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

Κίνδυνοι Κυβερνοεπιθέσεων και ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

νους στον οργανισμό στόχο προκειμένου όχι τόσο να υποκλέψουν προσωπικά δεδομένα του χρήστη (πχ αριθμούς λογαριασμών, στοιχεία πρόσβασης σε λογαριασμούς κοινωνικών δικτύων κλπ) όσο για να αποκτήσουν πρόσβαση στον υπολογιστή του χρήστη και από αυτόν πρόσβαση στους πόρους τους οργανισμού, που ο χρήστης έχει προνόμια πρόσβασης και χρήσης. Η ανίχνευση επιθέσεων πριν προλάβουν οι εγκληματίες να υποκλέψουν δεδομένα είναι πρόκληση. Το πλέον συνηθισμένο είναι οι κυβερνο-επιθέσεις να παραμένουν μη ανιχνεύσιμες για μεγάλα χρονικά διαστήματα που πολλές φορές ξεπερνά τους 6 μήνες.

Εισαγωγή, Παρακολούθηση και Έλεγχος

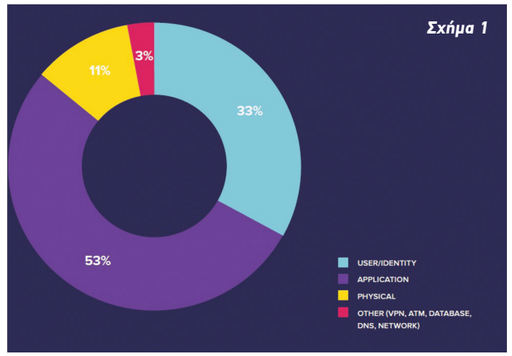
Από την 25 Μάϊου 2018 οι οργανισμοί (δημόσιοι και ιδιωτικοί) κάθε είδους, δεν έχουν πλέον τη δυνατότητα να αποκρύπτουν τυχόν επιθέσεις στα υπολογιστικά τους συστήματα, καθώς και τυχόν απώλειες δεδομένων προσωπικού χαρακτήρα. Μάλιστα ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων γνωστός και ως **GDPR** αλλά και ο προσαρμοστικός νόμος 4624/2109, επιβάλει την **ανακοίνωση οποιασδήποτε επίθεσης και απώλειας προσωπικών δεδομένων στην Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα** και στα υποκείμενα των προσωπικών δεδομένων εντός 72 ωρών από την ανίχνευση της επίθεσης και της διαρροής.

Με βάση την απαίτηση αυτή είναι απαραίτητη οι οργανισμοί να **αναθεωρήσουν** τη στρατηγική, τις πολιτικές, τις διαδικασίες και τα συστήματα ανίχνευσης κυβερνοεπιθέσεων και ασφαλείας δεδομένων με έμφαση τόσο στην αποτροπή όσο και στην έγκαιρη αποκάλυψη τυχόν διαρροής.

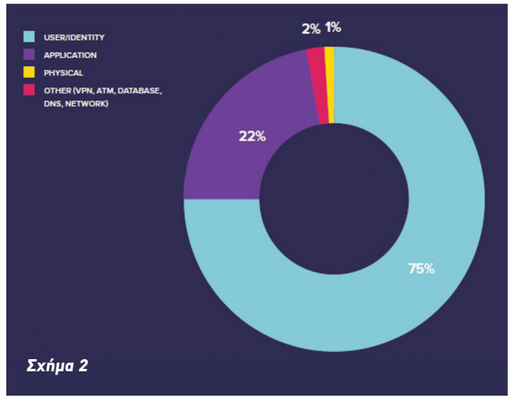
Συνηθισμένος **στόχος κυβερνοεπιθέσεων** είναι οι **διαδικτυακές σελίδες** (websites) των οργανισμών όπου σε πολλές περιπτώσεις περιλαμβάνουν ή παρέχουν πρόσβαση σε προσωπικά δεδομένα υπαλλήλων, πελατών ή άλλων συνεργαζόμενων. Όμως οι διαδικτυακές σελίδες δεν είναι ο μόνος στόχος, σε πολλές περιπτώσεις οι εγκληματίες χρησιμοποιούν τη μέθοδο phishing για να προσεγγίσουν χρήστες/εργαζόμε-

Πιθανές πηγές διαρροής δεδομένων και τρόποι αποτροπής.

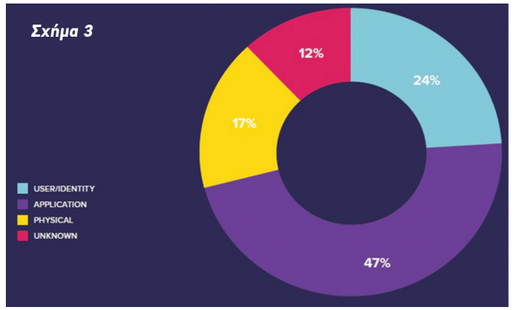
Περιπτώσεις κατηγοριοποιημένες κατά αρχικό στόχο επίθεσης - Στις περιπτώσεις που ο αρχικός στόχος της επίθεσης ήταν αναγνωρίσιμος, οι εφαρμογές ήταν ο πρώτος στόχος της επίθεσης σε ποσοστό 53% των περιπτώσεων (**σχήμα 1**).Τα στοιχεία ταυτοποίησης (προσωπικά δεδομένα) των χρηστών (identities) ήταν ο αρχικός στόχος στο 33% των περιπτώσεων. Τέλος, αθροιστικά οι επιτιθέμενοι είτε απευθείας σε εφαρμογές web είτε απευθείας σε χρήστη, προκειμένου να υποκλέψουν τα προσωπικά τους δεδομένα σε 86% των περιπτώσεων.



Αρχικός στόχος επίθεσης σε σχέση με τον πλήθος των δεδομένων που διέρρευσαν - Αναλύοντας τον αρχικό στόχο επίθεσης σε συσχετισμό με τον αριθμό των δεδομένων (Records) που διέρρευσαν, τότε το 75% ήταν επιτυχημένες διαρροές προσωπικών δεδομένων (**σχήμα 2**). Αυτό πρακτικά σημαίνει ότι οι επιτιθέμενοι προτιμούν αυτού του είδους τις επιθέσεις.



Αρχικός στόχος επίθεσης σε σχέση με το κόστος της διαρροής στον οργανισμό στόχο- Αν αναλυθεί η σχέση του αρχικού στόχου με το κόστος της διαρροής στον οργανισμό, η εικόνα είναι διαφορετική. Επιθέσεις που είχαν σαν αρχικό στόχο της εφαρμογές του οργανισμού στόχου, το κόστος της διαρροής είναι πολύ υψηλότερο (47%). Οι επιθέσεις σε δεδομένα ταυτοποίησης είναι στο 24% από πλευράς κόστους. Η πιθανή αιτία είναι ότι τα περισσότερα δεδομένα αυτού του τύπου συνήθως είναι User-Name, Password και διεύθυνση email, που όμως δεν καλύπτονται κανονιστικά σε σταθερή βάση παγκοσμίως. Φυσικά στην περίπτωση που τα δεδομένα αυτά υπόκεινται στον Γενικό Κανονισμό της Ευρωπαϊκής Ένωσης(EU 679/2016) και χρησιμοποιηθούν σε κακόβουλες/παράνομες δραστηριότητες (πχ πλαστογραφία) που οδηγούν σε ζημιά του κατόχου (υποκείμενο προσωπικών δεδομένων) τότε τα πρόστιμα μπορεί να οδηγήσουν σε σοβαρή οικονομική ζημία (4% του παγκόσμιου εισοδήματος του οργανισμού είτε 20 εκατομμύρια Ευρώ όποιο είναι μεγαλύτερο) καθώς επίσης σε κάποιες χώρες συμπεριλαμβανομένης της Ελλάδος προβλέπονται ποινικές ευθύνες και πρόστιμα για τους υπεύθυνους του οργανισμού που έγινε η διαρροή. Στην περίπτωση αυτή το διάγραμμα του **σχήματος 3** αντιστρέφεται.



Ανάλυση διαρροών ανά αιτία -Όπως είναι αναμενόμενο οι δύο κύριες αιτίες είναι εφαρμογές web και η υποκλοπή στοιχείων ταυτοποίησης (Phishing). Οπότε το 38% των αιτίων αφορούν εφαρμογές. Το Phishing είναι το 19%. Ο λόγος είναι ότι είναι εύκολο να ξεγελαστεί ένας χρήστης και να κλικάρει ένα κακόβουλο σύνδεσμο η να ανοίξει ένα κακόβουλο αρχείο, ανεξάρτητα την εκπαίδευση των χρηστών. Η φυσική κλοπή είναι στην τρίτη θέση στο 12% και είναι μία από τις βασικές αιτίες διαρροής εδώ και δεκαετίες. Συνήθως η φυσική κλοπή δεδομένων εμφανίζεται σε οργανισμούς όπου είναι συνήθεις πρακτική η τήρηση φυσικών αρχείων και η μεταφορά τους σε διάφορες μορφές (ταινίες, δίσκους, ακόμα και σε χάρτινα αρχεία) από ένα σημείο επεξεργασίας σε άλλο. Παρόλο που οι μη ασφαλισμένες βάσεις δεδομένων είναι στο 11 τις λίστας αξίζει να αναφερθεί ότι η μεταφορά των βάσεων δεδομένων στο Cloud ουσιαστικά αναβιώνει ένα παλιό πρόβλημα, το 66% των βάσεων συνδεδεμένων στο Internet που έγινε διαρροή βασίζονταν σε open source εργαλείο MongoDB, όπου καλό είναι να σημειωθεί ότι χρησιμοποιείται σε αρκετές περιπτώσεις Big Data Analytics και επομένως με την σειρά τους δημιουργούν υψηλό κίνδυνο διαρροής προφίλ από επεξεργασία προσωπικών δεδομένων. ITSecurity