KPMG

# Cyber Risk Insurance

## Οι απειλές του κυβερνοχώρου για τις επιχειρήσεις

**Νίκος Αστυφίδης**

-

12 Οκτωβρίου 2022

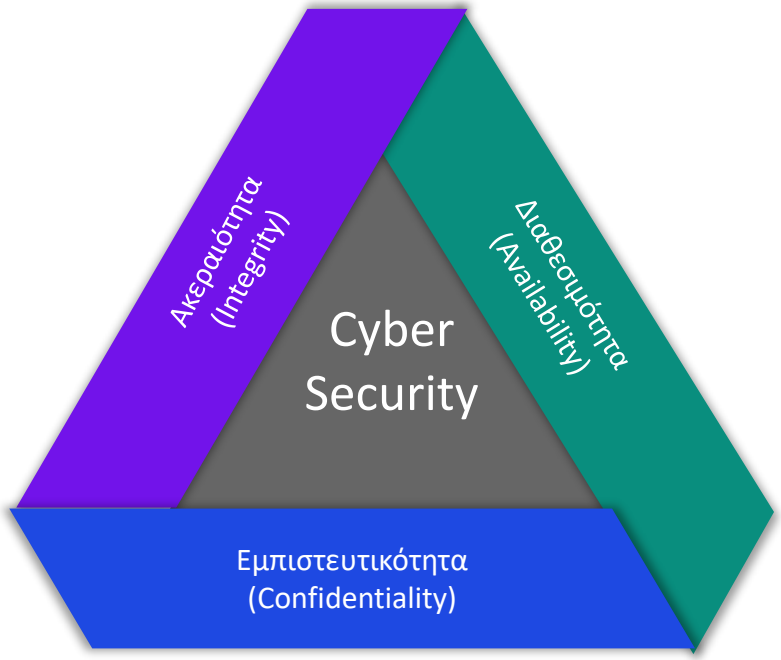
# Τι είναι η κυβερνοασφάλεια;

**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

Ransomware

Distributed DoS

Backdoor

Phishing

Person-in-the-middle

Insider threat

# 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.

Κίνδυνοι Προ-COVID

Επιτιθέμενος

Κίνδυνοι Μετά-COVID

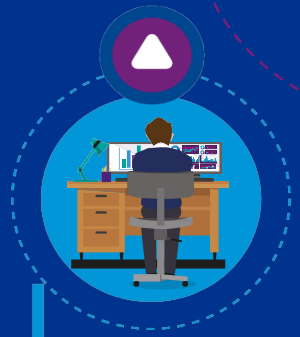
Οι κακόβουλοι εκτελούν την επίθεση με ransomware

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.



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

Αυξανόμενες απειλές για το cloud

**Μετά-COVID:**
Στοχευμένες επιθέσεις σε επιχειρήσεις

Οι επιτιθέμενοι εισχωρούν στα συστήματα

Αποκτούν 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.

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).

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

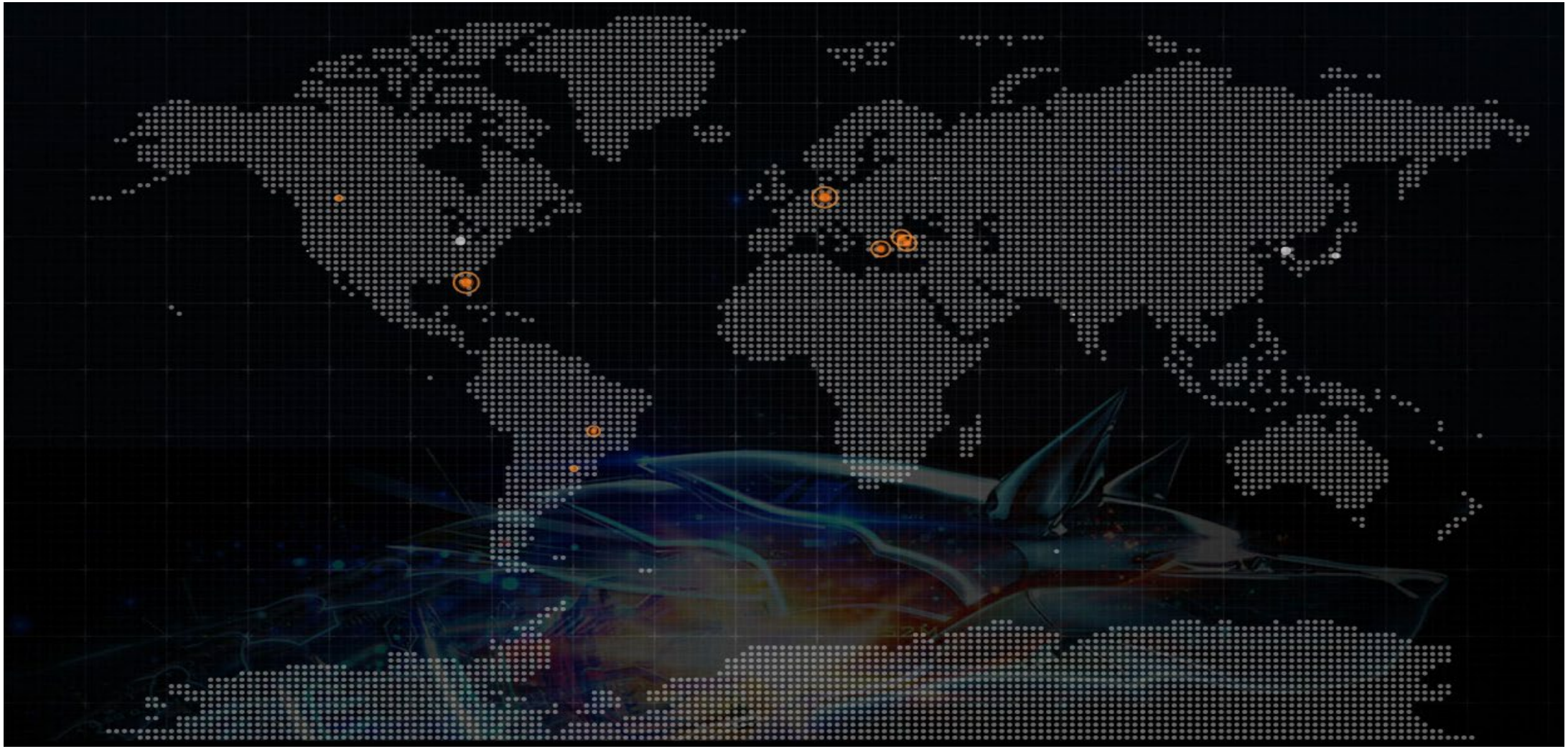
KPMG

# 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



**Document Classification: KPMG Public**