



Cyber Risk Insurance

Οι απειλές του κυβερνοχώρου για
τις επιχειρήσεις

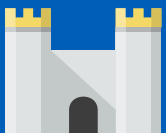
Νίκος Αστυφίδης

-

12 Οκτωβρίου 2022



Τι είναι η κυβερνοασφάλεια;



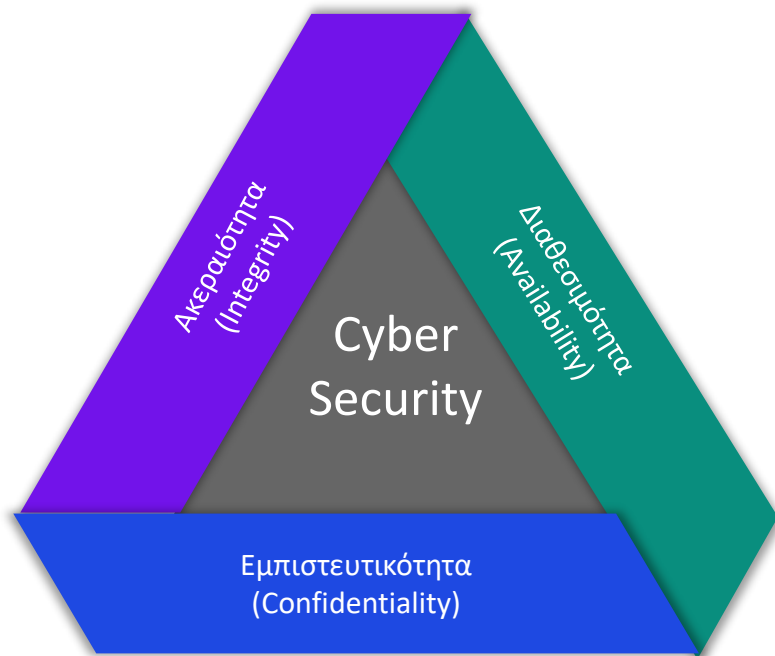
Κυβερνοασφάλεια (cyber security)

Το σύνολο των τεχνολογιών, διαδικασιών και μέτρων που λαμβάνονται προκειμένου να προστατέψουμε τα συστήματα και την πληροφορία που κατέχει ένας οργανισμός.



Κυβερνοεπίθεση (cyber attack)

Ορίζεται οποιαδήποτε κακόβουλη ενέργεια, η οποία σκοπό έχει να πλήξει την κυβερνοασφάλεια ενός οργανισμού.



Απειλές κυβερνοχώρου



Η νέα εποχή κυβερνοαπειλών

Προ-COVID:

Ακολουθούνταν ένα ευρύ φάσμα τεχνικών, επιθέσεων και απειλών για τις επιθέσεις



Ήταν σύνηθες για τους επιτιθέμενους να κρυπτογραφούν αρχεία, στερώντας τη πρόσβαση στις επιχειρήσεις μέχρι να πληρώσουν τα λύτρα.
Είχαν το χαρακτηριστικό καμπάνιας, χωρίς συγκεκριμένο στόχο, προσπαθώντας να απομυζήσουν όσο το δυνατόν περισσότερα κέρδη.

Οι κακόβουλοι εκτελούν την επίθεση με ransomware

Τα ευάλωτα συστήματα κρυπτογραφούνται απαγορεύοντας την πρόσβαση στα θύματα

Οι επιτιθέμενοι απαιτούν πληρωμή λύτρων

Η επιχείρηση πληρώνει χιλιάδες δολάρια σε λύτρα για την αποκατάσταση των συστημάτων

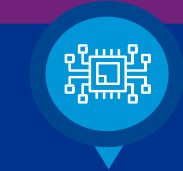
Τον Μάιο του 2017, το WannaCry επηρέασε το NHS. Εκτιμάται ότι αυτή η επίθεση απέφερε μόνο \$ 50K στους εγκληματίες, αλλά κόστισε στο NHS \$ 128M για να επανορθώσει τη ζημιά.

Επιτιθέμενος

Κίνδυνοι Προ-COVID



Κίνδυνοι Μετά-COVID



▶ Η εργασία από το σπίτι δημιουργεί 3,5 φορές μεγαλύτερο κίνδυνο*

Αυξανόμενες απειλές για το cloud

Τώρα, οι επιτιθέμενοι συχνά αποσπούν δεδομένα από κρίσιμα συστήματα, τα οποία μάλιστα κρυπτογραφούν. Διατηρούν τα δεδομένα για λύτρα και εάν δεν γίνει πληρωμή, τα δεδομένα διαρρέουν - αναγκάζοντας τα θύματα να αποκαλύψουν μια παραβίαση δεδομένων στις ρυθμιστικές αρχές. Αυτό θα μπορούσε να οδηγήσει σε πρόστιμο (έως και 4% του τζίρου).

Οι επιτιθέμενοι εισχωρούν στα συστήματα

Αποκοτούν δικαιώματα διαχειριστή του συστήματος και έτσι το ελέγχουν

Οι εισβολείς στοχεύουν βασικά συστήματα για να έχουν το μεγαλύτερο δυνατό αντίκτυπο και εκτελούν την επίθεση ransomware και το αίτημα για λύτρα


Η επιχείρηση πρέπει να πληρώσει εκατοντάδες χιλιάδες δολάρια για να αποκαταστήσει τα συστήματά της και να προστατεύσει τη φήμη της

Τον Ιούλιο του 2020, η Garmin επλήγη από μια επίθεση ransomware, που αναφέρεται ότι ήταν έργο της Evil Corp, η οποία απαίτησε \$ 10M για την επαναφορά των συστημάτων.

Μετά-COVID:
Στοχευμένες επιθέσεις σε επιχειρήσεις

* Πηγή: Identifying Unique Risks of Work from Home Remote Office Networks, Bitsight Blog, April 14, 2020.

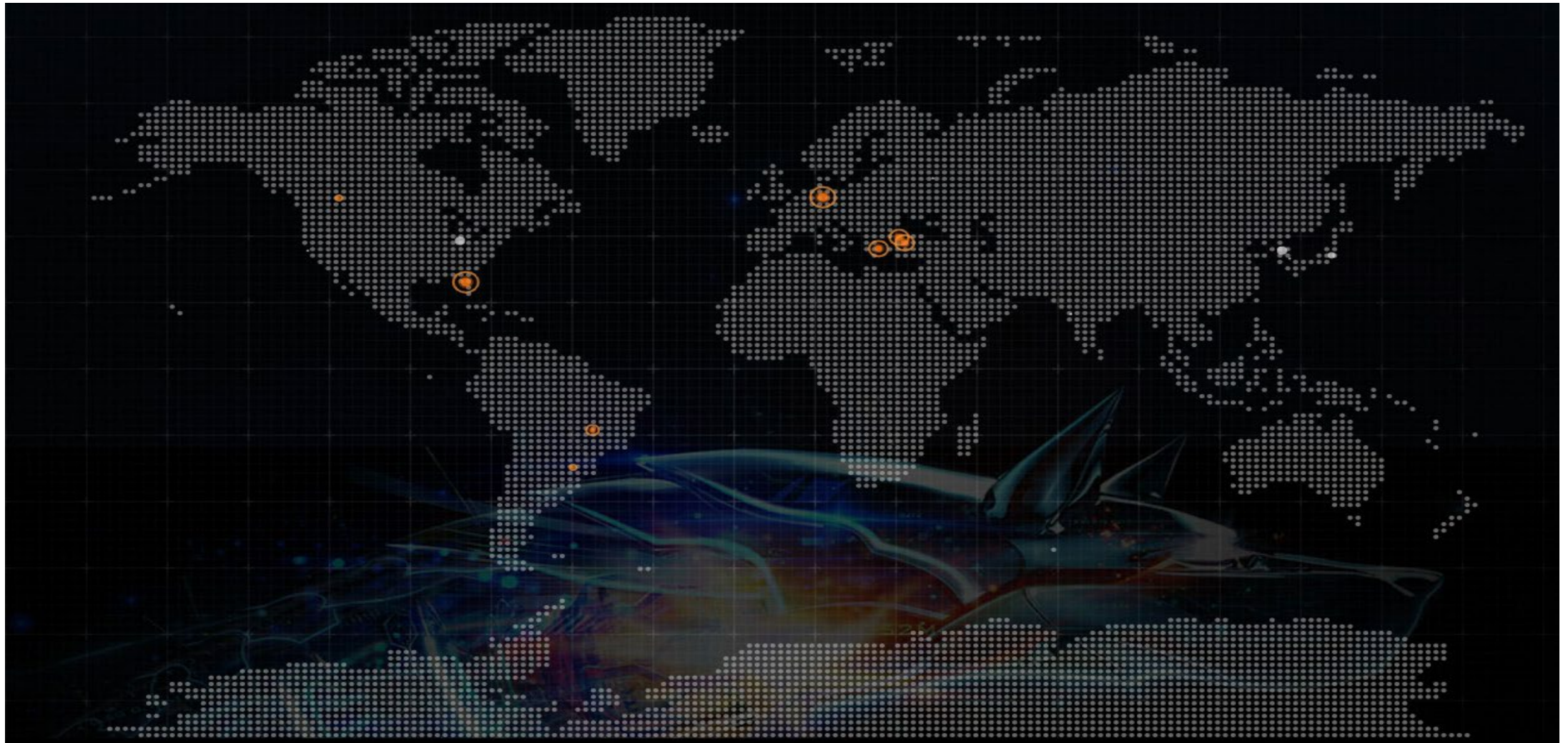
Το μέλλον σε νούμερα




Το κόστος από την παράνομη δραστηριότητα στον κυβερνοχώρο έως το 2025 αναμένεται να αγγίξει τα **10,5 τρισεκατομμύρια** δολάρια ετησίως *.

* Source: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

Κυβερνοεπιθέσεις σε πραγματικό χρόνο



Αντί επιλόγου



Αρκετά μεγάλο ποσοστό οργανισμών έχει υιοθετήσει τη ρήση *«Δεν πρέπει να σκέφτομαι το εάν θα δεχτώ επίθεση, αλλά το πότε»*.

Ακόμα και αυτό είναι πλέον ανεπαρκές, μιας και δεν οδηγεί στα επιθυμητά αποτελέσματα.

Η λογική πρέπει πλέον να είναι ότι:

«οι επιτιθέμενοι είναι ήδη μέσα, και καλούμαι να διασφαλίσω τη συνέχεια των εργασιών και λειτουργιών μου».

Thank you





www.kpmg.com/gr

© 2022 KPMG Σύμβουλοι Μονοπρόσωπη Α.Ε., Ελληνική Ανώνυμη Εταιρεία και μέλος του διεθνούς οργανισμού ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Limited, ιδιωτική Αγγλική εταιρεία περιορισμένης ευθύνης με εγγυητικές εισφορές. Με την επιφύλαξη κάθε δικαιώματος.
Οι πληροφορίες που περιέχονται στο παρόν είναι γενικής φύσεως και δεν έχουν σκοπό την επίλυση θεμάτων κάποιου συγκεκριμένου φυσικού προσώπου ή νομικής οντότητας. Αν και στόχος μας είναι να παρέχουμε ακριβείς και έγκαιρες πληροφορίες, δεν μπορεί να υπάρξει εγγύηση ότι πληροφορίες αυτές θα είναι ακριβείς κατά την ημερομηνία λήψης τους ή ότι θα συνεχίσουν να είναι ακριβείς στο μέλλον. Κανείς δεν πρέπει να ενεργεί βάσει αυτών των πληροφοριών χωρίς την κατάλληλη επαγγελματική συμβουλή η οποία θα παρέχεται μετά από ενδελεχή εξέταση της συγκεκριμένης περίπτωσης.
Το όνομα και το λογότυπο της KPMG είναι εμπορικά σήματα που χρησιμοποιούνται με άδεια του διεθνούς οργανισμού της KPMG από τις ανεξάρτητες εταιρείες-μέλη

Document Classification: KPMG Public