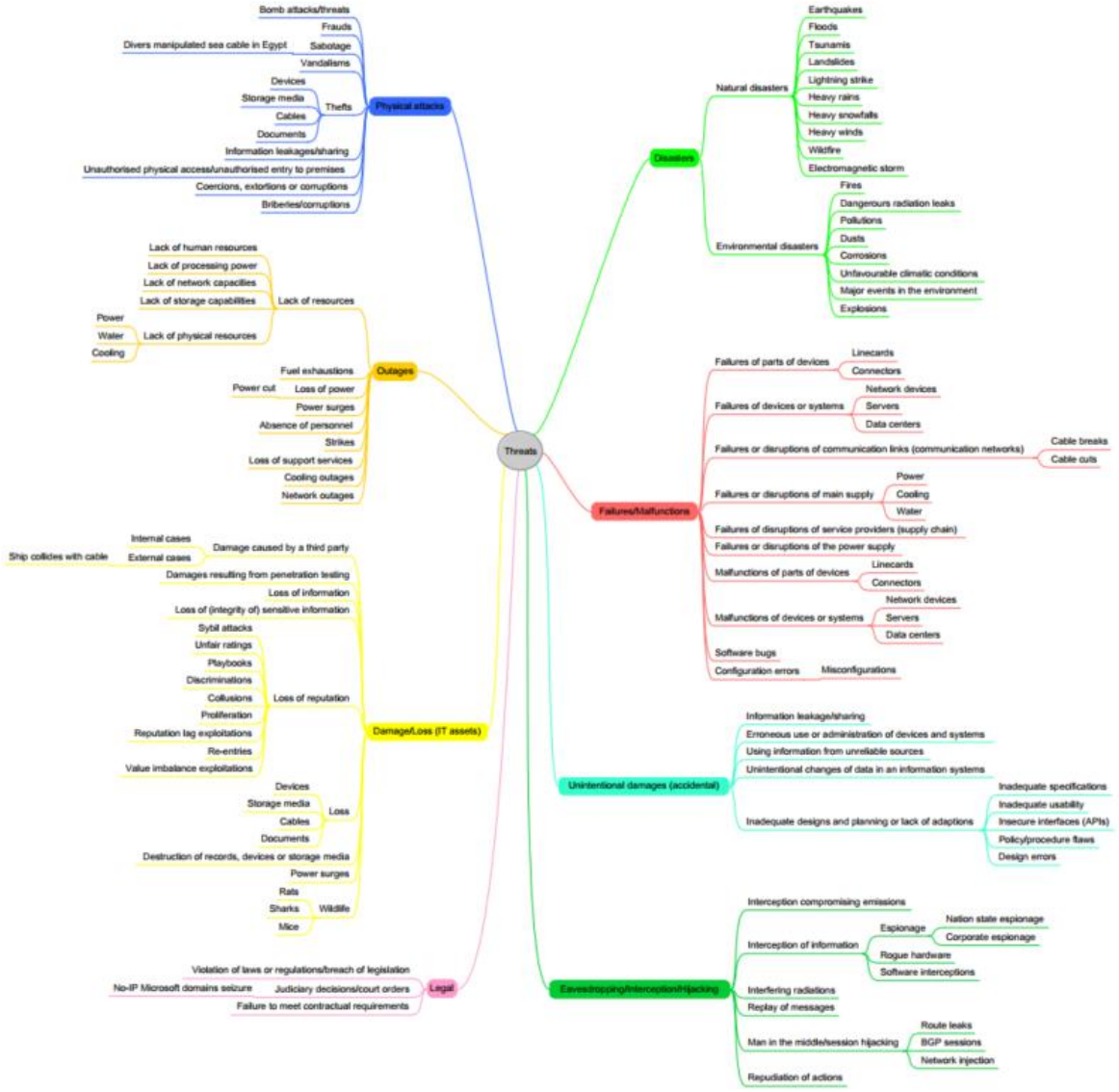
- *Ελεγκτές:* Ένα άτομο που επικυρώνει και επαληθεύει ότι ένα άτομο, διαδικασία ή σύστημα συμπεριφέρεται, εκτελείται ή χρησιμοποιείται σε ένα περιβάλλον όπως ορίζεται προηγουμένως.

- *Τελικοί χρήστες:* Ένα άτομο που χρησιμοποιεί ένα συγκεκριμένο προϊόν ή υπηρεσία.

Παράρτημα Β Λεπτομερής χαρτογράφος μυαλού για στοιχεία υποδομής διαδικτύου



Παράρτημα Γ Ανησυχίες Χάρτης



Παράρτημα Δ: Σύνδεση μεταξύ απειλών και περιουσιακών στοιχείων

Τύποι απειλών	Απειλές	Τύποι περιουσιακών στοιχείων
Φυσικές επιθέσεις		
	Επιδρομή βόμβας / απειλές	Hardware, Υποδομές, Ανθρώπινοι πόροι
	Απάτη	Ανθρώπινο δυναμικό
	Σαμποτάζ	Υλικό, Υποδομή
	Βανδαλισμός	*Ομοια*
	Κλοπές	*Ομοια*
	Διαρροές πληροφοριών / κοινή χρήση	Πληροφορίες, Υποδομές, Διασύνδεση
	Μη εξουσιοδοτημένη φυσική πρόσβαση / μη εξουσιοδοτημένες καταχωρήσεις σε χώρους	Υλικό, Υποδομή
	Εγκλήματα, εκβιασμοί ή διαφθορά	Υλικό, Υποδομή
	Δωροδοκίες / διαφθορά	Ανθρώπινο δυναμικό
Καταστροφές		
	Φυσικές καταστροφές	Hardware, Λογισμικό, Πληροφορίες, Υπηρεσίες, Διασύνδεση, Υποδομή, Ανθρώπινο πόροι
	Περιβαλλοντικές καταστροφές	*Ομοια*
Βλάβες / Βλάβες		
	Αποτυχίες μερών συσκευών	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Αποτυχίες συσκευών ή συστημάτων	*Ομοια*

	Αποτυχίες ή διακοπές δικτύου επικοινωνιών (επικοινωνία δίκτυα)	Ομοια
	Αποτυχίες ή διακοπές λειτουργίας της κύριας παροχής	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες, διασύνδεση, υποδομή
	Αδυναμίες διακοπών των παρόχων υπηρεσιών (αλυσίδα εφοδιασμού)	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Αποτυχίες ή διακοπές του τροφοδοτικού	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες, διασύνδεση, υποδομή
	Δυσλειτουργίες μερών συσκευών	*Ομοια*
	Δυσλειτουργίες συσκευών ή συστημάτων	Ομοια
	Σφάλματα λογισμικού	Πρωτόκολλα, λογισμικό, πληροφορίες, υπηρεσίες
	Σφάλματα διαμόρφωσης	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
Διακοπές		
	Ελλειψη πηγών	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες, Διασύνδεση, Υποδομές, Ανθρώπινοι πόροι
	Εξάντληση καυσίμου	Hardware, Υποδομές, Ανθρώπινοι πόροι
	Απώλεια ισχύος	*Ομοια*
	Ισχύς	*Ομοια*
	Απουσία προσωπικού	*Ομοια*
	Απεργίες	Ανθρώπινο δυναμικό

	Διακοπές δικτύου	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Διακοπή ψύξης	Υλικό, Υποδομή
Αθέλητες ζημιές (τυχαίες)		
	Διαρροή πληροφοριών / κοινή χρήση	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες, διασύνδεση
	Λανθασμένη χρήση ή διαχείριση συσκευών και συστημάτων	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Χρήση πληροφοριών από αναξιόπιστες πηγές	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Μη ακούσια αλλαγή δεδομένων σε ένα σύστημα πληροφοριών	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Ανεπαρκής σχεδιασμός και σχεδιασμός ή έλλειψη προσαρμογών	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες, διασύνδεση, υποδομή
Ζημιές / Απώλειες (στοιχεία ενεργητικού)		
	Ζημία που προκλήθηκε από τρίτους	Hardware, Λογισμικό, Πληροφορίες, Υπηρεσίες, Διασύνδεση, Υποδομή, Ανθρώπινο πόροι
	Ζημιές που προκύπτουν από δοκιμές διείσδυσης	Λογισμικό, πληροφορίες, υπηρεσίες
	Απώλεια	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, Υπηρεσίες, Διασύνδεση, Υποδομές, Ανθρώπινοι πόροι
	Απώλεια φήμης	Διασύνδεση, Ανθρώπινοι πόροι
Αφηρημένη δραστηριότητα /		

Κατάχρηση		
	Κλοπή ταυτότητας (απάτη / λογαριασμός ταυτότητας ή αεροπειρατεία υπηρεσίας)	Hardware, Λογισμικό, Πληροφορίες, Υπηρεσίες, Υποδομές, Ανθρώπινοι πόροι
	Μη ζητηθέντα μηνύματα ηλεκτρονικού ταχυδρομείου	Hardware, Λογισμικό, Υπηρεσίες
	Malware και ιούς	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Πιθανώς ανεπιθύμητο λογισμικό	*Ομοια*
	Κατάχρηση διαρροών πληροφοριών	*Ομοια*
	Συμβιβασμός εμπιστευτικών πληροφοριών (παραβιάσεις δεδομένων)	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Δημιουργία και χρήση αδίστακτων πιστοποιητικών	Hardware, Λογισμικό, Πληροφορίες, Υπηρεσίες, Ανθρώπινοι πόροι
	Χειρισμός υλικού και λογισμικού	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Χειρισμός πληροφοριών	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες, διασύνδεση, υποδομή, ανθρώπινο πόροι
	Κατάχρηση πληροφοριακών / πληροφοριακών συστημάτων	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, υπηρεσίες, διασύνδεση
	Κατάχρηση των αδειών	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, Υπηρεσίες, Διασύνδεση, Υποδομές, Ανθρώπινοι πόροι
	Κατάχρηση προσωπικών	Ανθρώπινο δυναμικό

	δεδομένων	
	Μη εξουσιοδοτημένες δραστηριότητες	Πρωτόκολλα, υλικό, λογισμικό, πληροφορίες, Υπηρεσίες, Διασύνδεση, Υποδομές, Ανθρώπινοι πόροι
	Επιθέσεις άρνησης εξυπηρέτησης (DoS / DDoS)	Υλικό, λογισμικό, πληροφορίες, υπηρεσίες
	Χρονοδιαγράμματα	*Ομοια*
	Κοινωνική μηχανική	Ανθρώπινο δυναμικό
	Προβλεπόμενη ομοιότητα των αναγνωριστικών	Πληροφορίες, Υπηρεσίες
	Απομακρυσμένες δραστηριότητες (εκτέλεση)	Λογισμικό, πληροφορίες, υπηρεσίες
	Εκμετάλλευση σφαλμάτων λογισμικού	Πρωτόκολλα, λογισμικό, πληροφορίες, υπηρεσίες
	Ωμής βίας	*Ομοια*
Υποκλοπή / Παρακολούθηση / Σφαγή		
	Υποκλοπή συμβιβασμού εκπομπών	Πρωτόκολλα, λογισμικό, πληροφορίες, υπηρεσίες
	Υποκλοπή πληροφοριών	Πρωτόκολλα, λογισμικό, πληροφορίες, υπηρεσίες
	Παρενέργειες ακτινοβολίας	Hardware, Διασύνδεση, Υποδομές, Ανθρώπινοι πόροι
	Αναπαραγωγή μηνυμάτων	Λογισμικό, πληροφορίες, υπηρεσίες
	Άνθρωπος στη μεσολάβηση / απόπειρα αεροπειρατεία	Λογισμικό, πληροφορίες, υπηρεσίες
	Καταγγελία ενεργειών	Διασύνδεση, Ανθρώπινοι πόροι
Νομικός		
	Παραβιάσεις νόμων ή	Λογισμικό, Πληροφορίες,

	κανονιστικών ρυθμίσεων / παραβιάσεις της νομοθεσίας	Διασύνδεση, Ανθρώπινοι πόροι
	Δικαστικές αποφάσεις / δικαστικές αποφάσεις	*Ομοια*
	Μη τήρηση των συμβατικών απαιτήσεων	*Ομοια*

Παράρτημα Ε Λεπτομέρειες απειλής

Ο παρών πίνακας βασίζεται σε ένα εργαλείο γενικού σκοπού του ENISA για την καταγραφή μιας ταξινόμησης απειλών και σχετικών λεπτομερειών απειλής.

Ομάδες απειλών	Απειλή	Λεπτομέρειες απειλής	Πράκτορες απειλής	Τάση	Σχόλια, παραδείγματα
Φυσικές επιθέσεις					
	Επιδρομή βόμβας / απειλές		Κυβερνητικοί τρομοκράτες, υπάλληλοι, έθνη, εγκληματίες στον κυβερνοχώρο		
	Απάτες		Κυβερνητικοί τρομοκράτες, υπάλληλοι, εγκληματίες του κυβερνοχώρου, εταιρείες		
	Σαμποτάζ		Κυβερνητικοί τρομοκράτες, υπάλληλοι, εταιρείες, έθνη		
	Βανδαλισμός		Υπάλληλοι, εγκληματίες του κυβερνοχώρου		
	Κλοπές	Κλοπή της φυσικής ιδιοκτησίας της εταιρείας, όπως όπως και συσκευές, μέσα ενημέρωσης,	Υπάλληλοι, εγκληματίες του κυβερνοχώρου	Αύξηση	

		ή έγγραφα.			
	Διαρροές πληροφοριών / κοινή χρήση		Εργαζόμενοι, εταιρίες	Αύξηση	
	Μη εξουσιοδοτημένη φυσική πρόσβαση / μη εξουσιοδοτημένες καταχωρήσεις σε χώρους		Ομοια		
	Εγκλήματα, εκβιασμοί ή διαφθορά		Κυβερνητικοί τρομοκράτες, εγκληματίες του κυβερνοχώρου, υπάλληλοι, εταιρείες, έθνος κράτη μέλη		
	Δωροδοκίες / διαφθορά		Ομοια		

Ομάδες απειλών	Απειλή	Λεπτομέρειες απειλής	Πράκτορες απειλής	Τάση	Σχόλια, παραδείγματα
Καταστροφές					
	Φυσικές καταστροφές				
		Σεισμοί			
		Πλημμύρες			
		Κατοικίες			
		Αστραπή			

		Καταρρακτώδεις βροχές			
		Βαρύ χιονόπτωση			
		Βαρύς άνεμοι			
		Υγρό πύρ			
		Ηλεκτρομαγνητική καταιγίδα			
	Περιβαλλοντικές καταστροφές				
		Πυρκαγιές			
		Επικίνδυνες διαρροές ακτινοβολίας			
		Ρύπανση			
		Σκόνη			
		Διάβρωση			
		Μη ευνοϊκές κλιματολογικές συνθήκες			
		Σημαντικά γεγονότα στο περιβάλλον			
		Εκρήξεις			
Βλάβες / Βλάβες			Εργαζόμενοι, εταιρίες		
	Αποτυχίες μερών συσκευών				
	Αποτυχίες συσκευών ή συστημάτων				

Ομάδες απειλών	Απειλή	Λεπτομέρειες απειλής	Πράκτορες απειλής	Τάση	Σχόλια, παραδείγματα
	Αποτυχίες ή διαταραχές της επικοινωνίας συνδέσεις (δίκτυα επικοινωνίας)				
	Αποτυχίες ή διακοπές λειτουργίας της κύριας παροχής				
	Αδυναμίες διακοπών των παρόχων υπηρεσιών (αλυσίδα εφοδιασμού)				
	Αποτυχίες ή διακοπές του τροφοδοτικού				
	Δυσλειτουργίες μερών συσκευών				
	Δυσλειτουργίες συσκευών ή συστημάτων				
	Σφάλματα λογισμικού				
	Σφάλματα διαμόρφωσης	Ψευδής, ανεπαρκής ή ανασφαλής διαμόρφωση των συστημάτων, που αναφέρεται επίσης ως λανθασμένη διαμόρφωση .			Οι λανθασμένες τοποθεσίες Apache εκθέτουν [...] ιδιωτικά δεδομένα.
Διακοπές					
	Ελλειψη πηγών	Έλλειψη φυσικών πόρων καθώς και	Εργαζόμενοι, εταιρίες		

		δυναμικό επεξεργασίας, χωρητικότητα δικτύου ή ανθρώπινοι πόροι.			
	Εξάντληση καυσίμου		Ομοια		
	Απώλεια ισχύος		Οι τρομοκράτες του κυβερνοχώρου, οι online κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, οι υπάλληλοι, εταιρίες, έθνη		
	Ισχύς		Ομοια		
	Απουσία προσωπικού		Εργαζόμενοι, εταιρίες		
	Απεργίες		Υπαλλήλους		
	Διακοπές δικτύου		Οι τρομοκράτες του κυβερνοχώρου, οι online κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι		

			εγκληματίες στον κυβερνοχώρο, οι υπάλληλοι, εταιρίες, έθνη		
	Διακοπή ψύξης		Ομοια		
Αθέλητες ζημιές (τυχαίος)			Εργαζόμενοι, εταιρίες	Αύξηση	
	Διαρροή πληροφοριών / κοινή χρήση			Αύξηση	
	Λανθασμένη χρήση ή διαχείριση συσκευών και συστημάτων				
	Χρήση πληροφοριών από αναξιόπιστες πηγές				
	Μη ακούσια αλλαγή δεδομένων σε ένα σύστημα πληροφοριών				
	Ανεπαρκής σχεδιασμός και σχεδιασμός ή έλλειψη προσαρμογών	Ο ανεπαρκής σχεδιασμός περιλαμβάνει ανεπαρκή προδιαγραφές, χρηστικότητα και προκύπτοντα ανασφαλείς API ή σφάλματα σχεδίασης .			
Ζημιές / Απώλειες				Αύξη	

(στοιχεία ενεργητικού)				ση	
	Ζημία που προκλήθηκε από τρίτους		Οι τρομοκράτες του κυβερνοχώρου, οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, εθνικά κράτη		
	Ζημιές που προκύπτουν από δοκιμές διείσδυσης		Εταιρείες		
	Απώλεια	Απώλεια της ιδιοκτησίας της εταιρείας, όπως συσκευές, μέσα ενημέρωσης, εξουσία ή έγγραφα. Περιλαμβάνει απώλεια πληροφοριών.	Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, kiddie script, εγκληματίες στον κυβερνοχώρο, υπάλληλοι, εταιρείες, έθνη	Αύξηση	Οραματισμός. Έκθεση έρευνας παραβίασης δεδομένων Verizon 2014 . Ανατομία μιας παραβίασης δεδομένων

	Απώλεια φήμης	Η απώλεια της φήμης περιλαμβάνει επιθέσεις κατά της απώλειας και ακούσιας απώλειας ή ακόμα και άξιου. (Επιθέσεις Sybil, διακρίσεις, βαθμολογίες, συμπαιγνία, πολλαπλασιασμός ή επανεισαγωγή)	Οι τρομοκράτες του κυβερνοχώρου, οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες του κυβερνοχώρου, οι υπάλληλοι, οι εταιρείες, τα έθνη		
Αφηρημένη δραστηριότητα / Κατάχρηση					
	Ταυτότητα κλοπή (απάτη ταυτότητας / λογαριασμού ή την υπηρεσία σύνοδο αεροπειρατεία)		Οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, εμπιστευτικές, εθνικά	Αύξηση	

			κράτη		
	Μη ζητηθέντα μηνύματα ηλεκτρονικού ταχυδρομείου		Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, παιδικά σενάρια, εγκληματίες στον κυβερνοχώρο	Αύξηση	
	Malware και ιούς	Τα κακόβουλα προγράμματα μπορούν να ταξινομηθούν περαιτέρω σε ομάδες όπως ο ιός, ο ιός τύπου worm, ο trojan, το rootkit, τα botnets, το spyware, το scareware ή το rogueware.	Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, ιστορικοί, εγκληματίες στον κυβερνοχώρο, έθνη	Αύξηση	TDL / TDL4 / TDSS κακόβουλο λογισμικό (ιός, trojan, rootkit, botnet) μαζική μόλυνση κακόβουλου λογισμικού υψηλού επιπέδου Κιτ εκμετάλλευσης Blackhole Java vulnerabilities εκμεταλλεύονται για εισβολή σε ~ 90% των λοιμώξεων
	Πιθανώς ανεπιθύμητο λογισμικό	Έχει, σε αντίθεση με το	Οι διαδικτυακοί κοινωνικοί		

		κακόβουλο λογισμικό, νόμιμη λειτουργία για να αποκρύψει	χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο,		
		πραγματικούς στόχους. Εγκαταστήθηκε ακούσια, περιλαμβάνει adware και greyware.	υπαλλήλους		
	Κατάχρηση διαρροών πληροφοριών		Οι τρομοκράτες του κυβερνοχώρου, οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, δηλώνουν τα έθνη	Αύξηση	
	Συμβιβασμός εμπιστευτικών πληροφοριών (παραβιάσεις δεδομένων)		Οι τρομοκράτες του κυβερνοχώρου, οι διαδικτυακοί	Αύξηση	

			κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, κράτη μέλη, οι υπάλληλοι		
	Δημιουργία και χρήση αδίστακτων πιστοποιητικών	Διείσδυση SSL CA ή πιστοποιητικά SSL που εκδόθηκαν εσφαλμένα.	Οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, οι επιχειρήσεις, τα έθνη δηλώνουν		
	Χειρισμός υλικού και λογισμικού		Οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, οι επιχειρήσεις, τα έθνη δηλώνουν		

	Χειρισμός πληροφοριών		Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, παιδικά σενάρια, εγκληματίες του κυβερνοχώρου, υπάλληλοι, εταιρείες, έθνη κράτη μέλη		
		Παραποίηση εγγραφών			
		Επεξεργασία τραπέζης δρομολόγησης		Αύξηση	Indosat διαρροή δρομολόγησης που περιλαμβάνει> 320k μη ινδονησιακές διαδρομές BGP. Για ορισμένα προθέματα Akamai (δίκτυα), ο υποδοχέας Indosat hi ήταν ουσιαστικά πλήρης Η έναρξη της κυκλοφορίας ήταν σίγουρα ένα καυτό

					θέμα το 2013. Περίπου 1500 ατομικές IP έχουν μπλοκάρει τετράγωνα, σε διαρκή γεγονότα

Ομάδες απειλών	Απειλή	Λεπτομέρειες απειλής	Πράκτορες απειλής	Τάση	Σχόλια, παραδείγματα
		Διακίνηση DNS		Μειώνοντας	Επίθεση του DNS Κατευτική επίθεση Προστασία των επιθέσεων δηλητηρίασης DNS cache Η παράπλευρη ζημιά του Internet censorship από την ένεση DNS
		Παραποίηση της διαμόρφωσης			
		Ως χειραγώγηση			Χειρισμός αριθμών AS ή το ίδιο το σύστημα αρίθμησης.
	Κατάχρηση πληροφοριακών / πληροφοριακών συστημάτων		Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, παιδικά σενάρια, εγκληματίες		

			του κυβερνοχώρου, υπάλληλοι, εταιρείες, έθνος κράτη μέλη		
	Κατάχρηση των αδειών		Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, νεογέννητοι σεναρίου, εγκληματίες στον κυβερνοχώρο, υπάλληλοι		
	Κατάχρηση προσωπικών δεδομένων		Ομοια		
	Μη εξουσιοδοτημένες δραστηριότητες		Υπαλλήλους		
		Μη εξουσιοδοτημένη χρήση της διαχείρισης συσκευών και συστημάτων			
		Μη εξουσιοδοτημένη πρόσβαση στο σύστημα πληροφοριών / δίκτυο			
		Μη εξουσιοδοτημένες αλλαγές στα			

		αρχεία			
		Μη εξουσιοδοτημένη εγκατάσταση λογισμικού			
		Μη εξουσιοδοτημένη χρήση λογισμικού			
	Αρνηση του υπηρεσία επιθέσεις (DoS / DDoS)		Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, παιδικά σενάρια, εγκληματίες στον κυβερνοχώρο	Αύξηση	Το 41% όλων των οργανώσεων υπέστη παγκόσμια επίθεση DDoS κατά το τελευταίο έτος Πολλοί ανταποκριτές αναφέρουν πολύ μεγάλες επιθέσεις DDoS πάνω από το όριο των 100Gbps. Οι επιθέσεις στρώματος εφαρμογής εμφανίστηκαν από σχεδόν όλοι οι ερωτηθέντες. Επιθέσεις που στοχεύουν
					κρυπτογραφημένες υπηρεσίες Web (HTTPS) - αύξηση 17% σε σχέση με πέρυσι Αύξηση κατά 18% των συνολικών επιθέσεων DDoS (Q1 2014 έως Q4 2013). 39% αύξηση του μέσου εύρους ζώνης επίθεσης. 35% αύξηση των

					επιθέσεων υποδομής (επίπεδο 3 + 4). 114% αύξηση του μέσου εύρους ζώνης αιχμής. 36% μείωση στις επιθέσεις εφαρμογής (στρώμα 7). 24% μείωση της μέσης διάρκειας ζωής: 23 έναντι 17 ωρών. Στο 1ο τρίμηνο του 2014, το 41% των παρατηρούμενων επιθέσεων προέρχεται από την Κίνα (σε σύγκριση με 43% το 4ο τρίμηνο του 2013). Το Universal Plug & Play (UPnP) είναι το νέο διάσημο λιμάνι προσβολής (12% της κίνησης επίθεσης). Μικρή μείωση του αριθμού των επιθέσεων σε σύγκριση με το 4ο τρίμηνο του 2013: 283 (μείωση κατά 20%), αλλά αύξηση κατά 27% σε σύγκριση με το πρώτο τρίμηνο του 2013 Ένας από τους μεγαλύτερους ιστότοπους του Παγκοσμίου Ιστού που σπάει: Ενεργοποιεί τους επισκέπτες σε "Zombies DDoS"

		Ενταση ΗΧΟΥ			CloudFlare 400 Gbps N TP Επιπρόσθετη επίθεση DDoS Επαναλαμβανόμενες επιθέσεις έπληξαν τα δύο τρίτα των θυμάτων DDoS. Οι επιθέσεις ενίσχυσης DDoS εξακολουθούν να αποτελούν τρομακτική πρόκληση. Αύξηση κυβερνητικών στόχων, μείωση των τραπεζικών στόχων. Αύξηση των νόμιμων στόχων διακομιστή παιχνιδιών στο διαδίκτυο
		Εφαρμογή			
		Εκμετάλλευση πρωτοκόλλου			
		Παραπλανητική επίθεση πακέτων			
	Χρονοδιαγράμματα				
		Σάρωση / αισθητήρας μεγάλης κλίμακας	Οι σε απευθείας σύνδεση κοινωνικοί χάκερ, hacktivists, τα παιδικά σενάρια, τους εγκληματίες στον κυβερνοχώρο, τις εταιρείες, τα	Αύξηση	

			έθνη		
		Στοχευμένες επιθέσεις / προχωρημένες απειλές	Οι σε απευθείας σύνδεση κοινωνικοί χάκερ, hacktivists, παιδιού σεναρίου, εγκληματίες στον κυβερνοχώρο, έθνη	Σταθερός	
	Κοινωνική μηχανική		Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, παιδικά σενάρια, εγκληματίες στον κυβερνοχώρο		Κοινωνική μηχανική: Η τέχνη της ανθρώπινης πειρατείας
		Phishing		Αύξηση	
		Πρόβλεψη / εξαπάτηση			
	Προβλεπόμενη ομοιότητα των αναγνωριστικών		Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, παιδικά σενάρια, εγκληματίες στον κυβερνοχώρο		
		Σύγκρουση ονόματος τομέα			Ν AME Σύγκρουση στο DNS

		Τιμολόγηση, καταγραφή κοινών τομέων τύπων			Typosquatting - τι συμβαίνει όταν πληκτρολογείτε λάθος ένα όνομα ιστότοπου;
	Απομακρυσμένες δραστηριότητες (εκτέλεση)		Οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, εθνικά κράτη		
	Εκμετάλλευση σφαλμάτων λογισμικού		Ομοια		
		Σφάλμα πυρήνα			
		Σφάλμα σχεδιασμού			
		Έλεγχος υπερχείλισης buffer			
		Κατάσταση του αγώνα			
		Ανεπαρκής επικύρωση		Αύξηση	
	Ωμής βίας	Μια μέθοδος δοκιμής και σφάλματος που χρησιμοποιείται για τη λήψη πληροφοριών, όπως τα διαπιστευτήρια σύνδεσης,	Ομοια		Οι βίαιες επιθέσεις του RDP εξαρτώνται από τα λάθη μας Kaspersky: Οι σε απευθείας σύνδεση κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια

		αυτοματοποιημένο λογισμικό χρησιμοποιείται για τη δημιουργία ενός μεγάλου αριθμού διαδοχικών εικασιών ως προς την αξία των επιθυμητών δεδομένων.			προσπαθούν να αναλάβουν τους υπολογιστές να εκτελέσουν ning remote desktop λογισμικό
Υποκλοπή /Διακοπή /Αεροπειρατεία					
	Υποκλοπή συμβιβασμού εκπομπών		Οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, εταιρίες, έθνη		
	Υποκλοπή πληροφοριών	Υποκλοπή πληροφοριών μέσω κατασκοπείας, υλικού αδίστακτων ή άμεσης παρακολούθησης	Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, kiddie script, εγκληματίες στον κυβερνοχώρο,		Ο Snowden λέει ότι η NSA Eng βρίσκεται σε βιομηχανική κατασκοπία Η GCHQ και η NSA είναι υπόχρεες στις ιδιωτικές γερμανικές

		λογισμικού.	υπάλληλοι, εταιρείες, έθνη		εταιρείες
	Παρενέργειες ακτινοβολίας		Κυβερνητικοί τρομοκράτες, εταιρείες, έθνη		
	Αναπαραγωγή μηνυμάτων		Οι διαδικτυακοί κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, υπαλλήλους		
	Ανδρας σε ο Μέση / απόπειρα αεροπειρατεία	Παραδείγματα είναι διαρροές διαδρομής ή αεροπειρατείες BGP.	Διαδικτυακοί κοινωνικοί χάκερ, hacktivists, παιδικά σενάρια, εγκληματίες στον κυβερνοχώρο, εταιρείες, έθνη		NANOG49 μιλούν Πρακτικές άμυνες κατά της αεροπειρατείας του BGP
	Καταγγελία ενεργειών		Οι τρομοκράτες του κυβερνοχώρου, οι online κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια , οι εγκληματίες		

			στον κυβερνοχώρο, οι υπάλληλοι, εταιρίες, έθνη		
Νομικός					
	Παραβάσεις του νόμος ή ρύθμιση / παραβιάσεις της νομοθεσίας		Οι τρομοκράτες του κυβερνοχώρου, οι online κοινωνικοί χάκερ, οι hacktivists, τα παιδικά σενάρια, οι εγκληματίες στον κυβερνοχώρο, οι υπάλληλοι, εταιρίες, έθνη		
	Δικαστικές αποφάσεις / δικαστικές αποφάσεις		Τα εθνικά κράτη		
	Αποτυχία προς την πληρούν τις συμβατικές απαιτήσεις		Εργαζόμενοι, εταιρίες		

Παράρτημα ΣΤ Λεπτομέρειες καλών πρακτικών

Απειλές δρομολόγησης

Ως αεροπειρατεία:

- Χρησιμοποιήστε την πιστοποίηση πόρων (RPKI) για την επικύρωση της προέλευσης AS. Ειδικότερα, το RPKI χρησιμοποιείται για τη διασφάλιση του BGP μέσω του BGP Sec.

Διέλευση χώρου διευθύνσεων (προθέματα IP):

- Χρησιμοποιήστε την πιστοποίηση πόρων (RPKI) για την επικύρωση της προέλευσης AS. Ειδικότερα, το RPKI χρησιμοποιείται για τη διασφάλιση του BGP μέσω του BGP Sec.

- Καθορίστε μια πολιτική κατάλληλης χρήσης (AUP) όπως εξηγείται στο BCP 46, το οποίο προωθεί τους κανόνες για την εξασφάλιση της peering [115].

- Καθιέρωση φίλτρου εισόδου από την περιοχή άκρη στο Internet .

- Καθιέρωση προώθησης Unicast Reverse Path για επιβεβαίωση της εγκυρότητας μιας διεύθυνσης IP προέλευσης .

- Δημιουργήστε φιλτράρισμα εξόδου στο οριακό δρομολογητή για να φιλτράρετε προορατικά όλη την κυκλοφορία που πηγαίνει στον πελάτη που έχει διεύθυνση προέλευσης οποιασδήποτε από τις διευθύνσεις που έχουν εκχωρηθεί σε αυτόν τον πελάτη .

- Φιλτράρετε τις ανακοινώσεις δρομολόγησης και εφαρμόστε τεχνικές που μειώνουν τον κίνδυνο υπερβολικής φόρτωσης στη δρομολόγηση που παράγεται από παράνομες ενημερώσεις / ανακοινώσεις διαδρομών . Για παράδειγμα, η ρύθμιση της απόσβεσης των φλάντζων διαδρομής (RFD) με ένα καλά καθορισμένο κατώφλι μπορεί να συμβάλει στη μείωση του χρόνου επεξεργασίας του δρομολογητή μι.

- Οι βάσεις δεδομένων μητρώου όπως οι IRR, APNIC, ARIN και RIPE πρέπει να υπόκεινται σε συνεχή συντήρηση. Αυτό θα επιτρέψει τη χρήση επικαιροποιημένων πληροφοριών για την ασφαλή διασύνδεση . Για παράδειγμα, το πεδίο "Αντικείμενο διαδρομής" μπορεί να βοηθήσει στην επικύρωση των δρομολογίων που λαμβάνονται από τους συνομηλίκους .

- Οι ενημερώσεις διαμόρφωσης για την υποδομή δρομολόγησης μπορούν να εκτελούνται μόνο από μια ορισμένη αρχή που χρησιμοποιεί ισχυρό έλεγχο ταυτότητας .

- Παρακολουθήστε την κατάσταση του BGP για να ανιχνεύσετε ασυνήθιστη συμπεριφορά, όπως αλλαγές διαδρομής ή ασυνήθιστες ανακοινώσεις t.

Διαρροές διαδρομής:

- Διαμορφώστε το μέγιστο πρόθεμα BGP για να διασφαλίσετε την εγκυρότητα των δρομολογίων που ανακοινώθηκαν. Αν ληφθούν περισσότερα προθέματα, αυτό αποτελεί ένδειξη λανθασμένης συμπεριφοράς και η περίοδος BGP τερματίζεται.

- Χρησιμοποιήστε την πιστοποίηση πόρων (RPKI) για την επικύρωση της προέλευσης AS .

Απόσπαση της συνόδου του BGP:

- Καθιέρωση φίλτρου προθέματος και αυτοματοποίηση φίλτρων πρόθεμα .

- Χρησιμοποιήστε φιλτράρισμα μονοπατιού AS .

- Χρησιμοποιήστε το TCP-AO (επιλογή TCP-Authentication Option) για να εξασφαλίσετε τον έλεγχο ταυτότητας BGP για να αντικαταστήσετε το TCP-MD5. Το TCP-AO απλοποιεί την ανταλλαγή πλήκτρων .

Απειλές DNS

DNS καταχωρητής αεροπειρατεία:

- Οι καταχωρίζοντες πρέπει να προστατεύουν τα διαπιστευτήρια λογαριασμού s και να ορίσει εξουσιοδοτημένους χρήστες, ενώ οι καταχωρητές πρέπει να παρέχουν μια ασφαλή διαδικασία πιστοποίησης μικρό.

- Οι καταχωρίζοντες θα πρέπει να επωφεληθούν από την τακτική αλληλογραφία από τον καταχωρητή, όπως ειδοποίηση αλλαγής, πληροφορίες χρέωσης ή εγγραφές WHOIS. Ως εκ τούτου, οι καταχωρητές πρέπει να παρέχουν αυτές τις πληροφορίες .

- Οι καταχωρίζοντες πρέπει να τηρούν έγγραφα για να «αποδείξουν την εγγραφή» .

- Οι καταχωρίζοντες πρέπει να χρησιμοποιούν ξεχωριστές ταυτότητες για τους καταχωρίζοντες, τις τεχνικές, τις διοικητικές και τις επαφές χρέωσης. Έτσι, οι καταχωρητές πρέπει να επιτρέψουν μια πιο σύνθετη διαχείριση δικαιωμάτων των χρηστών .

- Οι καταχωρητές πρέπει να καθιερώσουν αποτελεσματική διαχείριση δεδομένων ζώνης .

- Οι καταχωρητές πρέπει να εξετάσουν το ενδεχόμενο υποστήριξης του DNSSEC .

- Οι καταχωρητές μπορούν να παρακολουθούν τις δραστηριότητες αλλαγής DNS .

Υποκλοπή DNS:

- Η ανάπτυξη του DNSSEC στοχεύει στην εξασφάλιση της ταυτότητας των DNS πελατών (resolvers) προέλευσης των δεδομένων DNS, της αυθεντικής άρνησης ύπαρξης και της ενσωμάτωσης δεδομένων ty.

DNS δηλητηρίαση:

- Η ανάπτυξη του DNSSEC στοχεύει στην εξασφάλιση της αυθεντικότητας των δεδομένων DNS των εξυπηρετητών DNS (resolvers), της αυθεντικής άρνησης ύπαρξης και της ακεραιότητας των δεδομένων .

- Περιορίστε τις μεταφορές ζώνης για να μειώσετε το φορτίο σε συστήματα και δίκτυα rk.

- Περιορίστε τις δυναμικές ενημερώσεις μόνο σε εξουσιοδοτημένες πηγές, για να αποφύγετε την κατάχρηση . Τέτοια κατάχρηση περιλαμβάνει την κατάχρηση ενός διακομιστή DNS ως ενισχυτή, δηλητηρίαση DNS cache ...

- Ρυθμίστε τον κύριο διακομιστή ονομάτων ως μη επαναλαμβανόμενο. Ξεχωριστοί αναδρομικοί διακομιστές ονομάτων από τον έγκυρο διακομιστή ονομάτων .

- Να επιτρέπεται η μεταφορά DNS μέσω του TCP για την υποστήριξη μη τυποποιημένων ερωτημάτων. Επιπλέον, το TCP μπορεί να είναι απαραίτητο για το DNSSEC .

Σύγκρουση ονόματος τομέα:

- Μην χρησιμοποιείτε τυχαία ονόματα τομέα που δεν είστε ιδιοκτήτες για την εσωτερική υποδομή σας. Για παράδειγμα, μην θεωρείτε το ιδιωτικό τομέα ονόματος τομέα ως τομέα ανωτάτου επιπέδου.

- Αποτρέψτε την αίτηση DNS για εσωτερικούς χώρους ονομάτων να διαρρεύσουν στο Internet εφαρμόζοντας πεδίο firewall σεις.

- Χρησιμοποιήστε αποκλειστικά TLD όπως .test, .example, .invalid ή .localhost .

Απειλές άρνησης εξυπηρέτησης

Ενίσχυση / αντανάκλαση:

- Υιοθετήστε επαλήθευση διεύθυνσης IP πηγής στην άκρη της υποδομής Internet (κοντά στην προέλευση της κυκλοφορίας) για να αποτρέψετε την πλαστογράφηση διεύθυνσης δικτύου μέσω φίλτρου εισόδου και εξόδου σολ.

- Οι χειριστές του αυθεντικού φορέα εξυπηρετητών ονομάτων θα πρέπει να εφαρμόσουν το RRL (Ratio Rate Response) .

- Οι φορείς εκμετάλλευσης διακομιστών ονομάτων DNS και οι ISP πρέπει να απενεργοποιούν την ανοικτή αναδρομή σε διακομιστές ονομάτων και μπορούν να δέχονται ερωτήματα DNS μόνο από αξιόπιστες πηγές .

Πλημμύρα:

- Οι κατασκευαστές και οι διαμορφωτές του εξοπλισμού δικτύου πρέπει να λάβουν μέτρα για να εξασφαλίσουν όλες τις συσκευές και πρέπει να τη διατηρούν ενημερωμένες .