Η IBM ανακοινώνει νέες δυνατότητες στον τομέα ασφάλειας

Η IBM ανακοίνωσε πρόσφατα νέες δυνατότητες αντιμετώπισης περιστατικών – οι οποίες προσφέρονται μέσα από το χαρτοφυλάκιο λύσεων ασφάλειας IBM Resilient – με σκοπό να βοηθήσει τις εταιρείες να ανταποκριθούν στις απαιτήσεις του νέου Ευρωπαϊκού Κανονισμού GDPR, ο οποίος θα τεθεί σε ισχύ στις 25 Μαΐου 2018 και θα επιφέρει μία από τις μεγαλύτερες αλλαγές των τελευταίων δεκαετιών στη νομοθεσία περί προστασίας προσωπικών δεδομένων.

Ο Κανονισμός GDPR απαιτεί σημαντικές αλλαγές στον τρόπο με τον οποίο οι επιχειρήσεις αντιδρούν στις παραβιάσεις που αφορούν δεδομένα καταναλωτών. Για παράδειγμα, οποιαδήποτε επιχείρηση δραστηριοποιείται στην Ευρώπη θα έχει 72 ώρες για να ειδοποιήσει την εποπτική αρχή και τα Υποκείμενα των Δεδομένων (όπως αυτά ορίζονται από τη νομοθεσία) για την παραβίαση, διαφορετικά κινδυνεύει με πρόστιμο ύψους 20 εκατομμυρίων Ευρώ ή μέχρι και το 4 τοις εκατό του συνολικού ετήσιου κύκλου εργασιών της. Μια πρόσφατη έρευνα του Ινστιτούτου Ponemon διαπίστωσε ότι το 75 τοις εκατό των επιχειρήσεων παραδέχονται ότι δεν έχουν επίσημο σχέδιο αντιμετώπισης περιστατικών ασφάλειας στον κυβερνοχώρο (Cyber Security Incident Response Plan – CSIRP) το οποίο να εφαρμόζεται συστηματικά στην επιχείρηση, γεγονός που θέτει ιδιαίτερες προκλήσεις στη συμμόρφωση με τον Κανονισμό GDPR. [1]

Οι νέες δυνατότητες που παρουσιάζει η IBM περιλαμβάνουν:

- **Resilient GDPR Preparatory Guide** . Ένα διαδραστικό εργαλείο που παρέχει βήμα προς βήμα οδηγίες για την ετοιμότητα της επιχείρησης ως προς τον Κανονισμό GDPR. Ο εν λόγω προπαρασκευαστικός οδηγός αξιοποιεί την ευελιξία της πλατφόρμας Resilient IRP (Incident Response Platform) και κάνει την προετοιμασία και το σχεδιασμό μια διαδραστική και δυναμική διαδικασία. Οι εργασίες στον οδηγό μπορούν να τροποποιηθούν ή να ανατεθούν ώστε η επιχείρηση να μπορεί να διαχειρίζεται πιο αποτελεσματικά τη ροή εργασιών, πέρα από την υποχρέωση ενημέρωσης σε περίπτωση παραβίασης. Ο οδηγός καλύπτει όλες τις πλευρές της προετοιμασίας, οι οποίες αποτυπώνονται αναλυτικά, διευκολύνοντας τη μελλοντική παρακολούθηση και τεκμηρίωση.
- **Resilient GDPR Simulation**. Μια νέα λειτουργία της πλατφόρμας Resilient IRP βοηθά τους αναλυτές ασφάλειας της επιχείρησης να προσομοιάσουν τις ενέργειες στις οποίες θα χρειαστεί, ενδεχομένως , να προβούν σε περίπτωση παραβίασης (βάσει του Κανονισμού GDPR), όπως η απαίτηση ενημέρωσης εντός 72 ωρών, η εκτίμηση του κινδύνου δυσμενών επιπτώσεων ή η επικοινωνία με τον υπεύθυνο ασφάλειας δεδομένων (Data Protection Officer – DPO) και την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Data Protection Authority – DPA). Στο πλαίσιο της προσομοίωσης, οι αναλυτές αξιολογούν ένα περιστατικό ως υψηλού, μεσαίου ή χαμηλού κινδύνου και ακολουθούν τα ενδεδειγμένα βήματα για την ενημέρωση της εποπτικής αρχής και των καταναλωτών των οποίων τα δεδομένα παραβιάστηκαν. Η έρευνα του Ινστιτούτου Ponemon διαπίστωσε επίσης ότι το μεγαλύτερο εμπόδιο στη θωράκιση έναντι των ψηφιακών απειλών είναι ο ανεπαρκής σχεδιασμός και η ελλιπής προετοιμασία. Οι προσομοιώσεις GDPR μπορούν να βοηθήσουν στην άρση αυτού του εμποδίου.
- **Resilient GDPR-Enhanced Privacy Module.** Η IBM πρόσθεσε τις απαιτήσεις του Κανονισμού GDPR στην παγκόσμια

λειτουργική μονάδα προστασίας της ιδιωτικότητας που διαθέτει και θα συνεχίσει να την ενημερώνει έτσι ώστε, όταν τεθεί σε ισχύ ο Κανονισμός GDPR στις 25 Μαΐου 2018, οι πελάτες που χρησιμοποιούν την πλατφόρμα IBM Resilient να έχουν πρόσβαση στη βάση δεδομένων των σχετικών οδηγιών και κανονισμών του GDPR. Το εκτεταμένο πεδίο εφαρμογής του Κανονισμού GDPR πρακτικά σημαίνει ότι δεσμεύονται από αυτόν και εταιρείες οι οποίες, αν και δεν έχουν την έδρα τους στην ΕΕ, συναλλάσσονται με χώρες της ΕΕ ή επεξεργάζονται πληροφορίες Υποκειμένων Δεδομένων της ΕΕ. Ωστόσο, παρά τον εκτεταμένο αντίκτυπο που έχει η εφαρμογή του GDPR, η έρευνα του Ινστιτούτου Ponemon αποκαλύπτει ότι μόλις οι μισοί από τους 4.268 επαγγελματίες του τομέα πληροφορικής και του τομέα ασφάλειας πληροφορικών συστημάτων που ρωτήθηκαν έχουν αρχίσει να προετοιμάζονται για τον Κανονισμό GDPR. [1]

"Ο Κανονισμός GDPR εγκαινιάζει μερικές από τις σημαντικότερες αλλαγές στις ευρωπαϊκές διατάξεις για την προστασία των προσωπικών δεδομένων τα τελευταία είκοσι έτη και οι περισσότερες από αυτές αφορούν πολιτικές και τεκμηρίωση που είναι δύσκολο να βελτιωθούν με την τεχνολογία" είπε ο John Bruce, επικεφαλής του τομέα IBM Resilient. *"Η πλατφόρμα Resilient Incident Response έχει σχεδιαστεί με τέτοιο τρόπο ώστε να βοηθήσει τις επιχειρήσεις να συμμορφωθούν με τις απαιτήσεις του Κανονισμού GDPR. Δίνει τις απαραίτητες οδηγίες και παράλληλα βοηθά στο συντονισμό ανθρώπων, διαδικασιών και τεχνολογίας για την αντιμετώπιση των περιστατικών παραβίασης δεδομένων με συγκεκριμένο τρόπο"*.

Οι περισσότερες επιχειρήσεις ήδη δυσκολεύονται να αμυνθούν στις κυβερνοεπιθέσεις. Σύμφωνα με άλλη έρευνα του Ινστιτούτου Ponemon, το 66 τοις εκατό των επαγγελματιών που ρωτήθηκαν είπαν ότι δεν αισθάνονται σίγουροι για την ικανότητα της επιχείρησής τους να αποκαταστήσει την εύρυθμη λειτουργία της μετά από ένα περιστατικό κυβερνοεπίθεσης. Επιπλέον, σε ποσοστό 41 τοις εκατό παραδέχονται ότι ο χρόνος επίλυσης ενός

περιστατικού κυβερνοεπίθεσης έχει αυξηθεί τους τελευταίους 12 μήνες. [2]

"*Ο Κανονισμός GDPR θα προσθέσει μια σειρά νέων προκλήσεων για την πλειοψηφία των επιχειρήσεων*" δήλωσε ο Dr. Larry Ponemon, Πρόεδρος και Ιδρυτής του Ινστιτούτου Ponemon. "*Η έρευνά μας καταδεικνύει ότι οι περισσότερες εταιρείες παγκοσμίως δεν έχουν εμπιστοσύνη στην ικανότητά τους να συμμορφωθούν με τις απαιτήσεις ενημέρωσης που επιβάλλει ο Κανονισμός σε περίπτωση παραβίασης δεδομένων. Για να ανταποκριθούν σε αυτές τις προκλήσεις, οι επιχειρήσεις πρέπει να σπεύσουν να λάβουν μέτρα θεσπίζοντας διαδικασίες και αναθέτοντας αρμοδιότητες ώστε να εξασφαλιστεί η συμμόρφωση με τις νέες απαιτήσεις*".

Δείτε τον τρόπο με τον οποίο η τεχνολογία IBM Resilient βοηθά στην αντιμετώπιση μιας παραβίασης δεδομένων μετά την εφαρμογή του Κανονισμού GDPR και μάθετε περισσότερα για τις λύσεις IBM Security αναφορικά με τον Κανονισμό GDPR εδώ.

Αναφορικά με τα συστήματα IBM Resilient

Τα συστήματα IBM Resilient στοχεύουν να βοηθήσουν τις επιχειρήσεις να αντιμετωπίσουν με επιτυχία και χωρίς επιπτώσεις οποιαδήποτε κυβερνοεπίθεση ή επιχειρησιακή κρίση. Η κορυφαία στην αγορά πλατφόρμα Incident Response Platform (IRP) δίνει στις ομάδες ασφάλειας μιας επιχείρησης τα απαραίτητα εργαλεία για να αναλύουν, να αναχαιτίζουν και να εξουδετερώνουν τα περιστατικά γρηγορότερα, εξυπνότερα και αποτελεσματικότερα. Η εν λόγω πλατφόρμα είναι η μοναδική ολοκληρωμένη πλατφόρμα IR της αγοράς για συντονισμένη και αυτοματοποιημένη αντιμετώπιση, η οποία δίνει τη δυνατότητα στις ομάδες ασφάλειας να συντονίζουν ανθρώπους, διαδικασίες και τεχνολογίες σε ένα ενιαίο μέτωπο άμυνας απέναντι στις απειλές. Με τις λύσεις Resilient, οι ομάδες ασφάλειας έχουν στη διάθεσή τους τις καλύτερες δυνατότητες της αγοράς για την

αντιμετώπιση περιστατικών επιθέσεων. Διαθέτει δε περισσότερους από 200 πελάτες σε όλο τον κόσμο, μεταξύ των οποίων 50 εταιρείες του Fortune 500, και εκατοντάδες συνεργάτες παγκοσμίως. Μάθετε περισσότερα στη διεύθυνση www.resilientsystems.com.

Αναφορικά με τον τομέα IBM Security

Ο τομέας IBM Security προσφέρει ένα από τα πιο εξελιγμένα και ολοκληρωμένα χαρτοφυλάκια προϊόντων και υπηρεσιών για την επιχειρησιακή ασφάλεια. Το χαρτοφυλάκιο, με την υποστήριξη της παγκοσμίως καταξιωμένης ερευνητικής προσπάθειας X-Force® της IBM, δίνει τη δυνατότητα στις επιχειρήσεις να διαχειρίζονται αποτελεσματικά τους κινδύνους και να αμύνονται έναντι των νεοεμφανιζόμενων απειλών. Η IBM διαθέτει έναν από τους μεγαλύτερους στον κόσμο οργανισμό έρευνας, ανάπτυξης και διάθεσης λύσεων στον τομέα της ασφάλειας, παρακολουθεί 35 δισεκατομμύρια περιστατικά την ημέρα σε περισσότερες από 130 χώρες και έχει στην κατοχή της πάνω από 3.000 διπλώματα ευρεσιτεχνίας. Για περισσότερες πληροφορίες, επισκεφθείτε τη διεύθυνση www.ibm.com/security, ακολουθήστε το @IBMSecurity στο Twitter ή επισκεφθείτε το ιστολόγιο IBM Security Intelligence.

[1] Ponemon Institute και IBM Resilient, “The Cyber Resilient Organization” 2016

[2] Ponemon Institute και Citrix, “The Need for a New IT Security Architecture” 2017