# ΠΡΟΕΤΟΙΜΑΣΤΕΙΤΕ:
# Αργά ή γρήγορα η επιχείρησή σας θα δεχτεί επίθεση

## 5 βήματα για να βελτιώσετε την ανθεκτικότητα σας στο ransomware

GIANT STRIDE
IT SUPPORT

# Αυτή είναι η πραγματικότητα: Το Ransomware ανθίζει

## Ορίστε μερικές απαντήσεις στις συχνότερες ερωτήσεις γύρω απο το ransomware.

**Τι είναι;**

Είναι όταν χάκερς εισβάλλουν στο δίκτυο σας, κρυπτογραφούν τα δεδομένα σας έτσι ώστε να μην μπορείτε να έχετε πρόσβαση σε αυτά - στη συνέχεια, σας χρεώνουν ένα μεγάλο ποσό λύτρων για να τα ανακτήσετε. Είναι το πιο ενοχλητικό και δαπανηρό είδος επίθεσης που μπορείτε να φανταστείτε. Και πολύ δύσκολο να αφαιρεθεί.

**Γιατί είναι τόσο σημαντικό;**

Οι επιθέσεις Ransomware έχουν αυξηθεί δραματικά εξαιτίας της πανδημίας. Όλες οι επείγουσες αλλαγές οι οποίες πέρασαν οι επιχειρήσεις τον προηγούμενο χρόνο δημιούργησαν μια τέλεια περίσταση, με πολλές νέες ευκαιρίες για τους χάκερ.

**Βρίσκεται πραγματικά σε κίνδυνο η επιχείρησή μου;**

Εξαιτίας αυτοματοποιημένων εργαλείων που χρησιμοποιούν οι χάκερ, όλες οι επιχειρήσεις γίνονται στόχοι διαρκώς. Στην πραγματικότητα, οι χάκερ προτιμούν να στοχοποιούν μικρές επιχειρήσεις, καθώς τέτοιες επιχειρήσεις επενδύουν λιγότερο χρόνο και χρήματα σε προληπτικά μέτρα ασφαλείας - σε σύγκριση με μεγαλύτερες εταιρείες.

Εκτιμάται ότι μια επιχείρηση μολύνεται από ransomware κάθε 14 δευτερόλεπτα.

Και οι χάκερ μπορούν να απαιτούν χιλιάδες επί χιλιάδων ευρώ για να ξεκλειδώσουν τα δεδομένα σας... χωρίς καμία εγγύηση ότι θα σας τα επιστρέψουν ακόμα κι αν έχετε πληρώσει.

**Πως μπορεί η επιχείρησή μου να μολυνθεί από Ransomware;**

Το 42% του ransomware προέρχεται από phishing emails. Το μόνο που χρειάζεται είναι να κλικάρετε πάνω σε ένα κακόβουλο σύνδεσμο για να αφήσετε τους χάκερ να εισέλθουν ήσυχα στο σύστημά σας. Και δεν είναι απαραίτητο να είστε εσείς αυτός που θα κάνετε το κλίκ..μπορεί να είναι οποιοδήποτε μέλος της ομάδας σας.

Οι κακόβουλες ιστοσελίδες αποτελούν το 23% των επιθέσεων. Επίσης οι παραβιασμένοι κωδικοί πρόσβασης αποτελούν το 21% των επιθέσεων ransomware.

## Γιατί είναι τόσο δύσκολο να το αντιμετωπίσετε;

Μια επίθεση ransomware παίρνει εβδομάδες στους χάκερ να την προετοιμάσουν. Από τη στιγμή που θα καταφέρουν να εισέλθουν στο δίκτυο σας, παραμένουν κρυμμένοι και παίρνουν το χρόνο τους για να κάνουν πολλές αλλαγές. Ουσιαστικά, καθιστούν αδύνατο για μια εταιρία πληροφορικής σαν τη δική μας να αποκαταστήσουμε τη ζημιά και να τους απωθήσουμε από τη στιγμή που έχει ξεκινήσει η επίθεση.

Εάν δεν είστε διεξοδικά προετοιμασμένοι για μια επίθεση ransomware - προτού συμβεί, είναι πολύ πιθανό να πρέπει να πληρώσετε τα λύτρα.

## Πόσο κοστίζουν τα λύτρα;

Οι χάκερ δεν είναι χαζοί. Γνωρίζουν ότι το να προσπαθήσουν να βγάλουν 150.000€ από μια μικρή επιχείρηση απλά δεν θα συμβεί. Αλλά μπορεί να δώσετε 10.000€ μόνο για να σταματήσετε την επίθεση. Θα αλλάξουν τις απαιτήσεις τους με βάση τα πόσα χρήματα θεωρούν ότι διαθέτει μια επιχείρηση. Σχεδόν το 50% των επιχειρήσεων είναι τόσο απροετοίμαστες που πρέπει να πληρώσουν για να επαναφέρουν τα δεδομένα τους.

Φυσικά, τα λύτρα δεν είναι το μόνο κόστος που σχετίζεται με μια επίθεση. Υπάρχουν αμέτρητα έμμεσα κόστη. Όπως το να μην μπορείτε να έχετε πρόσβαση στα δεδομένα σας ή τα συστήματά σας για εβδομάδες. Πόσο τρομακτικό είναι εάν κανείς δεν μπορεί να κάνει καμία δουλειά στον υπολογιστή του για μια εβδομάδα; Πως θα αντιδρούσαν σε αυτό οι πελάτες σας;

Μετά την επίθεση, η παραγωγικότητα είναι σχεδόν μηδενική, καθώς το προσωπικό συνηθίζει σε νέα συστήματα, νέους τρόπους εργασίας και μεγαλύτερα μέτρα προστασίας.

## Τι μπορώ να κάνω για να προστατεύσω την επιχείρησή μου;

Αυτή είναι η πιο σημαντική ερώτηση που πρέπει να κάνετε. Είναι εξαιρετικά δύσκολο να σταματήσετε μια επίθεση ransomware.
Αλλά μπορείτε να κάνετε μια τεράστια προετοιμασία, προκειμένου εάν κάποια επίθεση συμβεί, να αποτελεί ενόχληση και όχι καταστροφή.

# Αυτά είναι τα 5 βήματα που προτείνουμε για την αποτροπή του Ransomware


#1

## Δράστε σαν να μην υπάρχει κάποιο λογισμικό προστασίας

**Το λογισμικό είναι απαραίτητο για να κρατήσει την επιχείρησή σας ασφαλή. Αλλά υπάρχει ένα μειονέκτημα στη χρήση του: μπορεί να σας κάνει να  εφησυχάσετε.**

Βασικά, οι άνθρωποι είναι η πρώτη ασπίδα ενάντια σε κυβερνοεπιθέσεις. Για παράδειγμα, εάν η ομάδα σας δεν κλικάρει πάνω σε κακόβουλους συνδέσμους που προέρχονται από phishing mail, δεν χρειάζεται να βασίζεστε σε λογισμικό για να εντοπίσετε μια επίθεση και να να τη σταματήσετε.

Αυτό σημαίνει ότι πρέπει να εκπαιδεύετε όλους στην επιχείρησή σας - συνεχώς. Αυτό, πρέπει να συμβαίνει με τρόπο διασκεδαστικό! Κανείς δεν θέλει να κάνει βαρετές τεχνολογικές εκπαιδεύσεις... (ούτε καν εμείς).

# Βεβαιωθείτε ότι ο συνεργάτης IT διαθέτει ισχυρά συστήματα προστασίας

#2

**Πρέπει να έχετε ισχυρά συστήματα προστασίας, καθώς και λογισμικό που επιτρέπει σε επιλεγμένες εφαρμογές να χρησιμοποιηθούν στο δίκτυό σας.**

Από τον συνεργάτη IT, χρειάζεστε ένα κατάλληλο μείγμα από προληπτική υποστήριξη.

Η προληπτική υποστήριξη είναι κρίσιμη σε καταστάσεις που οι επιθέσεις ransomware είναι επιτυχημένες. Σημαίνει ότι έχετε ειδικούς, διαθέσιμους, για να ελαχιστοποιήσουν την επίδραση και να οδηγήσουν την επιχείρησή σας στη σωστή λειτουργία της το συντομότερο δυνατό.

Όμως η μακροχρόνια, κατάλληλη, προληπτική υποστήριξη είναι ζωτικής σημασίας. Αυτό σημαίνει ότι έχετε κάποιον να εργάζεται εξ' αποστάσεως, κρατώντας τα συστήματά σας ασφαλή και 100% ενημερωμένα. Ψάχνει για προβλήματα που μπορεί να προκύψουν στο μέλλον, και παρατηρεί οτιδήποτε διαφορετικό από τα συνηθισμένα. Αυτό σημαίνει, επίσης, ότι θα έχετε λιγότερη αναστάτωση από τέταοια ζητήματα, καθώς στη πλειοψηφία τους μπορεί να λυθούν πριν έχουν αντίκτυπο σε εσάς ή την ομάδα σας.

Στη περίπτωση επίθεσης ransomware, ένας συνεργάτης IT που δρα προληπτικά θα έχει ήδη μια στρατηγική προστασίας και επαναφοράς που μπορεί να ενεργοποιήσει άμεσα.

# Επενδύστε σε κορυφαίες λύσεις backup / recovery

#3

**Η αυτόματη δημιουργία αντιγράφων ασφαλείας (backup) εκτός γραφείου είναι ζωτικής σημασίας. Όμως, όταν έχετε ένα λειτουργικό αντίγραφο ασφαλείας, είναι δελεαστικό να μη κάνετε δεύτερες σκέψεις.**

Αλλά αξίζει να θυμάστε ότι οι Χακερς θα χρησιμοποιήσουν διάφορα μέσα για να σας κάνουν να πληρώσετε λύτρα. Αυτό σημαίνει ότι θα βάλουν στόχο και το backup σας. Συμπεριλαμβανομένων των cloud δεδομένων σας.

Είναι σημαντικό να δημιουργήσετε και να εφαρμόσετε μια ολοκληρωμένη προσέγγιση δημιουργίας αντιγράφων ασφαλείας και ανάκτησης όλων των δεδομένων της επιχείρησής σας. **Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας καθορίζει ένα πλαίσιο ασφάλειας το οποίο περιλαμβάνει βέλτιστες πρακτικές όπως:**

- **Συνεχόμενα backups:** Ιδανικά στο Cloud
- **Immutable storage:** Αυτό σημαίνει ότι μόλις δημιουργηθεί το backup - δεν μπορεί να αλλάξει
- **Firewalls:** Για να περιορίσετε τα δεδομένα που εισέρχονται και εξέρχονται

## Δημιουργήστε ένα πλάνο για κυβερνοεπιθέσεις

#4

**Όταν συμβαίνει μια κυβερνοεπίθεση, κάθε δευτερόλεπτο μετράει. Όσο το συντομότερο δράσετε, τόσο μικρότερη η ζημιά.**

Επομένως, προετοιμάστε ένα λεπτομερές πλάνο δράσης και σιγουρευτείτε ότι όλοι γνωρίζουν  τι περιλαμβάνει, που θα το βρουν και πως θα το ενεργοποιήσουν.

Ελέγχετε το πλάνο σας σε τακτική βάση για να βεβαιωθείτε για την αποτελεσματικότητά του, και απομακρύνετε κάθε ρίσκο αποτυχίας κρατώντας το λιγότερο τρία αντίγραφα του πλάνου σε διαφορετικά μέρη.

Το ένα θα πρέπει να είναι εκτυπωμένο και να βρίσκεται στο σπίτι κάποιου...σε περίπτωση που έχετε μηδενική πρόσβαση στο χώρο αποθήκευσης των δεδομένων σας.

## Προετοιμαστείτε, προετοιμαστείτε και προετοιμαστείτε λίγο ακόμα

#5

Δημιουργώντας μια πολυεπίπεδη προσέγγιση για την ανάκτηση των δεδομένων σας, μειώνετε την επίδραση οποιασδήποτε επίθεσης. Όσο το συντομότερο επαναφέρετε την επιχείρησή σας, τόσο λιγότερα χρήματα θα χάσετε και τόσο μικρότερη θα είναι η ζημιά που θα πρέπει να διαχειριστείτε - συμπεριλαμβανομένης της εμπιστοσύνης των πελατών σας.

**Το μεγαλύτερο συμπέρασμα είναι ότι είναι αδύνατο να προστατεύσετε την επιχείρηση σας 100%. Ενώ οι έμπιστοι συνεργάτες IT μπορούν να δημιουργήσουν ένα εξαιρετικά ασφαλές σύστημα, ρεαλιστικά μιλώντας, ποτέ δεν θα είστε 100% ασφαλείς.**


Με το να σχεδιάσετε το τι πρέπει να κάνετε σε περίπτωση που δεχτείτε μια επίθεση, ή γίνει απόπειρα επίθεσης, κάνετε την εταιρεία σας πολύ πιο ανθεκτική σε επιθέσεις ransomware.

Διακυβεύονται πολλά εδώ, έτσι δεν είναι; Για τους πελάτες μας, βάζουμε τα δυνατά μας!

**Είστε έτοιμοι να επιλέξετε έναν καινούριο συνεργάτη IT; Ας μιλήσουμε.**

GIANT STRIDE
IT SUPPORT

## Έτσι μπορείτε να επικοινωνήσετε μαζί μας:

**ΤΗΛ:** 2111985162 | **EMAIL** info@giantstride.gr
**WEBSITE:** www.giantstride.gr