Ιωάννης Λάλος
Chief Security Consultant Syntax
www.syntax.gr

Χρόνοι απόκρισης σε **Data Breach**

Οι εταιρείες υφίστανται πιέσεις για να διατηρούν τα δεδομένα τους ασφαλή, ενώ ταυτόχρονα πρέπει να ενεργούν με ταχύτητα και διαφάνεια σε περίπτωση παραβίασης των δεδομένων τους

Ο μεγάλος χρόνος ανταπόκρισης σε παραβιάσεις συνεπάγεται σε πρόστιμα από πολλαπλές κρατικές και διεθνείς κανονιστικές οντότητες, απώλεια παραγωγικού επιχειρησιακού χρόνου και εμπιστοσύνης των πελατών. Αυτές οι παραβιάσεις αποκτούν μεγαλύτερη δημοσιότητα και αυξάνονται με το πέρασμα του χρόνου.
Ένα πλήρες **Incident Response Plan περιλαμβάνει τα εξής 6 βήματα** : Preparation, Identification, Containment, Eradication, Recovery, Review Lessons Learned.

Τι είναι ένα Data Breach Response Plan;

Ένα Data Breach Response Plan αποτελεί τη στρατηγική που θα τεθεί σε εφαρμογή στο ενδεχόμενο ενός Data Breach ώστε να μειωθεί ο αντίκτυπός του. Μία σωστά σχεδιασμένη στρατηγική εξασφαλίζει ότι κάθε άτομο σε μια εταιρεία γνωρίζει τον ρόλο του κατά τη διάρκεια μιας παραβίασης για να την ανακαλύψει, να απαντήσει και να την περιορίσει εγκαίρως.
Ένα σωστό Data breach response plan, εξασφαλίζει ηρεμία κατά τη διάρκεια μιας κρίσης αφού τα βήματα έχουν ήδη δοκιμαστεί και διατυπωθεί, σε αντίθεση με την διαμόρφωση ενός σχεδίου εν μέσω παραβίασης. Το κόστος των data breaches καθώς και ο όγκος των δεδομένων που αποσπώνται συνεχώς αυξάνεται. Κατά μέσο όρο, οι εταιρείες χρειάζονται περίπου 197 ημέρες για να εντοπίσουν μια παραβίαση και 69 ημέρες για να την περιορίσουν.
Παράγοντες που επηρεάζουν τον χρόνο απόκρισης σε ένα data breach είναι:

- **Ετοιμότητα**
- **Τεχνολογίες**
- **Νόμοι περί απορρήτου**

Η ετοιμότητα/προετοιμασία, οι τεχνολογίες και η τήρηση των νόμων για την προστασία της ιδιωτικότητας έχουν αξιοσημείωτο αντίκτυπο στον χρόνο απόκρισης μιας επιχείρησης.

Ετοιμότητα

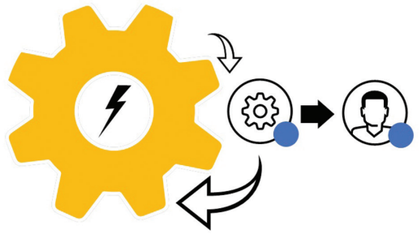
Από πολλές μελέτες προκύπτει ότι επιχειρήσεις που έχουν επενδύσει στον τομέα της ασφάλειας ανακάμπτουν ταχύτερα έπειτα από ένα περιστατικό data breach. Επιχειρήσεις με υψηλό επίπεδο ασφάλειας χαρακτηρίζονται οι εξής:

- Επιχειρήσεις που έχουν καθιερώσει έναν CISO (Chief Information Security Officer)
- Επιχειρήσεις που έχουν επαρκή προϋπολογισμό για την στελέχωση τμήματος security και επενδύουν σε τεχνολογίες ασφαλείας.
- Επιχειρήσεις που επενδύουν στρατηγικά σε κατάλληλες τεχνολογίες ασφαλείας.
- Επιχειρήσεις που πραγματοποιούν προγράμματα εκπαίδευσης και ευαισθητοποίησης που αποσκοπούν στην μείωση της αμέλειας των εργαζομένων.
- Επιχειρήσεις που πραγματοποιούν τακτικούς ελέγχους (Internal Audits, Vulnerability Assessments, Penetration Tests)
- Επιχειρήσεις που διατηρούν ένα ολοκληρωμένο πρόγραμμα με πολιτικές

Οι επιχειρήσεις με τα παραπάνω χαρακτηριστικά τείνουν να αντιδρούν άμεσα σε data breaches και να ανακάμπτουν από το περιστατικό σε ελάχιστο χρόνο. Αυτό επιδεικνύει ότι ο συνολικός σχεδιασμός είναι η ειδοποιός διαφορά μεταξύ μιας δαπανηρής και μίας παραβίασης με ελάχιστές επιπτώσεις

Τεχνολογίες

Οι τεχνολογίες που υλοποιούν οι επιχειρήσεις αποτελούν καθοριστικό παράγοντα στον χρόνο απόκρισης τους, ειδικότερα η αυτοματοποίηση της ασφάλειας.
Η αυτοματοποίηση διαφορετικών εργασιών ασφαλείας εξοικονομεί χρόνο και χρήμα με διάφορους τρόπους. Η αυτοματοποίηση βοηθάει στην γρήγορη ολοκλήρωση χρονοβόρων εργασιών που αναλώνουν το χρόνο του προσωπικού ασφαλείας από άλλες επιχειρησιακές δραστηριότητες. Επίσης ο αυτοματισμός εξαλείφει την πιθανότητα ανθρώπινου σφάλματος και αυξάνει τις πιθανότητες ανίχνευσης ενός περιστατικού ασφαλείας. Αυτός είναι και ο λόγος που οι λύσεις ασφαλείας που παρέχουν μια πανοραμική εικόνα στα δεδομένα των επιχειρήσεων είναι ζωτικής σημασίας για την στρατηγική της αντιμετώπιση περιστατικών data breach.



Ενδεικτικές Τεχνολογίες που βοηθούν σε αυτοματοποίηση και αντιμετώπιση data breaches

- **Hardware Authentication**
- **Data Loss Prevention**
- **Data Encryption**
- **Security Information and Event Management**
- **User Behavior Analytics**

Νόμοι περί απορρήτου

Πλέον με την επιβολή νόμων και κανονισμών (GDPR, ePrivacy, NIS κτλη) επηρεάζονται πολλές πτυχές μιας επιχείρησης. Αυτοί οι κανονισμοί έχουν συχνά ειδικούς κανόνες για χρόνους αναφοράς περιστατικών
Σύμφωνα με το GDPR για παράδειγμα, απαιτείτε από τις επιχειρήσεις να αναφέρουν συμβάντα data breach εντός 72 ωρών. Η μη συμμόρφωση με αυτό μπορεί να οδηγήσει σε πρόστιμα ύψους 20 εκατομμυρίων ευρώ ή 4% του ετήσιου παγκόσμιου κύκλου εργασιών.
Μόνο με την χρήση των κατάλληλων τεχνολογιών μπορεί μια επιχείρηση να ανταπεξέλθει στους χρόνους αναφοράς περιστατικών. ITSecurity

Σχετικά με την SYNTAX Πληροφορική ΑΒΕΕ
Η SYNTAX Πληροφορική ΑΒΕΕ, www.syntax.gr, ιδρύθηκε το 1994. Αποτελεί τη συνέχεια της εταιρείας Arabian American Information Systems Inc., πρωτοπόρου προμηθευτή λογισμικού και συμβούλου στον τομέα των τεχνολογιών πληροφορικής που λειτούργησε από το 1984 στον Αραβικό Κόλπο. Η SYNTAX εδρεύει στον Χολαργό, Μεσογείων 216, και σε συνεργασία με τις θυγατρικές της, SYNTAX IT Consulting WLL στο Κουβέιτ και SYNTAX Doha IT & Services WLL στο Κατάρ, δραστηριοποιείται στην EMEA.
Η SYNTAX προσφέρει σε μεγάλες επιχειρήσεις και οργανισμούς λογισμικό και συμβουλευτικές υπηρεσίες προσφέροντας τους τη δυνατότητα να αφομοιώνουν τεχνολογίες αιχμής και βέλτιστες πρακτικές, έτσι ώστε να διαφοροποιούνται στην αγορά, να μειώνουν το λειτουργικό τους κόστος, να αποκτούν ανταγωνιστικό πλεονέκτημα και βέλτιστη αποτελεσματικότητα (ROI). Η εταιρεία αναλαμβάνει έργα μελετών, ανάπτυξης, υλοποίησης και υποστήριξης τεχνολογιών αιχμής, λειτουργίας & διαχείρισης συστημάτων IT και εκχωρεί εξειδικευμένο προσωπικό με συμβάσεις ορισμένου χρόνου.
Τομείς εξειδίκευσης: Information Security/GRC & AML/CT - ALCM, Legacy Modernization, RDMBS – IT Operations Management - Business Service & SLA Management - DM & Analytics. Τον κατάλογο των πελατών κοσμούν κορυφαίες μεγάλες επιχειρήσεις και οργανισμοί από όλους τους τομείς της οικονομίας στην EMEA.
Η SYNTAX είναι πιστοποιημένη κατά ISO 9001: 2015 και 27001: 2013 και μέλος των φορέων ΣΕΠΕ, ΣΕΣΜΑ, ITSMF και TMF.