Acronis | ITWAY VALUE ADDED DISTRIBUTOR empower your IT

Report 2022

Acronis Cyberthreats Report 2022

At war with ransomware gangs: a year in review

Research

Acronis Cyberthreats Report 2022 – Τάσεις και προβλέψεις στις κυβερνοαπειλές

Η Acronis έχει τη δυνατότητα να παρακολουθεί και να καταγράφει αδιαλείπτως και για όλο τον κόσμο, τις τάσεις και τις προκλήσεις που σχετίζονται με τις απειλές στο κυβερνοχώρο, δημοσιεύοντας τα αποτελέσματα που συλλέγει σε ειδικές αναφορές, όπως αυτή που παρουσιάζουμε σε αυτό το άρθρο.

Η Acronis ήταν η πρώτη εταιρεία, που άρχισε να εφαρμόζει πλήρη και ολοκληρωμένη ασφάλεια στον κυβερνοχώρο, για την προστασία όλων των δεδομένων, των εφαρμογών και των συστημάτων. Η προστασία στον κυβερνοχώρο όμως απαιτεί έρευνα και παρακολούθηση των απειλών, καθώς και τήρηση των πέντε παραμέτρων του «SAPAS»: Safety, Accessibility, Privacy, Authenticity, and Security
Ως μέρος της στρατηγικής της, η εταιρία Acronis δημιούργησε τέσσερα Επιχειρησιακά Κέντρα Κυβερνοπροστασίας (**CPOC – Cyber Protection Operation Centers**) σε όλο τον κόσμο για την παρακολούθηση και την έρευνα κυβερνοαπειλών 24/7.

Η έκθεση **Acronis Cyberthreats Report 2022**, τα αποτελέσματα της οποίας αναφέρουμε σε αυτό το άρθρο, καλύπτει μια παγκόσμια οπτική και βασίζεται σε περισσότερα από 650.000 μοναδικά τελικά σημεία που κατανέμονται σε όλο τον κόσμο.

Βασικές κυβερνοαπειλές και τάσεις του 2021

1. Το Ransomware βρίσκεται στο υψηλότερο επίπεδο όλων των εποχών - Το δεύτερο εξάμηνο του 2021 ήταν πλούσιο σε δραστηριότητες συμμοριών εγκληματιών του κυβερνοχώρου, που αναπτύσσουν ransomware με αποτέλεσμα ολόκληρη η βιομηχανία της ψηφιακής ασφάλειας να

κατακλύζεται από μια σειρά από μεγάλες υποθέσεις. Αυτές οι συμμορίες ransomware ήταν πάρα πολύ δραστήριες και πολύ πιο επιθετικές. Για παράδειγμα, η ομάδα ransomware Ragnar Locker, ανακοίνωσε ότι θα δημοσιεύσει αμέσως όλα τα κλεμμένα δεδομένα, εάν το θύμα μιλήσει στην αστυνομία ή αναζητήσει οποιοδήποτε είδος επαγγελματικής βοήθειας. Πέρυσι, το Ragnar Locker παραβίασε την Campari και στη συνέχεια πλήρωσε για διαφημίσεις στο Facebook προκειμένου να πιέσει δημοσίως το θύμα του να πληρώσει λύτρα 15 εκατομμυρίων δολαρίων στις ΗΠΑ, διαφορετικά θα δημοσιευόταν 2 TB από τα κλεμμένα δεδομένα του. Ένα μεγάλο θύμα της συμμορίας εκβιαστών LockBit είναι και η Bangkok Airways, η οποία απασχολεί περισσότερους από 3.000 ανθρώπους σε 11 χώρες και έχει ετήσια έσοδα πάνω από 685 εκατομμύρια δολάρια ΗΠΑ. Η σχετικά νέα συμμορία ransomware Hive έπληξε τον κολοσσό λιανικής πώλησης ηλεκτρονικών MediaMarkt, με αρχική ζήτηση λύτρων 240 εκατομμυρίων δολαρίων ΗΠΑ τον Νοέμβριο, προκαλώντας το κλείσιμο των συστημάτων πληροφορικής και τη διακοπή των λειτουργιών αποθήκευσης τόσο στην Ολλανδία όσο και στη Γερμανία.

2. Το ηλεκτρονικό ψάρεμα και τα κακόβουλα email παραμένουν ο κύριος φορέας μόλυνσης - Τα Acronis CPOC απέκλεισαν 376.000 διευθύνσεις ηλεκτρονικού "ψαρέματος" (phishing) και κακόβουλες διευθύνσεις URL τον Οκτώβριο του 2021. Αυτό συνιστά μια τεράστια άνοδο σε σχέση με ένα χαμηλότερο τρίμηνο με μέσο όρο 58.000 το μήνα. Δυστυχώς, πολλά μηνύματα ηλεκτρονικού ταχυδρομείου με κακόβουλο περιεχόμενο εξακολουθούν να περνούν από βασικά φίλτρα email και να καταλήγουν στο τελικό σημείο του χρήστη. Έχουμε δει επίσης εισβολείς να ενσωματώνουν κωδικούς QR, σε κακόβουλες διευθύνσεις URL σε μηνύματα ηλεκτρονικού ψαρέματος. Πολλές λύσεις ασφαλείας δεν μπορούν να χειριστούν ακόμα κωδικούς QR, αλλά οι τελικοί χρήστες είναι υποχρεωμένοι να χρησιμοποιούν τα smartphone τους για να ακολουθούν τους συνδέσμους. Αυτός είναι ένας άλλος λόγος για τον οποίο είναι σημαντικό να έχουμε μια πολυεπίπεδη αμυντική προσέγγιση.

3. Επιθέσεις σε Linux και macOS - Έχουμε ήδη αναφέρει κάποιο ransomware Linux, αλλά αυτή δεν είναι η μόνη αναδυόμενη απειλή για αυτό το λειτουργικό σύστημα. Οι επιτιθέμενοι προσδίδουν ολοένα και μεγαλύτερη προσοχή στο Linux, καθώς υπάρχουν δεκάδες εκατομμύρια μηχανές συνδεδεμένες στο Διαδίκτυο —κυρίως διακομιστές— που προσφέρουν ένα σημαντικό κίνητρο, για την ανάπτυξη νέου κακόβουλου λογισμικού. Και εκτός από το ransomware, οι εγκληματίες του κυβερνοχώρου εστιάζουν σε cryptominers, trojans και πιο εξελιγμένο κακόβουλο λογισμικό, όπως τα rootkits.

Προβλέψεις για την Ασφάλεια το 2022

Καθώς η πανδημία του COVID-19 εξαπλώθηκε, όλοι έπρεπε να προσαρμοστούν σε μια πολύ διαφορετική ρουτίνα και σε προκλήσεις για τις οποίες λίγοι ήταν προετοιμασμένοι. Παρακάτω ακολουθούν οι βασικές τάσεις που είναι πιθανό να καθορίσουν το τοπίο της κυβερνοασφάλειας και το 2022.

1. Το Ransomware θα συνεχίζει να αναπτύσσεται και να εξελίσσεται παρά τις προσπάθειες των ΗΠΑ και της Interpol/ Europol

2. Το κρυπτονόμισμα θα γίνει ο αγαπημένος στόχος των επιτιθέμενων

3. Το phishing θα συνεχίσει να είναι ο κύριος φορέας μόλυνσης

4. Οι MSP θα αποτελούν στόχο μέσω των εργαλείων που χρησιμοποιούν

5. Η εμπιστοσύνη θα τεθεί σε κίνδυνο σε επίπεδο cloud με επιθέσεις API

6. Οι Παραβιάσεις δεδομένων για όλες τις επιχειρήσεις θα είναι πολύ συχνές

7. Αντίπαλες επιθέσεις στο AI θα κάνουν έντονη την εμφάνιση τους

8. Η ενοποίηση προϊόντων ασφάλειας . Η ευρύτερη κάλυψη ασφαλείας κάτω από ένα προϊόν ή μια ομπρέλα προϊόντων βοηθά στην ελαχιστοποίηση των επιθέσεων και επιτρέπει ταχύτερη αντίδραση και ανάκαμψη.

Μένοντας ασφαλείς το 2022

Οι επιχειρήσεις θα εξακολουθούν να αγωνίζονται να προστατεύσουν αποτελεσματικά ολόκληρο τον φόρτο εργασίας τους, στο περίπλοκο οικοσύστημα του cloud, του επαγγελματικού γραφείου και του οικιακού γραφείου. Για να γίνει αυτό απαιτούνται αποτελεσματικές λύσεις που **ενσωματώνουν την ασφάλεια στον κυβερνοχώρο με την προστασία δεδομένων**, καθώς και τη διαχείριση και παρακολούθηση τελικών σημείων.

Αυτή η **ολιστική προσέγγιση** για την προστασία στον κυβερνοχώρο επιτρέπει μια αυτοματοποιημένη απόκριση έναντι των απειλών στον κυβερνοχώρο. Στο **Acronis Cyber Protect**, χρησιμοποιούμε πολλές καλά ισορροπημένες και συντονισμένες τεχνολογίες ασφαλείας, συμπεριλαμβανομένων αρκετών μηχανών ανίχνευσης.

Για περισσότερες πληροφορίες, σχετικά με τις τεχνολογία ασφαλείας της **Acronis** , επικοινωνήστε με την **ITway Hellas**, τη διανομέα της στην **Ελλάδα, Κύπρο & Μάλτα**, για εξατομικευμένη αξιολόγηση και παρουσίαση της λύσης στον οργανισμό σας. Αγίου Ιωάννου 10 Χαλάνδρι , 2106801013, www.itway.gr ITSecurity