ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

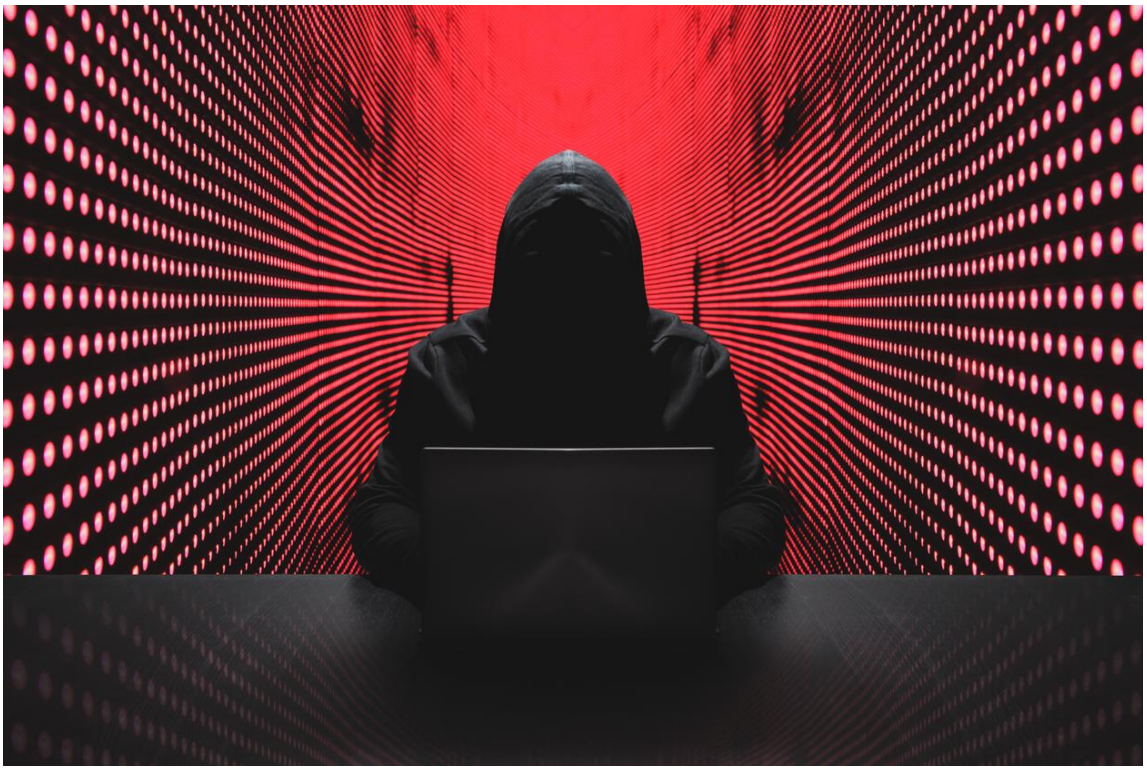
# *ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ*

*Τοπικότητα των Κυβερνοαπειλών: Ιομορφικό Λογισμικό*

*Ονοματεπώνυμα:*

*Μυρτώ-Χριστίνα Ελευθέρου, Α.Μ.: 3170046*

*Θανάς Κούρο, Α.Μ.: 3170078*



**1**

1 https://www.google.com/search?q=hacking&sxsrf=ALiCzsYiiztVoxUVCBxADVDTHnmyjfbOWQ:1652869517128&source=lnms&t

# Περιεχόμενα



# Εισαγωγή

Η κυβερνοασφάλεια αποτελεί μείζον ζήτημα της σύγχρονης κοινωνίας και είναι αναγκαίο να διασφαλιστεί η επίτευξή της. Οι πρακτικές, οι πολιτικές και η υλοποίηση της ασφάλειας, ποικίλουν, και διαφέρουν από χώρα σε χώρα, από κυβέρνηση σε κυβέρνηση και από οργανισμό σε οργανισμό. Αυτό, βέβαια, έχει ως αποτέλεσμα τη έντονη δυσκολία που αντιμετωπίζουν οι διαχειριστές έργων λογισμικού όταν πρόκειται να λάβουν αποφάσεις σχετικά με την ασφάλεια. Ιδανικά, για την επίλυση του συγκεκριμένου προβλήματος, οι κυβερνήσεις, οι εταιρίες και οι οργανισμοί θα έπρεπε να συνεργάζονται χρησιμοποιώντας τυπική ορολογία, ανταλλάσσοντας δεδομένα ή λαμβάνοντας μέρος σε έρευνες όποτε είναι δυνατόν, έτσι ώστε να υπάρχει μία συντονισμένη προσέγγιση για την πρόληψη και τον μετριασμό των επιθέσεων, καθώς και ενημέρωση για τις κυβερνητικές πολιτικές που επηρεάζουν την ασφάλεια στον κυβερνοχώρο.[15]

Επιπλέον, αξίζει να γίνει αναφορά στις κυβερνοεπιθέσεις, τον χακτιβισμό και την κυβερνοτρομοκρατία που αποτελούν τις κύριες απειλές για την κυβερνοασφάλεια, καθώς και να αποσαφηνιστούν οι όροι ώστε γίνουν κατανοητές οι διαφορές τους. Μια κυβερνοεπίθεση[20] είναι οποιοσδήποτε τύπος προσβλητικού ελιγμού που στοχεύει συστήματα πληροφορικής, υποδομές, δίκτυα υπολογιστών ή συσκευές προσωπικών υπολογιστών. Ο εισβολέας είναι ένα πρόσωπο ή μια διαδικασία που προσπαθεί να αποκτήσει πρόσβαση σε δεδομένα, λειτουργίες ή σε άλλες απαγορευμένες περιοχές του συστήματος χωρίς εξουσιοδότηση, ενδεχομένως με κακόβουλη πρόθεση. Από την άλλη πλευρά, ο χακτιβισμός αναφέρεται στον συνδυασμό του hacking με τον πολιτικό ακτιβισμό. Σε αντίθεση με τους χάκερς, οι οποίοι έχουν συνήθως οικονομικά κίνητρα, οι χακτιβιστές προσπαθούν να επιτύχουν κοινωνικούς ή πολιτικούς σκοπούς. Τέλος, η κυβερνοτρομοκρατία αναφέρεται σε παράνομες επιθέσεις και απειλές επιθέσεων κατά υπολογιστών, δικτύων και των πληροφοριών που αποθηκεύονται σε αυτά, και γίνονται για να εκφοβίσουν μια κυβέρνηση ή τους ανθρώπους της με σκοπό την προώθηση πολιτικών ή κοινωνικών στόχων.[10]

Ωστόσο η μορφή επίθεσης που θα εξετάσουμε ως επί το πλείστων είναι το ιομορφικό λογισμικό (malware), το οποίο αποτελεί αναμφισβήτητα μία από τις σημαντικότερες απειλές για την ασφάλεια των πληροφοριακών συστημάτων.

## ΙομορφικόΛογισμικό

Το ιομορφικό λογισμικό θεωρείται το λογισμικό, που η εκτέλεσή του μπορεί να διαταράξει την ομαλή λειτουργία ενός συστήματος, συλλέγοντας ευαίσθητες πληροφορίες ή εκτελώντας ενέργειες μη εξουσιοδοτημένες από τον χρήστη του συστήματος.[16] Το ιομορφικό λογισμικό χωρίζεται σε τρεις κύριες κατηγορίες: τον Δούρειο Ίππο (Trojan Horse), τον Αναπαραγωγό (worm) και το Πρόγραμμα Ιός (virus).

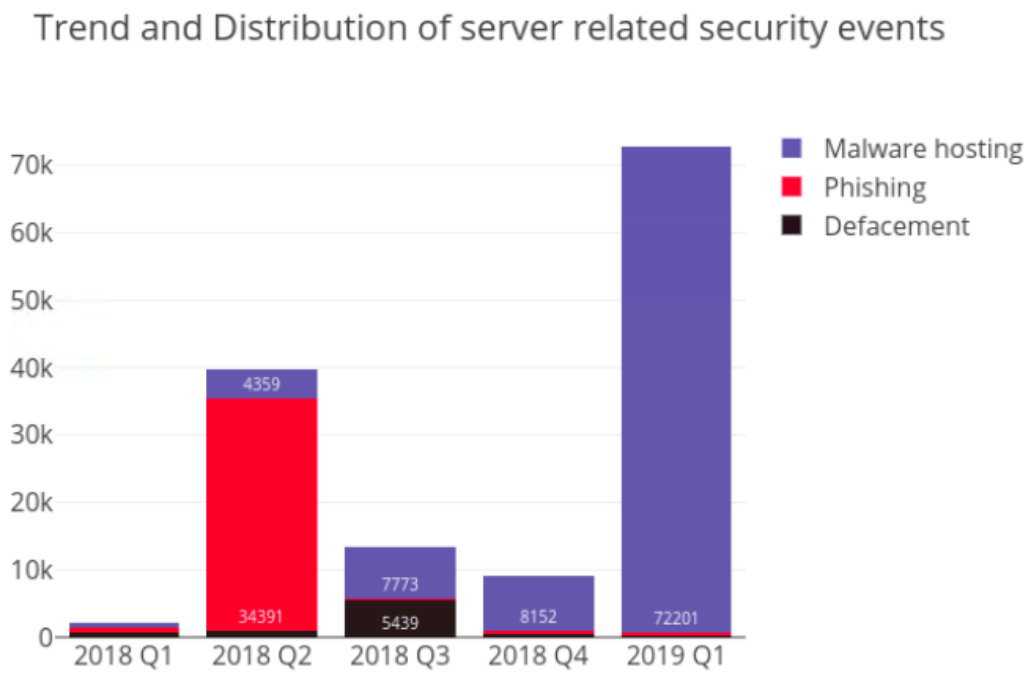
| | | |
|---|---|---|
| Δούρειος Ίππος ονομάζεται κάθε μορφή ιομορφικού λογισμικού που έχει τη δυνατότητα να συνυπάρχει με κάποιο λογικό αντικείμενο (ξενιστής) και να προκαλεί συνέπειες άγνωστες στο χρήστη του αντικειμένου αυτού | Αναπαραγωγός ονομάζεται κάθε μορφή ιομορφικού λογισμικού που έχει τη δυνατότητα να διαδίδεται αυτόαναπαραγόμενο και να προκαλεί συνέπειες άγνωστες στους χρήστες του συστήματος | Πρόγραμμα ιός ονομάζεται το εκτελέσιμο λογισμικό που έχει τη δυνατότητα να προστίθεται και να συνυπάρχει με άλλο λογικό αντικείμενο (ξενιστής), να αναπαράγεται μέσω της ενεργοποίησης του αντικειμένου αυτού και να προκαλεί συνέπειες άγνωστες στο χρήστη του αντικειμένου. [7] |

Όπως είναι προφανές, το κακόβουλο λογισμικό είναι λογισμικό που έχει σχεδιαστεί με πρόθεση να βλάψει τον χρήστη του υπολογιστή. Ανάλογα με τη φύση της βλάβης που στοχεύεται, χρησιμοποιείται ο κατάλληλος τύπος κακόβουλου λογισμικού. Μέχρι σήμερα, έχουν εντοπιστεί εκατομμύρια διαφορετικοί ιοί και άλλα κακόβουλα προγράμματα, ορισμένα από τα οποία έχουν προκαλέσει σημαντικές ζημιές σε άτομα και οργανισμούς, που φτάνουν ακόμα και ποσά δισεκατομμυρίων δολαρίων. Για παράδειγμα το κακόβουλο λογισμικό με τη μεγαλύτερη ζημιά που είναι γνωστό μέχρι σήμερα ήταν τα σκουλήκια Sasser και Netsky το 2004, με εκτιμώμενη ζημιά ύψους 31 δισεκατομμυρίων δολαρίων. Επιπλέον, αξίζει να σημειωθεί ότι, μερικές φορές, ακόμη και οι κυβερνήσεις τείνουν να χρησιμοποιούν κακόβουλο λογισμικό για κατασκοπεία και άλλα πολιτικά κίνητρα.

Ο συνηθέστερος τρόπος αντιμετώπισης τέτοιων λογισμικών, είναι η χρήση λογισμικού ασφαλείας, όπως τείχη προστασίας, λογισμικό προστασίας από ιούς και λογισμικό προστασίας από κατασκοπεία. Η χρήση λογισμικών ασφαλείας θεωρείται απαραίτητη, καθώς τα υπάρχοντα στοιχεία δείχνουν ότι η ανεύθυνη χρήση του διαδικτύου, όπως παραδείγματος χάριν η αποτυχία χρήσης λογισμικού ασφαλείας ή το κλικ σε αμφισβητούμενους ιστότοπους, μπορεί να οδηγήσει πολύ συχνά σε μόλυνση από κακόβουλο λογισμικό. Παράλληλα, για την αποτελεσματική αντιμετώπιση ενός κακόβουλου λογισμικού, πρέπει να εξεταστεί επίσης και η ανθρώπινη πλευρά του ζητήματος. Αυτό σημαίνει, ότι εφόσον οι προγραμματιστές κακόβουλου λογισμικού βελτιώνουν συνεχώς την ικανότητα τους να αναπτύσσουν κακόβουλο λογισμικό που δεν εντοπίζεται, τότε και οι προγραμματιστές μη κακόβουλου λογισμικού πρέπει να παραμένουν συνεχώς καινοτόμοι για την καταπολέμηση εξυπνότερου κακόβουλου λογισμικού. Αυτό επιβεβαιώνεται επίσης, από το γεγονός ότι οι εταιρίες προστασίας από ιούς αντιμετωπίζουν δεκάδες χιλιάδες νέα δείγματα κακόβουλου λογισμικού σε καθημερινή βάση.[8]

## Ιομορφικό Λογισμικό στο Χονγκ-Κονγκ

Το Χονγκ Κονγκ φαίνεται να αντιμετωπίζει και να βιώνει τεράστια αύξηση εγκλημάτων στον κυβερνοχώρο, κατά την τελευταία δεκαετία. Τα περιστατικά κυβερνοεπιθέσεων έχουν αυξηθεί από 2206 το 2011 σε 12916 το 2020 και μάλιστα σημειώθηκε 55% αύξηση αυτών το 2020 σε σχέση με το 2019. [14] Ειδικά, το 1ο τρίμηνο του 2019 ο συνολικός αριθμός των περιστατικών κυβερνοασφάλειας αυξήθηκε κατά 329% σε σχέση με το τελευταίο τρίμηνο του 2018. [13] Εντυπωσιακή αύξηση σημειώθηκε σε επιθέσεις που αφορούν το κακόβουλο λογισμικό (malware), όπου οι επιθέσεις αυτών ανήλθαν σε 72201 από 8152 το προηγούμενο τρίμηνο.




(Πηγή εικόνας: https://portswigger.net/cms/images/43/8f/35dcb5337f9b-article-screenshot_2019-05-02_at_10.54.38.png)

Μία σημαντική μορφή malware αποτελεί το ransomware που σύμφωνα με έρευνα, μία στις 10 εταιρίες στο Χονγκ Κονγκ έχει αντιμετωπίσει επίθεση ransomware. [2] Στο Χονγκ Κονγκ, ως παγκόσμιο οικονομικό κέντρο και λόγω της ευρείας χρήσης της τεχνολογίας από επιχειρήσεις και οργανισμούς επεξεργασίας δεδομένων, αυξάνεται ο κίνδυνος επιθέσεων κακόβουλου λογισμικού. Αυτό συνεπάγεται σε πιθανές απώλειες, υποκλοπές ή και διαγραφές δεδομένων, όπου αν δε ληφθούν μέτρα πρόληψης -όπως η δημιουργία αντιγράφων ασφαλείας σε cloud- θα είναι οριστικές.

Ένα πρόβλημα που υπάρχει είναι πως το Χονγκ Κονγκ δε διαθέτει αυτόνομη νομοθεσία για την ασφάλεια στον κυβερνοχώρο ή τα εγκλήματα στον κυβερνοχώρο.[19] Παρά το γεγονός αυτό, το Διάταγμα Προσωπικών Απόρρητων Δεδομένων (PDPO) θεσπίζει το

νομικό πλαίσιο προστασίας δεδομένων ιδιωτικού απορρήτου του Χονγκ Κονγκ. Όλοι οι οργανισμοί που είναι χρήστες δεδομένων, δηλαδή επεξεργάζονται, χρησιμοποιούν ή διατηρούν προσωπικά δεδομένα, θα πρέπει να συμμορφώνονται με το PDPO και με τις έξι βασικές αρχές του.

Ο νέος νόμος κατά του doxing του Χονγκ Κονγκ, που ποινικοποιεί τη μη συναινετική αποκάλυψη ευαίσθητων προσωπικών δεδομένων, έχει τεθεί σε ισχύ παρά την αντίθεση αρκετών εταιριών πληροφορικής και οργανισμών υποστηρικτών προστασίας της ιδιωτικής ζωής.[1] Το PCPD (Office of Privacy Commissioner for Personal Data), η εγχώρια ρυθμιστική αρχή προστασίας δεδομένων του Χονγκ Κονγκ είναι εξουσιοδοτημένο να μπορεί να ελέγχει ολόκληρους ηλεκτρονικούς εξοπλισμούς παρόχων διαδικτυακών υπηρεσιών. Αυτό συμπεριλαμβάνει και την δυνατότητα συλλήψεων χωρίς εντάλματα και μπορεί να αιτείται να αφαιρεθεί περιεχόμενο αναρτημένο στο διαδίκτυο σε ιστοτόπους που βρίσκονται εκτός του Χονγκ Κονγκ. Συνέπεια μη τήρησης των παραπάνω κανόνων και νόμων είναι η επιβολή μεγάλων προστίμων σε εταιρίες και οργανισμούς. Όλες αυτές οι νέες διατάξεις έχουν προκαλέσει ανησυχία σε εταιρίες πληροφορικής, οι οποίες φοβούνται για τον κίνδυνο στον οποίο ενδεχομένως να εκτίθενται το προσωπικό τους.

Αξιοσημείωτη αποτελεί η επιστολή που στάλθηκε από την Asia Internet Coalition (AIC) , μία εμπορική ένωση που εκπροσωπεί μεταξύ άλλων την Google, το Facebook, και το Twitter, προς την κυβέρνηση του Χονγκ Κονγκ. Όπως αναφερόταν, «η θέσπιση κυρώσεων που στοχεύουν σε άτομα δεν ευθυγραμμίζεται με τους παγκόσμιους κανόνες και τάσεις» σημειώνοντας πως οι εταιρίες τεχνολογίας ενδέχεται να αποθαρρυνθούν και να «απέχουν από το να επενδύσουν και να προσφέρουν τις υπηρεσίες τους στο Χονγκ Κονγκ».

## Ιομορφικό Λογισμικό στις Ηνωμένες Πολιτείες

Μία από τις σοβαρότερες προκλήσεις που αντιμετωπίζουν οι Ηνωμένες Πολιτείες του 21ου αιώνα είναι οι απειλές που αφορούν τον κυβερνοχώρο, όπως για παράδειγμα το ιομορφικό λογισμικό. Συγκεκριμένα, μία πολύ συχνή μορφή ιομορφικού λογισμικού που εμφανίζεται στις Ηνωμένες Πολιτείες είναι το ransomware[4]. Το ransomware είναι μια μορφή κακόβουλου λογισμικού που εξελίσσεται συνεχώς και έχει σχεδιαστεί για την κρυπτογράφηση αρχείων σε μια συσκευή, καθιστώντας τυχόν αρχεία και τα συστήματα που βασίζονται σε αυτά άχρηστα. Οι κακόβουλοι “ηθοποιοί” στη συνέχεια ζητούν λύτρα με αντάλλαγμα την αποκρυπτογράφηση.[5]

Για την αντιμετώπιση και την προστασία από τις κυβερνοαπειλές έχουν θεσπιστεί κάποιοι νόμοι. Οι τρεις από τους σημαντικότερους νόμους που αφορούν την κυβερνοασφάλεια στις Ηνωμένες Πολιτείες είναι οι εξής:

- Health Insurance Portability and Accountability Act (HIPAA)[3]
- Gramm-Leach-Bliley Act [9]
- Homeland Security Act [11]

Ο πρώτος κανόνας ασφάλειας HIPAA προστατεύει όλες τις μεμονωμένα αναγνωρίσιμες πληροφορίες υγείας που δημιουργεί, λαμβάνει, διατηρεί ή μεταδίδει σε ηλεκτρονική μορφή μια καλυπτόμενη οντότητα.

Ο δεύτερος νόμος Gramm-Leach-Bliley Act απαιτεί από τα χρηματοπιστωτικά ιδρύματα, δηλαδή από εταιρείες που προσφέρουν στους καταναλωτές χρηματοοικονομικά προϊόντα ή υπηρεσίες όπως δάνεια, οικονομικές ή επενδυτικές συμβουλές ή ασφάλειες, να εξηγούν τις πρακτικές ανταλλαγής πληροφοριών στους πελάτες τους και να προστατεύουν τα ευαίσθητα δεδομένα.

Ο τρίτος νόμος Homeland Security Act ενοποιεί 22 διαφορετικές υπηρεσίες και γραφεία στο Υπουργείο Εσωτερικής Ασφάλειας (DHS) με εντολή την πρόληψη και την αντιμετώπιση φυσικών και ανθρωπογενών καταστροφών.

Ωστόσο, μετά την έναρξη του πολέμου Ρωσίας - Ουκρανίας το πρόβλημα έχει πάρει ακόμα μεγαλύτερες διαστάσεις. Η Αμερική, η οποία υποστηρίζει την Ουκρανία, πρέπει να βρίσκεται συνεχώς σε ετοιμότητα για πιθανές κυβερνοεπιθέσεις από την ρωσική κυβέρνηση και οι ήδη υπάρχοντες νόμοι δεν φαίνεται να είναι επαρκής.

Έτσι, με αφορμή την ρωσική απειλή, την Τρίτη 15 Μαρτίου ο Πρόεδρος Μπάιντεν υπέγραψε νόμο, ο οποίος καθιστά υποχρεωτική την αναφορά περιστατικών κυβερνοασφάλειας που συμβαίνουν σε υποδομές ζωτικής σημασίας.

Αρχικά, ως υποδομές ζωτικής σημασίας ορίζονται τα συστήματα, τα δίκτυα, φυσικά ή εικονικά και τα περιουσιακά στοιχεία του κυβερνοχώρου που είναι τόσο σημαντικά για τις Ηνωμένες Πολιτείες που η αδυναμία ή η καταστροφή τους θα είχε εξουθενωτική επίδραση στην ασφάλεια, την εθνική οικονομική ασφάλεια, την εθνική δημόσια υγεία ή ασφάλεια, ή οποιονδήποτε συνδυασμό αυτών (παραδείγματος χάριν εταιρείες χρηματοοικονομικών υπηρεσιών, εταιρείες ενέργειας, εταιρίες πληροφορικής).[6]

Ο νόμος ορίζει ότι μια καλυπτόμενη οντότητα[2] που αντιμετωπίζει ένα καλυπτόμενο περιστατικό[3] στον κυβερνοχώρο υποχρεούται να αναφέρει το περιστατικό στην CISA εντός 72 ωρών από τη στιγμή που η οντότητα πιστεύει ότι συνέβη το συμβάν. Επιπλέον, σε περίπτωση που μία καλυπτόμενη οντότητα πραγματοποιήσει οποιαδήποτε πληρωμή λύτρων (εξαιτίας επίθεσης ransomware), το γεγονός αυτό πρέπει να αναφερθεί στην CISA εντός 24 ωρών. Σε περίπτωση που διατίθενται νέες ή ουσιαστικές πληροφορίες για κάποιο γεγονός, οι οντότητες είναι υποχρεωμένες να συνεχίσουν να υποβάλλουν ενημερωμένες αναφορές στην CISA.[12]

Τέλος, ο Πρόεδρος Μπάιντεν ανέφερε[17] πρόσφατα σε ομιλία του ότι επειδή το μεγαλύτερο μέρος της υποδομής ζωτικής σημασίας της Αμερικής λειτουργεί από τον ιδιωτικό τομέα, είναι σημαντικό οι τομείς να επιταχύνουν τις προσπάθειες για να κλειδώσουν τις ψηφιακές τους πόρτες όσο το δυνατόν συντομότερο. Στη συνέχεια προτρέπει τους εταίρους του στον ιδιωτικό τομέα να σκληρύνουν άμεσα την άμυνα

[2] Ο νόμος ορίζει μια «καλυπτόμενη οντότητα» ως «μια οντότητα σε τομέα υποδομής ζωτικής σημασίας.

[3] Ενα «καλυπτόμενο περιστατικό στον κυβερνοχώρο» σημαίνει «ένα σημαντικό περιστατικό στον κυβερνοχώρο που συμβαίνει από μια καλυπτόμενη οντότητα».

τους στον κυβερνοχώρο εφαρμόζοντας διάφορες πρακτικές[18] που έχουν δημοσιευθεί στον ιστότοπο του Λευκού Οίκου.

## Συμπέρασμα

Από όσα αναφέρθηκαν παραπάνω καταλήγουμε στο συμπέρασμα ότι στις Ηνωμένες Πολιτείες Αμερικής ενέχουν πολλοί κίνδυνοι και η πιθανότητα μιας κυβερνοεπίθεσης που σχετίζεται με κάποιο ιομορφικό λογισμικό είναι πολλή μεγάλη. Αντίστοιχα, το Χονγκ Κονγκ έχει αποτελέσει κέντρο αρκετών κυβερνοεπιθέσεων, ως παγκόσμιο οικονομικό κέντρο. Η επέκταση ενός Μη Κυβερνητικού Οργανισμού στις Ηνωμένες Πολιτείες είναι εφικτή, εφόσον όμως συμβαδίζει με τους νόμους που είναι σε ισχύ έτσι ώστε να μην υπάρχουν κυρώσεις και να επιτευχθεί όσο το δυνατόν μεγαλύτερη ασφάλεια. Ωστόσο ίσως να μην είναι η κατάλληλη στιγμή να γίνει μια τέτοια ενέργεια, τουλάχιστον για όσο χρονικό διάστημα ο πόλεμος Ρωσίας-Ουκρανίας βρίσκεται σε εξέλιξη με αποτέλεσμα οι κυβερνοεπιθέσεις να βρίσκονται σε έξαρση. Αναφορικά με το Χονγκ Κονγκ, μέτρα και νόμοι έχουν ληφθεί από οργανισμούς για την κυβερνοασφάλεια, αλλά δεν υπάρχει αυτόνομη νομοθεσία για τον κυβερνοχώρο. Παρότι οι νέοι αυτοί νόμοι, κυρίως κατά του doxxing έχουν ως σκοπό την προστασία προσωπικών δεδομένων, πολλές εταιρίες είναι αντίθετες ως προς του νόμους αυτούς λόγω της αυστηρότητας και του κινδύνου που μπορεί να βρεθεί το προσωπικό των εταιριών αυτών. Όσο αφορά το Χονγκ Κονγκ, λοιπόν, υπάρχει μία αποθάρρυνση εταιριών για την προσφορά υπηρεσιών τους στο Χονγκ Κονγκ, όπως αναφέρεται παραπάνω.

## Βιβλιογραφία


[1] Adam Bannister, 2021. *Hong Kong's anti-doxxing law comes into force despite human rights criticism.* [online] Available at: <https://portswigger.net/daily-swig/hong-kongs-anti-doxxing-law-comes-into-force-despite-human-rights-criticism> [Accessed 25 April 2021].

[2] BSA, 2017. *Survey Shows That One out of Ten Companies in Hong Kong Have Faced a Ransomware Attack.* [online] Available at: <https://www.bsa.org/news-events/news/survey-shows-that-one-out-of-ten-companies-in-hong-kong-have-faced-a-ransomware-attack> [Accessed 24 April 2021].

[3] CDC. ***Health Insurance Portability and Accountability Act of 1996 (HIPAA).*** Available at: <https://www.cdc.gov/phlp/publications/topic/hipaa.htm> [Accessed 23 April 2021].

[4] CISA. 2021. ***Trends show increased globalized threat of ransomware*** . Available at: <https://www.cisa.gov/uscert/ncas/alerts/aa22-040a> [Accessed 24 April 2021].

[5] CISA. ***Guidance and Resources***. Available at: <https://www.cisa.gov/stopransomware> [Accessed 23 April 2021].

[6] CISA. ***INFRASTRACTURE SECURITY***. Available at: <https://www.cisa.gov/infrastructure-security> [Accessed 22 April 2021].

[7] Dimitris Gritzalis. 2014. ***Malware: A primer***. Available at: <infosec.aueb.gr/Publications/University%20Peireus%20Malware%202012.pdf> [Accessed 21 April 2021].

[8] Fawn T. Ngo, Anurag Agarwal, Ramakrishna Govindu, Calen MacDonald. 2020. ***Malicious Software Threats.*** Available at: <https://link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3_35?noAccess=true> [Accessed 20 April 2021].

[9] Federal Trade Commision. 2002. ***Gramm-Leach-Bliley Act***. Available at: <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act> [Accessed 23 April 2021].

[10] Gabriel Weimann. 2004. ***Cyberterrorism***. Available at: <https://www.usip.org/sites/default/files/sr119.pdf> [Accessed 20 April 2021].

[11] Homeland Security. 2002. ***Public Law 107–296.*** Available at: <https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf> [Accessed 23 April 2021].

[12] House of Representatives Committee on Rules. 2002. ***RULES COMMITTEE PRINT 117–35.*** Available at: <https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR2471SA-RCP-117-35.pdf> [Accessed 23 April 2021].

[13] Jessica Haworth, 2019. *Security incidents in Hong Kong up nearly 400% in Q1* [online] Available at: <https://portswigger.net/daily-swig/security-incidents-in-hong-kong-up-nearly-400-in-q1> [Accessed 23 April 2021].

[14] King Au, 2021. *Hong Kong Business – Hong Kong can do more in fight against rising cybercrime in financial sector* [online] Available at: <https://www.fsdc.org.hk/en/media/hong-kong-business-20211004-hong-kong-can-do-more-in-fight-against-rising-cybercrime-in-financial-sector#> [Accessed 23 April 2021].

[15]Michael Neumann. 2008. ***Cybersecurity Economic Issues*** Available at: <https://www.rand.org/content/dam/rand/pubs/research_briefs/2008/RAND_RB9365-1.pdf> [Accessed 23 April 2021].

[16] Muchammad Naseer. 2021. ***Malware Detection: Issues and Challenges.*** Available at: <https://iopscience.iop.org/article/10.1088/1742-6596/1807/1/012011/pdf> [Accessed 20 April 2021].

[17] WHITEHOUSE. 2022. ***Statement by President Biden on our Nation's Cybersecurity***. Available at: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/> [Accessed 21 April 2021].

[18] WHITEHOUSE. 2022. ***Act now to Protect Against Potential Cyberattacks***. Available at: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/> [Accessed 21 April 2021].

[19] Yuet Ming Tham, 2021. *The privacy, Data Protection and Cybersecurity Law Review: Hong Kong.* [online] Available at: <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/hong-kong#:~:text=Although%20Hong%20Kong%20does%20not,to%20cyber%20threats%20and%20incidents> [Accessed 24 April 2021].

[20] Παναγιώτης Νιάκαρης. 2019. ***Η κυβερνοεπίθεση ως νέα παγκόσμια απειλή. Οι Ευρωπαϊκές απαντήσεις.*** Available at: <http://pandemos.panteion.gr/index.php?op=record&pid=iid:20098&lang=e> [Accessed 22 April 2021].