Πολιτικές Ασφάλειας και Ιδιωτικότητας στο Διαδίκτυο

Κυβερνοεπιθέσεις Μελέτες Περίπτωσης

Ελένη Χριστοπούλου
hristope@ionio.gr

Μελέτες Περίπτωσης

1. Προσδιορίστε εάν το περιστατικό απειλούσε την Εμπιστευτικότητα, την Ακεραιότητα ή / και τη Διαθεσιμότητα
2. Δηλώστε την κύρια αιτία του συμβάντος
3. Προσδιορίστε την πραγματική ή πιθανή ζημία του συμβάντος

Μελέτες Περίπτωσης

HE-2: Hacktivist Attack – the Epluribus Enum, σελ. 19

HE-3: Partner Misuse – the Indignant Mole, σελ.24

HE-4: Disgruntled Employee – the Absolute Zero, σελ. 29

CD-3: IoT Calamity – the Panda Monium, σελ. 46

CE-2: DDoS attack – the 12000 Monkeyz, σελ. 61

Attack-defend card example

<Scenario Name> — the <Scenari-cature>

specific (victim), indirect (e.g., open port, application), opportunistic (e.g., phishing)

1-5 based on tactics and techniques

confidentiality, integrity, availability

Breach scenario

Breach scenario

Sophistication level

1 2 3 4 5

Attributes

Incident pattern

Pattern

Time to discovery

H D W M Y

Time to containment

H D W M Y

most relevant incident pattern for the scenario

hours, days, weeks, months, years

hours, days, weeks, months, years

threat actor types

espionage, financial, ideology, grudge

1-5 VERIS threat actions[4]

Threat actor

Composition

Motives

Tactics and techniques

Targeted victims

Industries

Key stakeholders

Countermeasures

relevant NAICS industries[3]

key IR stakeholders

CIS Critical Security Controls

high-level description of the breach scenario

Verizon Data Breach Digest

HE-2: Hacktivist Attack – the Epluribus Enum (σελ. 19)

- Προσδιορίστε εάν το περιστατικό απειλούσε την Εμπιστευτικότητα, την Ακεραιότητα ή / και τη Διαθεσιμότητα
  - Εμπιστευτικότητα (Confidentiality): , αποκτήθηκαν και μοιράστηκαν προσωπικά στοιχεία δύο στελεχών
  - Ακεραιότητα (Integrity): μία από τις ιστοσελίδες των εταιρειών «παραποιήθηκε» *(defaced)*
- Δηλώστε την κύρια αιτία του συμβάντος
  - Ο ιστότοπος είχε γίνει στόχος χακτιβιστών (hacktivists)
  - Η αρχική παραβίαση (breach) έγινε μέσω μιας επίθεσης κοινωνικής μηχανικής, με φορέα απειλής κάποιον που υποδυόταν άτομο από το προσωπικό της εταιρείας
- Προσδιορίστε την πραγματική ή πιθανή ζημία του συμβάντος
  - Η άμεση ζημία ήταν η παραποίηση ενός εταιρικού website
  - Πραγματοποιήθηκαν προσπάθειες DDoS. μία από αυτές μπορεί να είναι επιτυχής στο μέλλον
  - Τα άτομα των οποίων οι πληροφορίες αποκτήθηκαν βρίσκονταν σε «κίνδυνο» για προσωπική επίθεση ή απάτη

HE-3: Partner Misuse – the Indignant Mole (σελ. 24)

- Προσδιορίστε εάν το περιστατικό απειλούσε την Εμπιστευτικότητα, την Ακεραιότητα ή / και τη Διαθεσιμότητα
  - Εμπιστευτικότητα (Confidentiality): υπήρξε πρόσβαση σε λογαριασμούς πελατών
  - Ακεραιότητα (Integrity): πληρωμές λογαριασμών κατευθύνθηκαν αλλού
- Δηλώστε την κύρια αιτία του συμβάντος
  - Ένας υπάλληλος τηλεφωνικού κέντρου χρησιμοποίησε φωτογραφίες από οθόνες του συστήματος για να καταγράψει πληροφορίες
  - Χρησιμοποιώντας αυτά τα δεδομένα, ένας ξάδερφος του εργαζόμενου θα δημιουργούσε έναν απατηλό λογαριασμό
- Προσδιορίστε την πραγματική ή πιθανή ζημία του συμβάντος
  - Οι επιστροφές είχαν «παρεκλίνει» στους απατηλούς/δόλιους λογαριασμούς
  - Αυτό θα μπορούσε να συνεχιστεί, οδηγώντας σε περισσότερες απώλειες

HE-4: Disgruntled Employee – the Absolute Zero (σελ. 29)

- Προσδιορίστε εάν το περιστατικό απειλούσε την Εμπιστευτικότητα, την Ακεραιότητα ή / και τη Διαθεσιμότητα
  - Ακεραιότητα: ο υπάλληλος χρησιμοποίησε την πρόσβαση που είχε ως διαχειριστής για να καταλάβει λογαριασμούς
  - Εμπιστευτικότητα: λόγω της λήψης (download) πληροφοριών της εταιρείας

- Δηλώστε την κύρια αιτία του συμβάντος
  - Ο δυσαρεστημένος υπάλληλος χρησιμοποίησε την πρόσβασή του για να κλέψει αρχεία και να ορίσει εντολές διαγραφής για μελλοντικές ημερομηνίες
  - Οι ερευνητές βρήκαν επίσης ένα USB plug extension το οποίο έστελνε την είσοδο πληκτρολογίου σε ένα ρουμανικό εξυπηρετητή (που δεν σχετίζεται με τις ενέργειες του υπαλλήλου)

- Προσδιορίστε την πραγματική ή πιθανή ζημία του συμβάντος
  - Και οι δύο απειλές ανακαλύφθηκαν πριν από την πραγματική βλάβη
  - Οι πληροφορίες που έκλεψε ο υπάλληλος, καθώς και οι μελλοντικές εντολές που είχε θέσει στα συστήματα, θα μπορούσαν να προκαλέσουν σημαντικές διαταραχές στην επιχείρηση
  - Οι πληροφορίες που αποκτήθηκαν μέσω του keylogger θα μπορούσαν να παρέχουν πληροφορίες σε έναν άλλο φορέα απειλής για να μπει στο σύστημα της εταιρείας και να προκαλέσει διάφορα είδη ζημιάς, ανάλογα με τα κίνητρά του

CD-3: IoT Calamity – the Panda Monium (σελ. 46)

- Προσδιορίστε εάν το περιστατικό απειλούσε την Εμπιστευτικότητα, την Ακεραιότητα ή / και τη Διαθεσιμότητα
  - Διαθεσιμότητα: το υπερφορτωμένο σύστημα επιβράδυνε όλες τις δραστηριότητες στην πανεπιστημιούπολη
- Δηλώστε την κύρια αιτία του συμβάντος
  - Ένας άγνωστος επιτιθέμενος δημιούργησε ένα botnet, το οποίο προκάλεσε πολλές συσκευές IoT στην πανεπιστημιούπολη να «πλημμυρίσουν» τον server με αιτήματα
- Προσδιορίστε την πραγματική ή πιθανή ζημία του συμβάντος
  - Το άμεσο πρόβλημα ήταν αργές υπηρεσίες διαδικτύου για τους χρήστες
  - Ο επιτιθέμενος θα μπορούσε να είχε αρχίσει άμεσα επηρεάζοντας τα φώτα, τα συστήματα θέρμανσης και άλλα συνδεδεμένα συστήματα στην πανεπιστημιούπολη

CE-2: DDoS attack – the 12000 Monkeyz (σελ. 61)

- Προσδιορίστε εάν το περιστατικό απειλούσε την Εμπιστευτικότητα, την Ακεραιότητα ή / και τη Διαθεσιμότητα
  - Διαθεσιμότητα: η προσπάθεια να ξεκινήσει ένα στοχευμένο DDoS περιόδους μεγάλου φόρτου
- Δηλώστε την κύρια αιτία του συμβάντος
  - Ο επιτιθέμενος χρησιμοποίησε αρκετούς τύπους επιθέσεων στοχεύοντας τους δρομολογητές που χρησιμοποιούσαν παλιό firmware με ενεργοποιημένο το UPnP., ήταν πολλές οι πιθανότητες αυτοί να ήταν "NYP'd" (vot yet patched)
- Προσδιορίστε την πραγματική ή πιθανή ζημία του συμβάντος
  - Η επίθεση ανακαλύφθηκε πριν το πρόβλημα γίνει πολύ μεγάλο
  - Εάν το DDoS χτυπούσε όπως είχε προγραμματιστεί, η εταιρεία θα αντιμετώπιζε θυμωμένους πελάτες και ενδεχομένως να έχανε αρκετούς, καθώς και πρόβλημα δημοσίων σχέσεων. Αυτό θα μπορούσε να προκαλέσει μακροπρόθεσμες απώλειες της επιχείρησης και της φήμης της