Incident responders: οι πιλότοι της κυβερνοασφάλειας

Αθανάσιος Πανδής
Μέλος ΑΛΛΗΛΟΝ
IT Engineer, BTech in Telecommunications, BSc in Computer Science, MSc in Information Security & Computer Forensics
Athanasios Pandis | Linkedin

Περίληψη

Οι Incident Responders, όπως οι πιλότοι μαχητικών, βρίσκονται στην πρώτη γραμμή της «ψηφιακής μάχης». Σε ένα τοπίο συνεχώς εξελισσόμενων κυβερνοεπιθέσεων, απαιτείται ταχύτητα, αποφασιστικότητα και ρεαλιστική εκπαίδευση. Δεν υπάρχει χρόνος για αμφιβολία ή μελέτη πρωτοκόλλων η αμεσότητα και η εμπειρία καθορίζουν την επιτυχία. Η φιλοσοφία «Train as you fight» υπογραμμίζει ότι η σωστή προετοιμασία επιτρέπει μια γρήγορη, στοχευμένη αντίδραση, σώζοντας πολύτιμο χρόνο και αποτρέποντας κρίσιμες ζημιές. Έτσι, οι Incident Responders αναδεικνύονται σε «πιλότους» του ψηφιακού κόσμου, έτοιμοι να διαχειριστούν οποιαδήποτε κρίση χωρίς δισταγμό.

Η κυβερνοασφάλεια, σε έναν κόσμο που εξαρτάται από την τεχνολογία και το διαδίκτυο, έχει γίνει ένας από τους πιο κρίσιμους τομείς. Καθώς οι επιθέσεις στο διαδίκτυο γίνονται πιο εξελιγμένες και απειλητικές, οι Incident Responders, δηλαδή οι επαγγελματίες που αναλαμβάνουν την αποκατάσταση της ασφάλειας μετά από μια κυβερνοεπίθεση, έχουν αναδειχθεί σε απαραίτητους «μαχητές» στον ψηφιακό πόλεμο. Αν και ο τομέας της κυβερνοασφάλειας περιλαμβάνει πολλές διαφορετικές πτυχές, οι Incident Responders βρίσκονται στην πρώτη γραμμή, έτοιμοι να διαχειριστούν τις πιο επικίνδυνες καταστάσεις.

Η σύνδεση του ρόλου τους με τον τομέα της Πολεμικής Αεροπορίας είναι άμεση, και η σύγκριση των Incident Responders με τους πιλότους μαχητικών αεροσκαφών είναι εξαιρετικά αποκαλυπτική. Η εμπειρία που απέκτησα από την Πολεμική Αεροπορία με δίδαξε ότι οι κατάλληλοι χειρισμοί σε καταστάσεις πίεσης και κρίσης απαιτούν ψυχραιμία, εκπαίδευση και, κυρίως, ταχύτητα αντίδρασης. Όπως λέει και ο Maverick στην ταινία **Top Gun: Maverick, "Do not think, just do. If you think, you're dead."** Στο πεδίο της κυβερνοασφάλειας, αυτή η φράση αποκτά ολοκληρωμένο νόημα.

Ο Χρόνος: Ο Μεγαλύτερος Αντίπαλος

Όταν η κρίσιμη στιγμή φτάνει και ο κόσμος γύρω σου καταρρέει, ο χρόνος είναι ο εχθρός σου. Η διαφορά μεταξύ της επιτυχίας και της αποτυχίας μπορεί να είναι απλά δευτερόλεπτα. Η φράση **"If you think, you're dead"** αποτελεί την απόλυτη αλήθεια για τους Incident Responders. Όταν μια κυβερνοεπίθεση ξεκινά, δεν υπάρχει χώρος για αμφιβολίες ή για αναβολές. **"Do not think, just do"** – είναι η βασική αρχή που καθοδηγεί κάθε Incident Responder.

Σε κάθε περιστατικό, ο χρόνος για να αντιδράσεις είναι περιορισμένος. Οι κυβερνοεπιθέσεις συχνά εξαπλώνονται γρήγορα, παρακάμπτοντας τα παραδοσιακά συστήματα ασφαλείας και προκαλώντας τεράστιες ζημιές. Σε αυτές τις καταστάσεις, η γρήγορη και αποφασιστική αντίδραση είναι το κλειδί για την αποτροπή μεγαλύτερων επιπτώσεων. Όταν το σύστημα υφίσταται επίθεση, δεν υπάρχει χρόνος για να διαβάσεις τις πολιτικές και τα πρωτόκολλα της εταιρείας. Όπως στην Πολεμική Αεροπορία, **"train as you fight"**. Όλες οι προετοιμασίες και οι εκπαίδευση πραγματοποιούνται υπό συνθήκες ρεαλιστικής πίεσης και σεναρίων, έτσι ώστε όταν η στιγμή της κρίσης έρθει, να μπορείς να αντιδράσεις με τον ίδιο ακριβώς τρόπο όπως αν ήταν πραγματική αποστολή.

Εκπαίδευση και Τακτική: «Train as You Fight»

Η φράση **"Train as you fight"** είναι βαθιά ριζωμένη στην εκπαιδευτική φιλοσοφία της Πολεμικής Αεροπορίας. Η έννοια πίσω από αυτήν είναι ότι η εκπαίδευση πρέπει να προσομοιώνει όσο το δυνατόν περισσότερο

τις πραγματικές συνθήκες ενός πολέμου ή μιας κρίσης. Αυτή η φιλοσοφία βρίσκει άμεση εφαρμογή στον τομέα της κυβερνοασφάλειας. Όπως οι πιλότοι εκπαιδεύονται με ασκήσεις προσομοίωσης πολεμικών καταστάσεων, έτσι και οι Incident Responders υποβάλλονται σε συνεχείς ασκήσεις και σενάρια που προσομοιώνουν κυβερνοεπιθέσεις.

Οι **red team/blue team** ασκήσεις είναι ένα παράδειγμα αυτού του τύπου προσομοίωσης. Οι ομάδες επιτίθενται και αμύνονται με στόχο να αναπτύξουν καλύτερες στρατηγικές και να εντοπίσουν αδυναμίες που ενδέχεται να υπάρχουν στα συστήματα ασφαλείας. Οι Incident Responders δεν εκπαιδεύονται μόνο για να κατανοούν τις διαδικασίες αποκατάστασης των συστημάτων, αλλά και για να αντιλαμβάνονται τα «σημάδια» μιας επίθεσης πολύ πριν αυτή εξελιχθεί σε κρίσιμο σημείο.

Όπως το γνωρίζουμε και από την Πολεμική Αεροπορία, όταν η στιγμή της κρίσης έρθει, η εκπαίδευση πρέπει να έχει εδραιώσει τις αντιδράσεις σου. Οι σωστές αποφάσεις δεν παίρνονται με βάση την αναζήτηση πληροφοριών ή τη μελέτη της πολιτικής της εταιρείας – πρέπει να είναι αυθόρμητες και να προκύπτουν από την εμπειρία και την προετοιμασία.

Ο Ρόλος του Incident Responder: Ο Πιλότος στον Ψηφιακό Πόλεμο

Ο Incident Responder έχει τον ρόλο του «πιλότου μαχητικού αεροσκάφους» στον ψηφιακό πόλεμο. Όπως οι πιλότοι επιφυλακής αναλαμβάνουν αποστολές υψηλού ρίσκου, έτσι και οι Incident Responders πρέπει να αναλάβουν την ευθύνη να αποκαταστήσουν την ασφάλεια, να εντοπίσουν την πηγή της επίθεσης και να αποτρέψουν την εξάπλωσή της. Η διαφορά είναι ότι σε αυτή την περίπτωση, οι αποστολές δεν εκτελούνται στον αέρα, αλλά μέσα σε υπολογιστικά δίκτυα και ψηφιακά συστήματα.

Η σύγκριση είναι εύκολη: Ο πιλότος πρέπει να έχει γρήγορη αντίληψη, να παίρνει γρήγορες αποφάσεις και να έχει άριστη γνώση του αεροσκάφους του. Το ίδιο ισχύει και για τον Incident Responder, που πρέπει να έχει πλήρη γνώση του συστήματος που προστατεύει, να αντιδράσει γρήγορα και να αντιμετωπίσει οποιαδήποτε κρίση προκύψει χωρίς να παραλύει από την πίεση.

Οι Incident Responders πρέπει να γνωρίζουν ότι η επιτυχία τους δεν εξαρτάται μόνο από την ταχύτητα με την οποία ενεργούν, αλλά και από την ικανότητά τους να διαχειριστούν το άγνωστο. Όπως σε έναν πόλεμο, οι αντιδράσεις δεν βασίζονται μόνο σε προκαθορισμένα σχέδια, αλλά και σε αυτοσχεδιασμούς. Αυτό είναι κάτι που μαθαίνεται μόνο μέσω της συνεχούς εκπαίδευσης και της πρακτικής.

Η Προετοιμασία είναι το Κλειδί για την Επιτυχία

Το σημαντικότερο μάθημα από την εμπειρία στην Πολεμική Αεροπορία, και που ισχύει και στην κυβερνοασφάλεια, είναι ότι η προετοιμασία είναι το παν. Όταν η κρίσιμη στιγμή φτάσει, δεν υπάρχει χρόνος για να διαβάσουμε τις πολιτικές και τα πρωτόκολλα. Όπως ένας πιλότος που πρέπει να ανταποκριθεί άμεσα σε έκτακτη κατάσταση χωρίς να έχει το περιθώριο να κοιτάξει τα εγχειρίδια, έτσι και οι Incident Responders πρέπει να είναι πλήρως προετοιμασμένοι να αναλάβουν δράση χωρίς καθυστέρηση.

Η εμπειρία δείχνει ότι οι Incident Responders που έχουν περάσει μέσα από σενάρια «πραγματικών» επιθέσεων, είναι πιο ικανοί να διαχειριστούν τις καταστάσεις με ψυχραιμία. Είναι ικανότατοι να αξιολογούν την κατάσταση με ακρίβεια και να ενεργούν με γρήγορη αντίληψη, αποφεύγοντας την παγίδα της καθυστερημένης αντίδρασης.

Συμπέρασμα: Είσαι Έτοιμος για την Μάχη;

Ο κόσμος της κυβερνοασφάλειας, όπως και ο κόσμος της Πολεμικής Αεροπορίας, απαιτεί αποφασιστικότητα, ταχύτητα και εκπαίδευση. Οι Incident Responders είναι οι «πιλότοι» του ψηφιακού κόσμου, αναλαμβάνοντας αποστολές σε συνθήκες υψηλής πίεσης και με απόλυτη ετοιμότητα να ανταπεξέλθουν σε κάθε κρίση που μπορεί να προκύψει. Το κάλεσμα για αυτούς είναι ξεκάθαρο: **"Train as you fight"**, γιατί όταν η ώρα της μάχης έρθει, δεν υπάρχει χρόνος για να διαβάσουμε πολιτικές ή πρωτόκολλα. Στην κυβερνοασφάλεια, η αντίδραση είναι το παν – και για να αντιδράσεις σωστά, πρέπει να έχεις εκπαιδευτεί για κάθε ενδεχόμενο.