Του Δρ. Διονύση Μουζάκη
Επιστημονικός Συνεργάτης & Επιθεωρητής
TÜV HELLAS (TÜV NORD)

Μέθοδοι περιορισμού των **κινδύνων διαρροής δεδομένων** και αποφυγής **μη συμμόρφωσης** με τον **ΓΚΠΠΔ (GDPR)**

Ποια είναι τα βασικά μέτρα που πρέπει να πάρει ένας οργανισμός για ανιχνεύει τις κυβερνο-επιθέσεις νωρίς και να αποφύγει τα πρόστιμα του ΓΚΠΠΔ;

Τα παρακάτω 10 μέτρα μπορούν να παρέχουν μια καλή βάση για την έγκαιρη ανίχνευση κυβερνο-επιθέσεων και επομένων να περιορίσει τον κίνδυνο προστίμων επιδεικνύοντας προβλεψιμότητα και υπευθυνότητα στην ασφάλεια των προσωπικών δεδομένων.

Έλεγχος του Website σε μόνιμη βάση

Έλεγχοι ρουτίνας πρέπει να γίνονται σε ημερήσια βάση αναζητώντας περίεργες αλλαγές στις σελίδες, για παράδειγμα ένα καινούργιο περίεργο κείμενο με κάποιο σύνδεσμο, σφάλματα PHP μπορεί να παραπέμπουν σε κυβερνο-επίθεση

Τακτική παρακολούθηση των συναγερμών (χρήσης) του Website

Αυτό που χαρακτηρίζει τις κυβερνο-επιθέσεις σε ένα Website είναι συγκεκριμένο 'σχήμα' στην ροή των προσβάσεων (Access Traffic) η οποία συνήθως στην εκδήλωση της επίθεσης παρουσιάζει απότομη έως και δραματική αύξηση σε μικρό χρονικό διάστημα (Spike) οπότε η συνεχής παρακολούθηση θα εντοπίσει ένα η περισσότερα Spikes και μπορεί να οδηγήσει στην αποκάλυψη της κυβερνο-επίθεσης.

Χρήση λογισμικού ανίχνευσης απειλών

Τα κορυφαία λογισμικά του είδους μπορούν να ανιχνεύσουν εισβολές μέσα σε λεπτά από την εκδήλωσή τους, είναι μια επένδυση που αξίζει τον κόπο, αφού μπορεί να προλάβει πρόστιμα και κακή δημοσιότητα του οργανισμού που δέχεται την επίθεση λόγω υπέρβασης του ορίου των 72 ωρών για ενημέρωση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και των εμπλεκομένων υποκείμενων επεξεργασίας. Στην περίπτωση αυτή η άγνοια του συμβάντος δεν γίνεται αποδεκτή από την ΑΠΔΠΧ, το μόνο που θα μετρήσει θετικά είναι εφόσον ο οργανισμός που δέχτηκε την επίθεση μπορέσει να τεκμηριώσει ότι έλαβε όλα τα Τεχνικά και οργανωτικά μέτρα που απαιτούνται προκειμένου να αποτρέψει την επίθεση και την διαρροή.

Χρήση της τεχνικής του «βάζου με το μέλι»

Ουσιαστικά με την τεχνική αυτή δημιουργούνται περιοχές στο δίκτυο του οργανισμού που εμφανίζουν να περιέχουν δεδομένα χρήσιμα σε ένα επιτιθέμενο, ακριβώς για να τραβήξουν την προσοχή του, στην πραγματικότητα είναι δολώματα και τα δεδομένα που περιέχουν είναι άχρηστα στον επιτιθέμενο αλλά ενεργοποιούν συναγερμούς στο σύστημα κυβερνοασφάλειας του οργανισμού οπότε η επίθεση μπορεί να αντιμετωπισθεί στην εκδήλωση της χωρίς να προλάβει να επεκταθεί σε χρήσιμα δεδομένα.

Μάθε από το παρελθόν για να προβλέψεις μελλοντική επίθεση.

Οι κυβερνο-εγκληματίες μαθαίνουν από τη εμπειρία από επιτυχημένες επιθέσεις σε επιχειρήσεις και οργανισμούς οπότε αξίζει τον κόπο να χρησιμοποιηθούν τα συμπεράσματα από επιτυχημένες επιθέσεις όσο και αν είναι επώδυνη η διαδικασία. Οι κυβερνο-εγκληματίας αρέσκονται στο να χτυπούν τον ίδιο οργανισμό πάνω από μία φορά και μάλιστα με την ίδια μέθοδο. Λαμβάνοντας μέτρα ασφαλείας βασισμένα σε προηγούμενη επιτυχημένη επίθεση μπορεί να οδηγήσει σε άμεση ανίχνευση μιας καινούργιας.

Εκπαίδευση του προσωπικού.

Διατηρώντας το προσωπικό εκπαιδευμένο και ενήμερο σχετικά με τις κυβερνο-απειλές κάνει πολύ ποιο πιθανή την κατανόηση μίας επίθεσης και λιγότερο πιθανό το κλικάρισμα σε ένα καλά καμουφλαρισμένο phishing email

Τέλος αν και τα παραπάνω θα βοηθήσουν να μειωθεί ο χρόνος αναγνώρισης μιας κυβερνο-επίθεσης αξίζει να επενδύσει ένας οργανισμός σε πόρους για να αποτρέψει μια επίθεση. Οι κυβερνο-εγκληματίες αναζητούν Websites με αδυναμίες ασφάλειας όπως το να μην έχουν επικαιροποιημένο λογισμικό. Με την εγκατάσταση όλων των τελευταίων επικαιροποιήσεων μειώνεται αρκετά η πιθανότητα να ασχοληθεί ένας κυβερνο-εγκληματίας με το Website, απλά θα αναζητήσει έναν ευκολότερο στόχο. Στατιστική έρευνα σε 60,000 Websites απέδειξε ότι το 78% ήταν ευάλωτες σε επιθέσεις και ο λόγος ήταν μη εγκατεστημένες επικαιροποιήσεις.

Εντοπισμός διαρροών σε επίπεδο συστημάτων και εφαρμογών.

Εντοπισμός Διαρροής - Βασικό ρόλο στην αντιμετώπιση των διαρροών και φυσικά στη συμμόρφωση με τον Κανονισμό

παίζει το πως ανιχνεύονται οι διαρροές. Στην απλούστερη μορφή τους αν το προσωπικό ενός οργανισμού διαπιστώσει ότι κατά λάθος έχει εκθέσει προσωπικά δεδομένα αυτό θα μπορούσε να λειτουργήσει σαν εντοπισμός διαρροής. Στον αντίποδα συστήματα ασφάλειας και παρακολούθησης δεδομένων μπορούν να εντοπίσουν και να ενημερώσουν για μια διαρροή προσωπικών δεδομένων.

Προκειμένου αυτό να γίνει με επιτυχία απαιτεί την ύπαρξη των κατάλληλων μηχανισμών ελέγχου (οπως εξάλλου απαιτείται από τον GDPR) που επιτρέπουν την ανίχνευση και την αντιμετώπιση συμβάντων ασφάλειας. Ένα ακόμα χειρότερο σενάριο είναι η αποτυχία της ανίχνευσης της διαρροής λόγω της ανυπαρξίας των κατάλληλων μηχανισμών ελέγχου, αλλά κάποιος τρίτος φορέας την ανακαλύπτει και την δημοσιοποιεί, αυτό μπορεί να οδηγήσει σε πολύ υψηλά πρόστιμα (2% το ετήσιο εσόδου η €10 εκατομμύρια οποιοδήποτε είναι μεγαλύτερο).

Ανταπόκριση σε διαρροή δεδομένων = αποτελεσματικές διαδικασίες ασφάλειας δεδομένων.

Το ερώτημα είναι τι κάνει μία διαδικασία αποτελεσματική; Βασικό στην περίπτωση αυτή είναι η σωστή προετοιμασία και η δημιουργία αποτελεσματικού και δοκιμασμένου σχεδίου αντιμετώπισης. Το σχέδιο αντιμετώπισης διαρροής δεδομένων θα πρέπει να περιλαμβάνεται στο Πλάνο Αντιμετώπισης Απειλών Πληροφοριακών Συστημάτων, ΠΑΑΠΣ (Cyber Incident Response Plan CIRP). Το ΠΑΑΠΣ τεκμηριώνει και αποδεικνύει ότι ένας οργανισμός έχει διερευνήσει όλες τις πιθανές απειλές ασφαλείας των πληροφοριακών συστημάτων του (Risk Assessment/Risk Treatment Plan) και έχει εκπονήσει και οργανώσει τις κατάλληλες διαδικασίες για να τις αντιμετωπίσει. Ένα καλό ΠΑΑΠΣ θα καλύψει πολλές και διαφορετικές πηγές ανίχνευσης, πολλές δεν είναι καν πληροφοριακά συστήματα. Στην πραγματικότητα ένα ΠΑΑΠΣ θα πρέπει να είναι σε θέση να ελέγξει απειλές και συμβάντα που αφορούν τόσο ένα χαμένο φωριαμό αρχειοθέτησης όσο και την εισβολή σε ένα ψηφιακό δίκτυο.

Θα πρέπει να ξεκινήσει από την κατανόηση/χαρτογράφηση ενός οργανισμού και των απειλών που αντιμετωπίζει καθώς και τις προκύπτουσες απαιτήσεις για την αντιμετώπιση τους. Στην πραγματικότητα η υποχρέωση του οργανισμού για ενημέρωση τυχόν συμβάντων ασφάλειας δεδομένων τόσο νομικά όσο και κανονιστικά είναι απλά η κορυφή το παγόβουνου. Ένα ισχυρό ΠΑΑΠΣ καλύπτει ένα μεγάλο φάσμα θεμάτων μεταξύ άλλων, διαδικασίες αποφάσεων σε καταστάσεις κρίσης, σχέσεις με τα ΜΜΕ, μεθόδους και διαδικασίες περιορισμού του αντικτύπου στις εργασίες, ενσωματωμένη ασφαλιστική κάλυψη, καθορισμός ρόλων και πως να οργανώσεις την ανταπόκριση 'εν θερμώ' σε στιγμές κρίσης.

Στην Ευρώπη έχουμε βιώσει πολλές διαρροές δεδομένων, που κατέληξαν να εξελιχθούν σε πολύ ποιο σοβαρά γεγονότα από απλές διαρροές πληροφοριακών συστημάτων. Πολλά δημόσια γεγονότα όπως η διαρροή TalkTalk και τα όσα επακολούθησαν θα πρέπει να παρακινήσουν ένα οργανισμό να πάρει απειλές αυτού του είδους στα σοβαρά. Αν αυτό δεν έχει ήδη συζητηθεί στο διοικητικό συμβούλιο του οργανισμού σας, θα πρέπει να γίνει άμεσα και να οριστεί (αν δεν υπάρχει) ομάδα αντιμετώπισης κρίσεων (Crisis Management Team) που θα περιλάβει αυτές τις απειλές στο Business Continuity Plan του οργανισμού. Οργανισμοί που η μετοχή τους διαπραγματεύεται δημόσια έχουν ήδη εγγράψει αυτό το ρίσκο στην ετήσια έκθεση προς τους μετόχους.

Ένα εμπεριστατωμένο ΠΑΑΠΣ θα αντιμετωπίζει και άλλους τύπου πληροφοριακού ρίσκου. Η επένδυση που απαιτείται για την δημιουργία ενός τέτοιου συστήματος μπορεί να αποσβεστεί από την χρόνια προστιθέμενη αξία που προσφέρει στον οργανισμό εφόσον όμως ελέγχεται η λειτουργία του και ενημερώνεται κανονικά.

Παρ' όλα αυτά ακόμα και αν η τεχνολογία προστασίας δεδομένων ενός οργανισμού είναι σε θέση να ανίχνευση το 95% των συνηθισμένων επιθέσεων και η ικανότητα παρακολούθησής είναι σε θέση να ανακαλύψει κάθε ανώμαλη συμπεριφορά στο δίκτυο του οργανισμού, αυτό από μόνο του δεν είναι αρκετό όταν μιλάς για το GDPR. Τα άτομα και η διαδικασίες είναι εξίσου σημαντικά.

Ο λόγος γι' αυτό είναι η απαίτηση των 72 ωρών για την ενημέρωση των αρχών και των υποκειμένων για μια διαρροή. Αυτή ουσιαστικά καθορίζει τις προδιαγραφές για το σύστημα παρακολούθησης της ασφάλειας των δεδομένων, το σύστημα ανίχνευσης και αναφοράς διαρροής δεδομένων των σχετικών διαδικασιών που έχουν καθοριστεί από τον οργανισμό και έχουν τεκμηριωθεί στο ΠΑΑΠΣ.

Όμως αν δεν έχουν καθοριστεί αρμοδιότητες και διαδικασίες που θα εξασφαλίζουν ότι διαρροές προσωπικών δεδομένων θα ανιχνεύονται, θα περιορίζονται και θα αναφέρονται στον Data Protection Officer είναι σχεδόν αδύνατο να κατατεθεί αναφορά στην ΑΠΔΠΧ εντός 72 ωρών. Αυτό είναι ακόμα ποιο δύσκολο σε μεγάλους οργανισμούς διεσπαρμένους σε μεγάλη γεωγραφική έκταση και χρονικές ζώνες. Η αναφορά στην ΑΠΔΠΧ μπορεί να γίνει και μετά τις 72 ώρες εφόσον ο λόγος της καθυστέρησης μπορεί νομικά να τεκμηριωθεί. Η αδυναμία αναφοράς εντός 72 ωρών στις αρχές το λιγότερο θα οδηγήσει σε μια σε βάθος επιθεώρηση (Audit) της εφαρμογής του Κανονισμού από τον Οργανισμού εκ μέρους της ΑΠΔΠΧ. Τα βασικά βήματα είναι να ξέρεις τα δεδομένα σου, να έχεις χαρτογραφήσει τα προσωπικά δεδομένα και που αυτά βρίσκονται μέσα στην ¨περίμετρο¨. Όμως πολύ σημαντικό είναι να υπάρχει χαρτογράφηση για τα προσωπικά δεδομένα και έξω από την περίμετρο, για παράδειγμα στο Cloud. Αυτό επιτρέπει να απαιτείς από τους τρίτους επεξεργαστές (processors) προσωπικών δεδομένων, όπως προμηθευτές υπηρεσιών υπολογιστικού νέφους (Cloud), να υπογράψουν συμφωνίες επεξεργασίας δεδομένων (Data Processing Agreements) προκειμένου να κάνουν αναφορές διαρροών που ανιχνεύουν αρκετά γρήγορα ώστε να μπορεί ο υπεύθυνος επεξεργασίας (controller) οργανισμός να κάνεις αναφορά διαρροής στις αρχές εντός του "παραθύρου" των 72 ωρών.

Υπάρχει ένα επιπλέον βήμα και αυτό είναι ο έλεγχος (Testing, Internal Auditing, Pen tests etc). Είναι σημαντικό να υπάρχει ένα πλαίσιο με μηχανισμούς τεχνικών ελέγχων, πολιτικές, ατόμων και διαδικασιών που έχουν ελεγχθεί σε σχέση με πραγματικά σενάρια. Σίγουρα η στιγμή που αποκαλύπτεται μια διαρροή δεν είναι κατάλληλη για να ανακαλύψει κανείς ότι η διαδικασίες που έχει ορίσει για τον περιορισμό της διαρροής, την εξουδετέρωση της διαρροής, την ανάκαμψη μετά την διαρροή και η αναφορά δεν λειτουργούν όπως αναμενόταν.

8 απλά βήματα για την αντιμετώπιση διαρροών.

Έχει παρατηρηθεί ότι κατά μέσο όρο ένας οργανισμός χρειάζεται 191 ημέρες η 6 μήνες μέχρι να ανιχνεύσει μια διαρροή δεδομένων (2017 Costs OF Data Breach Study, Ponemon Institute). Εφόσον μια διαρροή ανιχνευτεί έγκαιρα ένας οργανισμός μπορεί ελέγξει την κατάσταση πχ δημιουργώντας γραμμή επικοινωνίας για την παροχή βοήθειας προς τους χρήστες που έχουν υποστεί επίθεση η στέλνοντας email ώστε να συντονίσει την αλλαγή των Passwords, να τους προτρέψει να ελέγχουν για ψευδείς τραπεζικές συναλλαγές, να εγγραφούν σε υπηρεσίες παρακολούθησης πιστώσεων η ότι άλλο απαιτείται παίρνοντας μέτρα προστασίας.

Προκειμένου ένας οργανισμός να βοηθηθεί ώστε να ανιχνεύσει μια διαρροή το γρηγορότερό θα πρέπει:

1. **Να καλέσει ειδικούς κυβερνοασφάλειας:** Αυτό αν και προφανές σημαίνει ότι ένας οργανισμός πρέπει να έχει προσλάβει ικανό αριθμό ειδικών στην κυβερνοασφάλειας πριν να υπάρξει διαρροή.
2. **Να φροντίσει να δημιουργήσει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών** κατά τα πρότυπα ISO/IEC27001, προστασίας προσωπικών δεδομένων ISO/IEC 27701 και επιχειρησιακής συνέχειας ISO/IEC 22301.
3. **Να κρατά συστήματα και χρήστες ενήμερους στις τελευταίες εξελίξεις στην κυβερνοασφάλεια:** Το περιβάλλον των κυβερνοαπειλών συνεχώς βελτιώνεται με αποτέλεσμα
4. **να απαιτείται ένας οργανισμός να εξελίσσεται μαζί του.** Αυτό σημαίνει ότι απαιτείτε ο οργανισμός να εξελίσσεται παράλληλα κρατώντας ενήμερα συστήματα και άτομα.
5. **Να χρησιμοποιεί ενήμερα ΄εργαλεία΄ ανίχνευσης διαρροών.**
6. **Ο οργανισμός θα πρέπει χρησιμοποιεί και να αξιοποιεί γενικές πληροφορίες έρευνας κυβερνοασφάλειας:** Σε αυτή την περίπτωση έχει παρατηρηθεί ότι οργανισμοί που αξιοποιούν γενικές πληροφορίες κυβερνοασφάλειας ανταποκρίνονται γρηγορότερα και με μεγαλύτερη ακρίβεια σε περίπτωση διαρροής.
7. **Παρακολούθηση των δεδομένων του οργανισμού:** Προκειμένου να μπορέσουν οι ειδικοί να αναλύσουν μια διαρροή θα πρέπει να λάβουν γνώση βασικών παραμέτρων που να αποδεικνύουν την διαρροή. Αυτό περιλαμβάνει τηλεμετρία σε επίπεδο δικτύου, και ημερολόγια χρήσης (logs) από τα συστήματα των υποδομών, των εφαρμογών και της ασφάλειας.
8. **Παρακολούθηση και συλλογή πληροφοριών από εκστρατείες επιθέσεων:** Τα συμβατικά προϊόντα ανίχνευσης κακόβουλων εφαρμογών (malware) επιτρέπουν την ανίχνευση στιγμιαίων γεγονότων επίθεσης δημιουργώντας απλές αναφορές. Αυτό συχνά σημαίνει ότι ειδικοί στην κυβερνο-ασφάλεια αφήνονται να προσπαθούν να αναλύσουν ένα ατελείωτο πλήθος από άσχετους και φαινομενικά ασύνδετους συναγερμούς από συμβάντα. Αντίθετα αν η ανίχνευσή γίνεται σε επίπεδο εκστρατείας κακόβουλων επιθέσεων ο οργανισμός έχει την ¨μεγάλη¨ εικόνα από την κακόβουλη εκστρατεία ώστε να ανιχνεύσει την διαρροή εγκαίρως,
9. **Ο Οργανισμός διατηρεί το προσωπικό σε επίγνωση του κινδύνου με συστηματική εκπαίδευση:** Η αμέλεια είναι συχνά ένας σημαντικός παράγοντας που υποθάλπει τις διαρροές. Ο οργανισμός θα πρέπει τακτικά να εκπαιδεύει το προσωπικό του στο πως να αναγνωρίζει μια επίθεση αλλά και αδυναμίες του συστήματος καθώς και τι πρέπει να κάνουν σε μια τέτοια περίπτωση. Η εκπαίδευση θα πρέπει να γίνετε τουλάχιστον μία φορά το χρόνο. ITSecurity