

Acronis

ITWAY
do IT your way

Comprehensive cyber protection

Layered protection built to address
all cyberthreats — today and tomorrow



#CyberFit

Τα προϊόντα της Acronis διανέμονται μέσω δικτύου εξουσιοδοτημένων συνεργατών σε Ελλάδα, Κύπρο και Μάλτα από την Itway Hellas SA, Αγίου Ιωάννου 10 Χαλάνδρι, 2106801013, www.itway.gr

Αντιμετωπίστε τις **επιθέσεις phishing**, με το **Acronis Cyber Protect**

Γρήγορη και αξιόπιστη ανάκτηση της λειτουργίας του συστήματός σας, μέσα σε λίγα δευτερόλεπτα!



Καθημερινά συμβαίνουν συνεχώς κυβερνοεπιθέσεις, για αυτό και είναι απαραίτητο να λαμβάνουμε όσο πιο συχνά γίνεται, πληροφορίες σχετικά με αυτές τις επιθέσεις, προκειμένου να είμαστε σε θέση να υπερασπιστούμε τις πληροφοριακές υποδομές, στοχεύοντας τόσο στην αποτροπή τους, όσο και στην καλή επίγνωση των λύσεων που απαιτούνται για να αντιμετωπιστούν οι ζημιές που μπορεί να προκληθούν από αυτές τις επιθέσεις, μιας και δεν μπορούν πάντα να αποφευχθούν.



Είναι αλήθεια ότι οι εγκληματίες του κυβερνοχώρου – μέσα από τις επιθέσεις που εξαπολύουν – μπορούν να υπαρπάξουν πολλά και πολύτιμα δεδομένα και προσωπικές πληροφορίες, με τις οποίες μπορούν να υποκλέψουν την ταυτότητα κάποιου ιδιώτη ή μιας εταιρίας, καθιστώντας τα θύματα τους ανήμπορα να αντιδράσουν με απρόβλεπτες συνέπειες για τη λειτουργία τους. Πως όμως όλα αυτά μπορούν να αποφευχθούν;

Αποφυγή phishing

Πολλές φορές, μπορεί σίγουρα να αναρωτιέστε τι είναι εφικτό να κάνετε για να αποφύγετε το phishing. Φυσικά, το πρώτο που πρέπει να κάνετε, είναι να είστε πάντα προσεκτικοί σε κάθε σας ενέργεια στο κυβερνοχώρο και σε περίπτωση που υποπτευτείτε ή εντοπίσετε κάποιον κίνδυνο, είτε σε κάποιο email που λαμβάνετε, είτε σε άλλες περιπτώσεις που σας ζητείται να εισάγετε εμπιστευτικά δεδομένα... πολύ απλά να μην το κάνετε!

Να προσέχετε πάντα και πάρα πολύ τους συνδέσμους και όπου άλλου μπορεί να ελλοχεύουν κίνδυνοι για τα δεδομένα σας.

Χρησιμοποιώντας ένα πρόγραμμα προστασίας από ιούς ή ένα καλό τείχος προστασίας, είναι ένας συμβατικός τρόπος για να προστατευτείτε, αλλά να έχετε πάντα κατά νου, ότι οι κακόβουλοι χάκερ, το γνωρίζουν αυτό και προσπαθούν να βρουν νέους τρόπους για να σας παραπλανήσουν και να παρακάμψουν αυτά τα προγράμματα, με στόχο να περάσουν απαρατήρητοι, χωρίς κανένα φίλτρο ασφαλείας να τους εντοπίσει.

Το περιβάλλον στον κυβερνοχώρο είναι σε συνεχή εξέλιξη, τόσο σε ότι αφορά το έγκλημα όσο και στους μηχανισμούς προστασίας, οπότε όλα εξαρτώνται από το ποιος είναι ένα βήμα πιο μπροστά και διαθέτει πιο προηγμένα εργαλεία, είτε για να αφαρπάξει δεδομένα, είτε για να προστατεύσει τα δεδομένα. Οπότε λοιπόν, δεν πρέπει να ξεχνάτε να διατηρείτε πλήρως ενημερωμένα και το πρόγραμμα περιήγησής στο internet και τα πρόσθετα του, καθώς και το antivirus και το τείχος προστασίας που χρησιμοποιείτε.

Η χρήση ενός απαραιτημένου συστήματος προστασίας ή η εισαγωγή ενός νέου τρόπου πρόσβασης στον Ιστό μπορεί να είναι αρκετό για να εκδηλωθεί μια επίθεση. Τι γίνεται λοιπόν σε αυτήν την περίπτωση που εκδηλωθεί η επίθεση; Τι γίνεται με τα δεδομένα και τα προσωπικά στοιχεία; Εάν δεν είχατε δημιουργήσει ένα αντίγραφο ασφαλείας, τότε ναι μπορεί και να τα χάσατε.

Μην εισάγετε λοιπόν, ποτέ εμπιστευτικά δεδομένα σε μη ασφαλείς ιστότοπους που δεν ξεκινούν με <https://> και εάν έχετε κάποιες αμφιβολίες μην προχωράτε σίγουρα σε εισαγωγή των στοιχείων σας. Και φυσικά, μην δίνετε ποτέ εμπιστευτικά δεδομένα μέσω τηλεφώνου ή ως απάντηση σε οποιοδήποτε email που μπορεί να έχει αυτή την απαίτηση.

Δημιουργία αντιγράφων ασφαλείας δεδομένων

Η δημιουργία αντιγράφων ασφαλείας προσφέρει σαφώς ένα πλεονέκτημα σε περίπτωση εκδήλωσης επίθεσης από κακόβουλο λογισμικό, αφού σε αυτή τη δύσκολη περίπτωση, ακόμα και αν έχουν παραβιαστεί οι υποδομές σας και έχουν καταφέρει οι επιτιθέμενοι να έχουν πρόσβαση στα δεδομένα σας στο cloud ή ακόμα και αν τα διαγράψουν, τότε θα υπάρχει η εναλλακτική δυνατότητα να έχετε ξανά όλες αυτές τις πληροφορίες διαθέσιμες.

Τα **αυτόματα αντίγραφα ασφαλείας** διευκολύνουν σε πολύ μεγάλο βαθμό τον εκάστοτε χρήστη, ο οποίος μπορεί να τα εκτελέσει σε προγραμματισμένη βάση και στο παρασκήνιο, χωρίς να μειώσει την απόδοση της εργασίας του.

Η δυνατότητα να υπάρχει ένα "backup of a backup" είναι πολύ σημαντική και βοηθάει πολλούς επαγγελματίες και εταιρίες κάθε κλίμακας μεγέθους, αλλά και ιδιώτες, να είναι σε θέση να ανακάμψουν από μια επίθεση κακόβουλων χάκερ και παράλληλα να έχουν τη δυνατότητα να αποκαταστήσουν τις πληροφορίες ή ολόκληρο το σύστημα τους γρήγορα και αποτελεσματικά. Αυτό αποφεύγει πολλές προβληματικές καταστάσεις και πάνω από όλα, το άκρως δυσάρεστο γεγονός μια επιχείρηση να σταματάει τη λειτουργία της λόγω μιας επίθεσης ηλεκτρονικού "ψαρέματος" (phishing) που μπορεί να έχει κλέψει για παράδειγμα την «ταυτότητα της εταιρείας». Το **Acronis Cyber Protect** ενσωματώνει σε μια μόνο **ενιαία λύση την καλύτερη δυνατή δημιουργία αντιγράφων ασφαλείας, προηγμένη προστασία από κακόβουλα λογισμικά και υψηλού επιπέδου διαχείριση προστασίας τελικών σημείων.**

Με το Acronis Cyber Protect, έχετε μια ενοποιημένη λύση που παρέχει πλήρη προστασία από όλες τις σημερινές απειλές.

Συμβουλές κοινής λογικής

- Να θυμάστε πάντα να ενημερώνετε τους κωδικούς πρόσβασης κατά συχνά χρονικά διαστήματα και μην χρησιμοποιείτε σε όλες τις εφαρμογές τους ίδιους, καθώς μια γενικευμένη επίθεση μπορεί να σας εκθέσει σε πολλούς λογαριασμούς.
- Να προσέχετε πάντα και με μεγάλη λεπτομέρεια τα email που λαμβάνετε καθώς και να μην ενεργείτε βιαστικά, πατώντας σε συνδέσμους που ελλοχεύουν κινδύνους. Ελέγξτε πρώτα ότι όλα είναι σωστά και νόμιμα.
- Δημιουργήστε όσο πιο τακτικά γίνεται αντίγραφα ασφαλείας όλων των δεδομένων σας, ώστε, σε περίπτωση καταστροφής, να τα έχετε πάντα διαθέσιμα.
- Ελέγξτε την προέλευση των εισερχόμενων email και τις διευθύνσεις URL που επισκέπτεστε. Ενισχύστε την προστασία των συσκευών σας και των δεδομένων σας.
- Και πάνω απ' όλα, χρησιμοποιήστε την κοινή λογική, αυτή είναι που ίσως σας αποτρέψει καλύτερα από την επίθεση phishing. Δεν μπορείτε να αποφύγετε τη λήψη του email, αλλά μπορείτε να το αγνοήσετε. Είναι στα χέρια σας!

Για περισσότερες πληροφορίες, σχετικά με τις τεχνολογίες ασφαλείας της **Acronis**, επικοινωνήστε με την **Itway Hellas**, τον **διανομέα της στην Ελλάδα, Κύπρο & Μάλτα**, για εξατομικευμένη αξιολόγηση και παρουσίαση της λύσης στον οργανισμό σας.

Στοιχεία επικοινωνίας: Αγίου Ιωάννου 10 Χαλάνδρι, τηλ.: 2106801013, www.itway.gr **ITSecurity**