Corfu

Ψηφιακή Εγκληματολογία και Αναγνώριση Απειλών: Ανταπόκριση σε Περιστατικά
Ο ρόλος της ψηφιακής εγκληματολογίας

Dr. Stylianos Karagiannis (PhD)
Ionian University, Corfu, Greece

</> Stylianos Karagiannis

Corfu, Kozani, Greece Lisbon, Portugal

PhD in Cybersecurity - Post Doc @ Ionian University Department of Informatics, Corfu, Greece
Senior Researcher @ PDMFC, Lisbon, Portugal

Research Interests: Cybersecurity, Privacy, Capture The Flag (CTF) Challenges, Cyber Ranges
Gamification, Incident Handling, Virtual Labs, Game-Based Learning
Social Constructivism, Learning Theories

Email: skaragiannis@ionio.gr, LinkedIn, NMSLab

Διαχείριση Περιστατικών

- **Απειλές στη Σύγχρονη Τεχνολογία Πληροφοριών:** Από script kiddies που χρησιμοποιούν έτοιμο κώδικα έως κρατικούς αντιπάλους με εξελιγμένα εργαλεία, το τοπίο των απειλών είναι εκτεταμένο και ανησυχητικό. Η προετοιμασία είναι κρίσιμη ώστε οι οργανισμοί να μειώσουν την έκθεσή τους.
- **Παραδείγματα Επιθέσεων:** Ένα μεμονωμένο ransomware από εσωτερικό υπάλληλο μπορεί να προκαλέσει σοβαρές επιπτώσεις. Ακόμη πιο περίπλοκες επιθέσεις, όπως εκμετάλλευση δικτύων ή παραβιάσεις δεδομένων, εντείνουν το χάος σε έναν οργανισμό.
- **Διαχείριση Περιστατικού:** Το τεχνικό προσωπικό πρέπει να εντοπίσει ποια συστήματα έχουν επηρεαστεί και να περιορίσει την απώλεια δεδομένων. Ταυτόχρονα, τα ανώτερα στελέχη απαιτούν ενημερώσεις για το μέγεθος και τις αιτίες του περιστατικού.
- **Σημασία Ορθής Αντίδρασης:** Η οργανωμένη ανταπόκριση επιτρέπει τον περιορισμό ζημιάς και την ταχύτερη ανάκαμψη από κυβερνοεπιθέσεις. Για το λόγο αυτό, οι οργανισμοί ενσωματώνουν την αντιμετώπιση περιστατικών στις πολιτικές και διαδικασίες τους.
- **Θεμέλια Ικανότητας Ανταπόκρισης.** Απαιτείται:
  - Γνώση της διαδικασίας ανταπόκρισης
  - Εξειδικευμένο προσωπικό στον πυρήνα της ομάδας
  - Επίσημο σχέδιο με σαφείς διαδικασίες
  - Με αυτό το πλαίσιο, οι οργανισμοί είναι έτοιμοι να αντιμετωπίσουν τις αναδυόμενες απειλές.

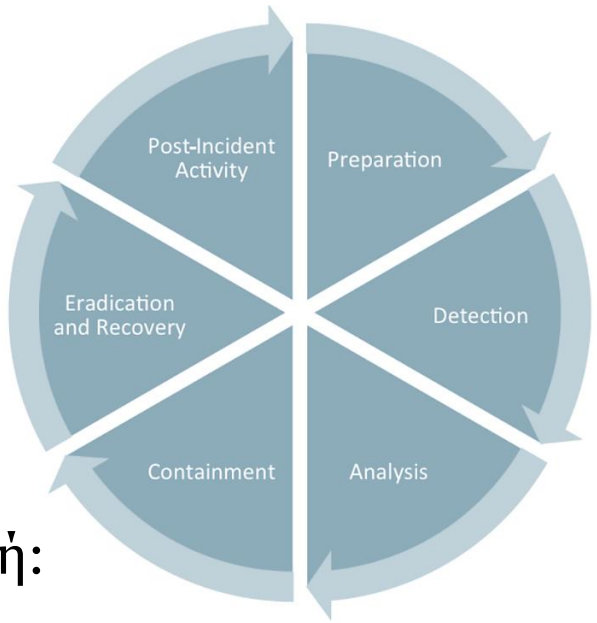
Διαδικασία Ανταπόκρισης

Κάθε περιστατικό ακολουθεί μια γενική πορεία στον κύκλο ζωής του. Ένας ώριμος οργανισμός έχει μέτρα σε κάθε στάδιο ώστε να περιορίσει τις επιπτώσεις.

- **Έναρξη Περιστατικού:** Η διαδικασία ξεκινά με την ανίχνευση κακόβουλης δραστηριότητας. Η ανίχνευση προκύπτει από:
  - Ειδοποίηση συστήματος ασφαλείας
  - Πληροφόρηση από εξωτερικό φορέα

Ανάλυση & Αντιμετώπιση: Μετά τον συναγερμό, ο οργανισμός

- Προχωρά σε ανάλυση του περιστατικού
- Εφαρμόζει μέτρα περιορισμού
- Επιδιώκει επαναφορά σε κανονική λειτουργία



Κυκλική Διαδικασία: Η ανταπόκριση δεν είναι γραμμική, αλλά κυκλική:

- Η προετοιμασία αποτελεί την αφετηρία
- Μετα-περιστασιακή δραστηριότητα τροφοδοτεί εκ νέου την προετοιμασία
- Κάθε περιστατικό οδηγεί σε βελτίωση της ετοιμότητας του οργανισμού

Φάσεις Ανταπόκρισης

Η διαδικασία χωρίζεται σε **έξι στάδια**. Κάθε στάδιο περιλαμβάνει κρίσιμες ενέργειες που ενισχύουν την αποτελεσματική αντιμετώπιση.

1. **Προετοιμασία (Preparation):** Χωρίς σωστή προετοιμασία, κάθε ανταπόκριση είναι ανοργάνωτη.Απαιτείται: σχέδιο, εκπαιδευμένο προσωπικό, εργαλεία εγκληματολογίας και τακτικές ασκήσεις.
2. **Ανίχνευση (Detection):** Η ανίχνευση κακόβουλων ενεργειών είναι σύνθετη.Αναλυτές πρέπει να ξεχωρίσουν τον «θόρυβο» από τα σημαντικά δεδομένα, με χρήση SIEM και εξωτερικών πηγών πληροφόρησης.
3. **Ανάλυση (Analysis):** Συλλογή αποδεικτικών στοιχείων (RAM, logs, δικτυακές συνδέσεις).Στόχος: root cause analysis και κατανόηση της διαδρομής του επιτιθέμενου.
4. **Περιορισμός (Containment):** Εφαρμογή μέτρων για να εμποδιστεί η συνέχιση της επίθεσης. Παραδείγματα: α) αποκλεισμός IP, β) αποσύνδεση μηχανήματος, γ) αλλαγή ρυθμίσεων firewall.
5. **Εξάλειψη & Αποκατάσταση (Eradication & Recovery):** Απομάκρυνση επιτιθέμενου και επανεγκατάσταση συστημάτων. α) Εφαρμογή patches, β) επαναφορά από backup και γ) έλεγχος ευπαθειών πριν την πλήρη αποκατάσταση.
6. **Μετα-περιστασιακή Δραστηριότητα (Post-incident activity):** Ανασκόπηση ενεργειών και δημιουργία αναλυτικής αναφοράς. α) Καταγραφή διδαγμάτων και β) βελτίωση διαδικασιών για μελλοντικά περιστατικά.

Πλαίσιο Ανταπόκρισης

- Η ανταπόκριση σε περιστατικά δεν πρέπει να είναι **αποσπασματική διαδικασία**. Χωρίς καθορισμένες διαδικασίες, ο οργανισμός δεν μπορεί να εκτιμήσει την **έκταση** του περιστατικού ή να το **περιορίσει έγκαιρα**, μειώνοντας τη ζημιά.
- Η προσπάθεια δημιουργίας σχεδίου **την ώρα του περιστατικού** μπορεί να καταστρέψει **αποδεικτικά στοιχεία** ή να προκαλέσει **νέα προβλήματα**.
- Η κατανόηση της διαδικασίας αποτελεί μόνο το **πρώτο βήμα** για την οικοδόμηση ικανότητας μέσα στον οργανισμό. Απαιτείται ένα **πλαίσιο** που αξιοποιεί τις διαθέσιμες πηγές και θέτει σε εφαρμογή τις διαδικασίες.
- Το πλαίσιο περιλαμβάνει κρίσιμα στοιχεία όπως **προσωπικό, πολιτικές και διαδικασίες**, μέσω των οποίων ο οργανισμός χτίζει την **λειτουργική του ικανότητα να ανταποκρίνεται** σε περιστατικά ασφαλείας.

Ο Χάρτης Απόκρισης

- Η ανάπτυξη ικανότητας ανταπόκρισης ξεκινά με απόφαση της **ανώτερης διοίκησης** ότι οι κίνδυνοι δεν μπορούν να αγνοηθούν. Ένα ανώτερο στέλεχος αναλαμβάνει **χορηγός έργου** και εκπονεί τον χάρτη απόκρισης, οδηγώντας στη δημιουργία του CSIRT.
- **Η CSIRT είναι η ομάδα απόκρισης** σε περιστατικά ασφαλείας υπολογιστών. **Ο χάρτης απόκρισης αποτελεί γραπτό έγγραφο που καθορίζει βασικά στοιχεία για τη λειτουργία και τη δομή της ομάδας.** Η υποστήριξη από την ανώτερη διοίκηση είναι κρίσιμη για τη βιωσιμότητα. Το CSIRT λειτουργεί ως ασφαλιστήριο συμβόλαιο, μειώνοντας τον αντίκτυπο και το κόστος περιστατικών, ακόμη και αν δεν αποφέρει άμεσα έσοδα.
- Το **πεδίο ευθύνης (constituency)** ορίζει ποια τμήματα και θυγατρικές υπάγονται στο CSIRT. Μπορεί να οριστεί ως domain ή ως ολόκληρος οργανισμός με συνδεδεμένες εταιρείες, διασφαλίζοντας σαφή αρμοδιότητα. Η **δήλωση αποστολής (mission statement**) ορίζει τον σκοπό του CSIRT και αποτρέπει το mission creep, π.χ. «Παροχή έγκαιρης ανάλυσης και δράσεων για περιστατικά που επηρεάζουν εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των συστημάτων και του προσωπικού».
- Ο **καθορισμός υπηρεσιών (service delivery)** περιλαμβάνει προληπτικές υπηρεσίες, όπως εκπαίδευση και ανάπτυξη εργαλείων ασφαλείας, και αντιδραστικές υπηρεσίες, όπως συλλογή αποδεικτικών στοιχείων, περιορισμό, εξάλειψη και τεκμηρίωση περιστατικών.
- Η **κοινωνικοποίηση της CSIRT** μειώνει φήμες και παρανοήσεις εντός του οργανισμού. Το προσωπικό κατανοεί τον σκοπό της ομάδας, ενώ οι περιοδικές ενημερώσεις στην ανώτερη διοίκηση επιβεβαιώνουν τη συνεισφορά της στην ασφάλεια του οργανισμού.

Στελέχωση CSIRT

- Μετά την ολοκλήρωση του **χάρτη αποστολής (incident response charter)**, το επόμενο βήμα είναι η **στελέχωση του CSIRT**. Οι μεγαλύτεροι οργανισμοί μπορούν να διαθέσουν προσωπικό με **πλήρη απασχόληση**, ενώ συχνότερα το προσωπικό έχει και άλλες υποχρεώσεις πέρα από την απόκριση σε περιστατικά.
- Το εσωτερικό προσωπικό του CSIRT χωρίζεται σε **τρεις κατηγορίες**: **βασική ομάδα (core team), τεχνική υποστήριξη (technical support) και οργανωτική υποστήριξη (organizational support)**. Κάθε μέλος αναλαμβάνει **συγκεκριμένο ρόλο** για την αποτελεσματική λειτουργία της ομάδας.
- Η δημιουργία ενός **λειτουργικού CSIRT** απαιτεί περισσότερα από απλή ανάθεση προσωπικού ή σύνταξη εγγράφων. Απαιτείται **συστηματική προσπάθεια**, κατάρτιση και συντονισμός για να υποστηριχθούν περιστατικά οποιασδήποτε κλίμακας.
- Κάθε κατηγορία διαθέτει **σχεδιασμένους ρόλους και ευθύνες**, ώστε να παρέχεται καθοδήγηση και υποστήριξη σε περιστατικά από **μικρής έως καταστροφικής κλίμακας**, εξασφαλίζοντας πλήρη κάλυψη των αναγκών του οργανισμού.

Συντονιστής Απόκρισης

Συντονιστής Απόκρισης σε Περιστατικά (Incident Response Coordinator): Αποτελεί **κρίσιμο στοιχείο** κάθε CSIRT. Χωρίς σαφή ηγεσία, η απόκριση σε περιστατικά μπορεί να γίνει **ανοργάνωτη** ή να επικρατήσει χάος λόγω διαφορών στην ανάληψη ελέγχου. Συχνά ο ρόλος αναλαμβάνεται από τον **CSO, CISO ή ISO**, που φέρουν συνολική ευθύνη για την ασφάλεια πληροφοριών.

- Ο **συντονιστής απόκρισης** διαχειρίζεται το CSIRT πριν, κατά τη διάρκεια και μετά το περιστατικό, εξασφαλίζοντας ότι τα σχέδια και οι πολιτικές **επανεξετάζονται και επικαιροποιούνται**.
- Διασφαλίζει ότι η ομάδα έχει την **κατάλληλη εκπαίδευση**, οργανώνει δοκιμές και ασκήσεις, και κατά τη διάρκεια περιστατικών καθοδηγεί την ομάδα στη **διαδικασία απόκρισης και αποκατάστασης**, συνεργαζόμενος με την ανώτερη διοίκηση.
- Μεταφράζει την **τεχνική ορολογία** σε κατανοητή γλώσσα για μη τεχνικά στελέχη και, μετά το περιστατικό, φροντίζει για την **τεκμηρίωση**, αποστολή αναφορών και ενσωμάτωση διδαγμάτων στο σχέδιο CSIRT.

Ανώτεροι Αναλυτές CSIRT

Ανώτεροι Αναλυτές CSIRT (CSIRT Senior Analysts): Διαθέτουν **εκτενή εκπαίδευση και εμπειρία** στην απόκριση σε περιστατικά, στη **ψηφιακή εγκληματολογία (digital forensics)** και στην **ανάλυση δεδομένων δικτύου**. Συνήθως έχουν πολυετή εμπειρία είτε ως σύμβουλοι είτε ως μέλη ενός εταιρικού CSIRT.

- Οι **ανώτεροι αναλυτές** διασφαλίζουν την **κατάρτιση και τις δεξιότητές τους** και συμμετέχουν στη **διαμόρφωση και αναθεώρηση του σχεδίου απόκρισης**.
- Εκπαιδεύουν **νεότερα μέλη** της ομάδας και κατά τη διάρκεια περιστατικών συλλέγουν και αναλύουν **αποδεικτικά στοιχεία**, κατευθύνουν δραστηριότητες **περιορισμού (containment)** και υποστηρίζουν την **αποκατάσταση**.
- Μετά το περιστατικό, τεκμηριώνουν τις ενέργειες, ετοιμάζουν **αναφορές** και διαχειρίζονται τα **αποδεικτικά στοιχεία**, εξασφαλίζοντας ότι η ομάδα λειτουργεί αποτελεσματικά και με συνέπεια.

Αναλυτές CSIRT

Αναλυτές CSIRT (CSIRT Analysts): Διαθέτουν **μικρότερη εμπειρία (1–2 χρόνια)** και εργάζονται υπό την καθοδήγηση των **ανώτερων αναλυτών**. Αποτελούν κρίσιμο μέρος της ομάδας για την **εκτέλεση καθημερινών εργασιών απόκρισης**.

- Οι **αναλυτές** εξελίσσουν τις δεξιότητές τους μέσω **εκπαίδευσης και ασκήσεων** και συμμετέχουν στις **αναθεωρήσεις σχεδίων απόκρισης**.
- Συλλέγουν δεδομένα από **πιθανά επηρεασμένα συστήματα**, δικτυακές συσκευές ή **αρχεία καταγραφής (logs)**, υποστηρίζοντας την **ανάλυση περιστατικών**.
- Συμμετέχουν ενεργά στη διαδικασία **ανάλυσης στοιχείων** και **αποκατάστασης**, εξασφαλίζοντας ότι τα περιστατικά αντιμετωπίζονται με συνέπεια και ακρίβεια.

Αναλυτές Κέντρου Επιχειρήσεων

Αναλυτές Κέντρου Επιχειρήσεων Ασφάλειας (SOC Analysts) & Μηχανικοί/Αναλυτές Ασφάλειας Πληροφοριακών Συστημάτων (IT Security Engineers/Analysts): Σε μεγάλες επιχειρήσεις, το **SOC** λειτουργεί 24/7. Οι **SOC Analysts** εντοπίζουν και ειδοποιούν για περιστατικά, αποτελώντας την **πρώτη γραμμή ανίχνευσης** και την **αρχική απόκριση**.

- Οι **IT Security Engineers/Analysts** αναλαμβάνουν την **ανάπτυξη, συντήρηση και παρακολούθηση εργαλείων και συσκευών ασφαλείας**, όπως antivirus, firewalls και SIEM.
- Κατά τη διάρκεια περιστατικού, παρακολουθούν τα **συστήματα ασφαλείας** για ενδείξεις κακόβουλης δραστηριότητας και συλλέγουν σχετικά στοιχεία.
- Μετά το περιστατικό, ρυθμίζουν τα συστήματα ώστε να **παρακολουθούν πιθανές επαναλήψεις**, διασφαλίζοντας ότι ο οργανισμός παραμένει προστατευμένος και έτοιμος για μελλοντικά περιστατικά.

Τεχνικό Προσωπικό Υποστήριξης

Τεχνικό Προσωπικό Υποστήριξης (Technical Support Personnel): Το **τεχνικό προσωπικό υποστήριξης** περιλαμβάνει άτομα που δεν έχουν καθημερινές αρμοδιότητες CSIRT, αλλά διαθέτουν **εξειδίκευση ή πρόσβαση** σε συστήματα και διαδικασίες που μπορεί να επηρεαστούν από ένα περιστατικό.

- Το CSIRT συνεργάζεται με παράδειγμα έναν **διαχειριστή διακομιστών (server administrator)** για τη συλλογή **αποδεικτικών στοιχείων**, όπως λήψη μνήμης (memory captures), εξαγωγή εικονικών συστημάτων ή αντιγραφή **log files**.
- Μόλις ολοκληρωθεί η συλλογή στοιχείων, ο ρόλος του **τεχνικού υποστηρικτή** τερματίζεται και συνήθως δεν εμπλέκεται περαιτέρω με το περιστατικό.
- Παράδειγμα προσωπικού που μπορεί να υποστηρίξει το CSIRT περιλαμβάνει **διαχειριστές διακομιστών, δικτυακούς διαχειριστές, τεχνικό προσωπικό εφαρμογών ή συστημάτων** που έχουν πρόσβαση σε κρίσιμες υποδομές κατά τη διάρκεια ενός περιστατικού.

Οργανωτική Υποστήριξη CSIRT (Organizational Support)

- **Αρχιτέκτονας/Διαχειριστής Δικτύου (Network Architect/Administrator):** Υπεύθυνος για την υποδομή δικτύου, όπως δρομολογητές και μεταγωγείς. Αναγνωρίζει **ανώμαλη δικτυακή κίνηση** και βοηθά στη συλλογή **αποδεικτικών στοιχείων**, όπως access logs και packet captures.
- **Διαχειριστής Διακομιστών (Server Administrator):** Υποστηρίζει κρίσιμους διακομιστές, όπως domain controllers και database servers. Συλλέγει **log files**, εντοπίζει νέους ή τροποποιημένους λογαριασμούς και βοηθά στην **ανάλυση συμβιβασμένων συστημάτων**.
- **Υποστήριξη Εφαρμογών (Application Support):** Εστιάζει σε διαδικτυακές εφαρμογές και **ευπάθειες**, όπως SQL injection. Συμβάλλει στην αναγνώριση αλλαγών στον κώδικα και στην **επιβεβαίωση ευπαθειών** κατά τη διερεύνηση περιστατικών.
- **Υποστήριξη Επιτραπέζιων Συστημάτων (Desktop Support):** Διαχειρίζεται DLP, antivirus και άλλα μέτρα προστασίας σε επιτραπέζιους υπολογιστές. Παρέχει **αρχεία καταγραφής**, βοηθά στον καθαρισμό μολυσμένων συστημάτων και υποστηρίζει την **αποκατάσταση**.
- **Γραφείο Υποστήριξης (Help Desk):** Λειτουργεί ως **προειδοποιητικός δείκτης** για περιστατικά. Εκπαιδεύεται στις διαδικασίες CSIRT, εντοπίζει αρχικά σημάδια μόλυνσης και βοηθά στην **κλιμάκωση και αναγνώριση επιπλέον επηρεασμένων χρηστών**.

Οργανωτική Υποστήριξη CSIRT (Organizational Support)

- **Νομική Υπηρεσία (Legal):** Συμμετέχει από τα πρώτα στάδια για να διασφαλίσει τη συμμόρφωση με νόμους και κανονισμούς, όπως HIPAA ή PCI DSS. Βοηθά στη σύνταξη ειδοποιήσεων παραβίασης και στην αντιμετώπιση εσωτερικών ή εξωτερικών αξιώσεων αποζημίωσης.
- **Ανθρώπινοι Πόροι (Human Resources):** Υποστηρίζει το CSIRT σε περιστατικά που αφορούν υπαλλήλους ή συνεργάτες, διασφαλίζοντας τη συμμόρφωση με την εργατική νομοθεσία. Συντονίζεται για τερματισμούς συνεργασίας, μειώνοντας τον κίνδυνο αγωγών για άδικη απόλυση.
- **Μάρκετινγκ / Επικοινωνία (Marketing/Communications):** Συμβάλλει στη διαχείριση της επικοινωνίας με πελάτες ή συνεργάτες σε περιστατικά, όπως παραβίαση δεδομένων ή DoS. Εξασφαλίζει **έγκυρη και έγκαιρη πληροφόρηση**, μειώνοντας αρνητικές αντιδράσεις.
- **Διεύθυνση Εγκαταστάσεων (Facilities):** Παρέχει πρόσβαση σε εγκαταστάσεις εκτός ωραρίου ή σε ειδικούς χώρους για παρατεταμένες επιχειρησιακές ανάγκες του CSIRT. Διασφαλίζει ότι οι φυσικοί χώροι υποστηρίζουν αποτελεσματικά τις ενέργειες απόκρισης.
- **Εταιρική Ασφάλεια (Corporate Security):** Υποστηρίζει το CSIRT σε περιστατικά κλοπής υλικών ή ψηφιακών πόρων. Διαθέτει πρόσβαση σε συστήματα παρακολούθησης, access badges και καταγραφές επισκεπτών για την ανασύνθεση των γεγονότων.

Σχέδιο Αντιμετώπισης Περιστατικών (Incident Response Plan)

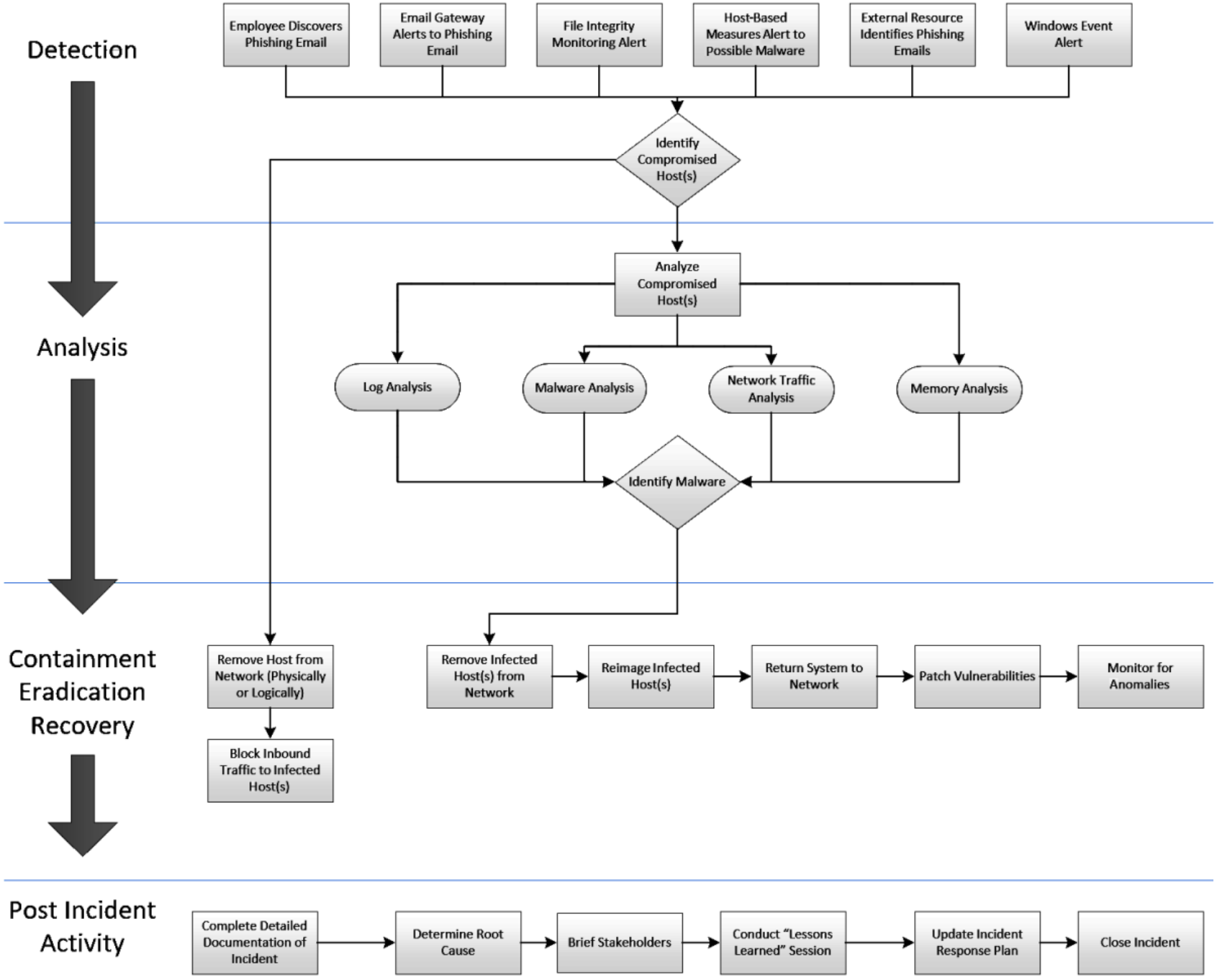
- **Καταστατικό Αντιμετώπισης:** Περιλαμβάνει τη δήλωση αποστολής και το κοινό-στόχο από το καταστατικό του CSIRT. Διασφαλίζει συνέχεια μεταξύ της δημιουργίας του CSIRT και της λειτουργίας του.
- **Εκτεταμένος Κατάλογος Υπηρεσιών:** Αναλύει λεπτομερώς τις υπηρεσίες που παρέχει το CSIRT, π.χ. ανάκτηση στοιχείων από δίσκους, ανάλυση μνήμης, αντίστροφη μηχανική κακόβουλου κώδικα, διαχωρίζοντας τα περιστατικά από κανονικά αιτήματα.
- **Προσωπικό CSIRT:** Καθορίζει σαφώς ρόλους και ευθύνες κάθε μέλους. Η σαφής οριοθέτηση μειώνει τις συγκρούσεις αρμοδιοτήτων και βελτιώνει την αποτελεσματικότητα κατά την αντιμετώπιση περιστατικών.
- **Κατάλογος Επαφών:** Περιλαμβάνει πρωτεύουσες και δευτερεύουσες επαφές για 24/7 ανταπόκριση, καθώς και εναλλασσόμενα μέλη σε κατάσταση ετοιμότητας για άμεση αντιμετώπιση περιστατικών.
- **Σχέδιο Εσωτερικής Επικοινωνίας:** Καθορίζει ροές πληροφοριών μεταξύ ανώτατης διοίκησης, βασικής ομάδας CSIRT και υποστηρικτικού προσωπικού, περιορίζοντας χάος και αντικρουόμενες οδηγίες.
- **Εκπαίδευση:** Καθορίζει τη συχνότητα εκπαίδευσης και συμμετοχής σε επιτραπέζιες ασκήσεις, με στόχο την κάλυψη τυχόν κενών και τη βελτίωση δεξιοτήτων.
- **Συντήρηση:** Προβλέπει ετήσια αναθεώρηση και ενημέρωση του σχεδίου σύμφωνα με αλλαγές σε υποδομές, απειλές και προσωπικό. Ενσωματώνει διδάγματα από ασκήσεις και πιστοποιήσεις προσωπικού.

Σχέδιο Αντιμετώπισης Περιστατικών (Incident Response Plan)

- **Καταστατικό Αντιμετώπισης:** Περιλαμβάνει τη δήλωση αποστολής και το κοινό-στόχο από το καταστατικό CSIRT. Διασφαλίζει συνέχεια μεταξύ της δημιουργίας του CSIRT και της λειτουργίας του.
- **Εκτεταμένος Κατάλογος Υπηρεσιών:** Αναλύει λεπτομερώς τις υπηρεσίες που παρέχει η CSIRT, π.χ. ψηφιακή εγκληματολογία, ανάκτηση στοιχείων από δίσκους, ανάλυση μνήμης, αντίστροφη μηχανική κακόβουλου λογισμικού.
- **Προσωπικό CSIRT:** Καθορίζει σαφώς ρόλους και ευθύνες κάθε μέλους, ώστε να αποφεύγονται συγκρούσεις αρμοδιοτήτων κατά την αντιμετώπιση περιστατικών.
- **Κατάλογος Επαφών:** Περιλαμβάνει επικοινωνίες για 24/7 ανταπόκριση, πρωτεύουσες και δευτερεύουσες επαφές, και προβλέπει εναλλασσόμενα μέλη σε κατάσταση ετοιμότητας.
- **Σχέδιο Εσωτερικής Επικοινωνίας:** Καθορίζει ροές πληροφοριών μεταξύ διοίκησης, βασικής ομάδας CSIRT και υποστηρικτικού προσωπικού, περιορίζοντας χάος και αντικρουόμενες οδηγίες.
- **Εκπαίδευση:** Προβλέπει ετήσιες επιτραπέζιες ασκήσεις και συνεχή εκπαίδευση, καλύπτοντας τυχόν κενά που εντοπίζονται μετά από περιστατικά.
- **Συντήρηση:** Καθορίζει αναθεώρηση και ενημέρωση του σχεδίου τουλάχιστον ετησίως. Ενσωματώνει διδάγματα από ασκήσεις και επιτρέπει βελτίωση δεξιοτήτων μέσω πιστοποιήσεων και ατομικής εκπαίδευσης.

Εγχειρίδιο Αντιμετώπισης Περιστατικών (Incident Response Playbook)

- **Ορισμός:** Το playbook είναι ένα σύνολο οδηγιών για κάθε βήμα της διαδικασίας αντιμετώπισης περιστατικών. Παρέχει σαφή πορεία δράσης με ευελιξία, ώστε να προσαρμόζεται σε διαφορετικά σενάρια περιστατικών.
- **Επιλογή Εγχειριδίων:** Κρίσιμα εγχειρίδια ορίζονται με βάση την αξιολόγηση κινδύνου του οργανισμού. Οι υψηλού κινδύνου απειλές, όπως zero-day exploits, ransomware ή phishing, πρέπει να έχουν αντίστοιχα playbooks.
- **Δομή Playbook:** Καλύπτει όλα τα στάδια της απόκρισης:
- **Προετοιμασία:** Εκπαίδευση προσωπικού, ευαισθητοποίηση σε phishing, προληπτικά μέτρα.
- **Ανίχνευση:** Ειδοποιήσεις από εργαζόμενους ή συστήματα ασφαλείας.
- **Ανάλυση:** Εξέταση μνήμης, logs και δικτυακής κίνησης για ταξινόμηση περιστατικού.
- **Διαχείριση Περιστατικού:**
- **Περιορισμός (Containment):** Απομόνωση συμβιβασμένων συστημάτων.
- **Εξάλειψη (Eradication):** Αφαίρεση malware ή επανεγκατάσταση συστημάτων.
- **Ανάκτηση (Recovery):** Σάρωση για ευπάθειες και παρακολούθηση.
- **Μετά το Περιστατικό (Post-incident):** Περιλαμβάνει τεκμηρίωση, αναφορά και βελτίωση διαδικασιών.
- **Σκοπός:** Τα playbooks μειώνουν τον χρόνο αντίδρασης και καθοδηγούν την CSIRT. Ενημερώνονται τακτικά και επιτρέπουν ευελιξία ώστε η ομάδα να αναλαμβάνει πρόσθετες ενέργειες όταν χρειάζεται.


Detection
Analysis
Containment
Eradication
Recovery
Post Incident
Activity
Employee Discovers Phishing Email
Email Gateway Alerts to Phishing Email
File Integrity Monitoring Alert
Host-Based Measures Alert to Possible Malware
External Resource Identifies Phishing Emails
Windows Event Alert
Identify Compromised Host(s)
Analyze Compromised Host(s)
Log Analysis
Malware Analysis
Network Traffic Analysis
Memory Analysis
Identify Malware
Remove Host from Network (Physically or Logically)
Block Inbound Traffic to Infected Host(s)
Remove Infected Host(s) from Network
Reimage Infected Host(s)
Return System to Network
Patch Vulnerabilities
Monitor for Anomalies
Complete Detailed Documentation of Incident
Determine Root Cause
Brief Stakeholders
Conduct "Lessons Learned" Session
Update Incident Response Plan
Close Incident

Διαδικασίες Κλιμάκωσης (Escalation Procedures)

Σκοπός: Οι διαδικασίες κλιμάκωσης καθορίζουν πότε ένα γεγονός ή σειρά γεγονότων μετατρέπεται από απλή ανωμαλία σε πλήρες περιστατικό. Στόχος είναι η αποτελεσματική αξιοποίηση της CSIRT, περιορίζοντας τα ψευδή θετικά και καλώντας προσωπικό μόνο όταν η εξειδίκευσή του είναι απαραίτητη.

Αρχική Κλιμάκωση: Οι πρώτες ενδείξεις ανωμαλίας προέρχονται συχνά από help desk ή τεχνικό προσωπικό. Αν, για παράδειγμα, εντοπιστεί malware που δεν αφαιρείται μέσω προληπτικών μέτρων, η υπόθεση κλιμακώνεται στο υπεύθυνο μέλος της CSIRT για έλεγχο και διαχείριση.

Πλήρης Κλιμάκωση: Σε πιο σύνθετες περιπτώσεις, όπως μη εξουσιοδοτημένοι λογαριασμοί διαχειριστή ή παραβίαση δεδομένων, η κλιμάκωση περιλαμβάνει: α) Διερεύνηση από αναλυτή CSIRT. β) Συνεργασία με διαχειριστή διακομιστή και δικτύου. γ) Εμπλοκή συντονιστή CSIRT για ενεργοποίηση επιπλέον πόρων. δ) Κλήση οργανωτικού προσωπικού (νομική, HR, επικοινωνία) αν απαιτείται.

Αρχές: α) Κάθε περιστατικό αξιολογείται για σοβαρότητα πριν κλιμακωθεί. β) Οι διαδικασίες καθορίζουν ποιος έχει εξουσιοδότηση να χαρακτηρίζει ένα γεγονός ως περιστατικό. γ) Οι οδηγίες διασφαλίζουν ότι το κατάλληλο προσωπικό και οι υποστηρικτικοί πόροι συμμετέχουν ανάλογα με τη σοβαρότητα.

Οφέλη: α) Αποφυγή υπερφόρτωσης της CSIRT. β) Σαφής κατανομή ρόλων και ευθυνών. γ) Γρήγορη και συντονισμένη αντίδραση σε περιστατικά υψηλής σοβαρότητας.

Δοκιμή του Πλαισίου Ανταπόκρισης σε Περιστατικά

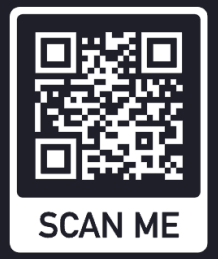
Σκοπός: Η δοκιμή της CSIRT εξασφαλίζει ότι οι διαδικασίες, τα playbooks και η ομάδα λειτουργούν αποτελεσματικά πριν την πραγματική ενεργοποίηση σε περιστατικό. **Βήματα:**

1. **Table-top Άσκηση:** Διεξάγεται ένα σενάριο υψηλού επιπέδου, χρησιμοποιώντας ένα ή περισσότερα playbooks. Η ομάδα εξετάζει τη διαδικασία από την ανίχνευση μέχρι την ανάκαμψη. Δημιουργείται αναφορά με εντοπισμένα κενά, προτάσεις τροποποίησης και συμπεράσματα προς τη διοίκηση.
2. **Σύνθετες Δοκιμές:** Red/Blue ή Purple Team άσκηση: η CSIRT αντιμετωπίζει εξουσιοδοτημένες δοκιμές διείσδυσης. Επιτρέπει αξιολόγηση των playbooks, της αντίδρασης της ομάδας και της ανθεκτικότητας της υποδομής.
3. **Συνεχής Εκπαίδευση:** Τα βασικά μέλη της CSIRT εκπαιδεύονται σε αναδυόμενες απειλές, τεχνικές ψηφιακής εγκληματολογίας και εργαλεία. Τα υποστηρικτικά τεχνικά μέλη ενημερώνονται τακτικά για εργαλεία και τεχνικές συλλογής αποδεικτικών στοιχείων. Το υπόλοιπο προσωπικό συμμετέχει σε table-top ασκήσεις για να εξοικειωθεί με τις διαδικασίες.
4. **Αναθεώρηση και Συντήρηση:** Ετήσια αναθεώρηση του σχεδίου αντιμετώπισης περιστατικών και των playbooks. Προσαρμογή playbooks σε νέες απειλές ή αλλαγές στην υποδομή ή την οργανωτική δομή. Οποιαδήποτε σημαντική αλλαγή ή νέο playbook οδηγεί σε νέα table-top άσκηση για επικύρωση.
5. **Οφέλη:** Διασφαλίζεται ότι η CSIRT είναι επιχειρησιακά έτοιμη. Εντοπίζονται και διορθώνονται αδυναμίες πριν την πραγματική κρίση. Η ομάδα παραμένει εκπαιδευμένη και έτοιμη για νέες ή σύνθετες απειλές.

NMSLab

Ευχαριστώ για την Προσοχή σας!

Dr. Stylianos Karagiannis, PhD



https://nmslab.di.ionio.gr