ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τοπικότητα των Κυβερνοαπειλών: Ιομορφικό Λογισμικό

Γραπτή Εργασία Εαρινού Εξαμήνου 2021-2022

ΣΤΟΙΧΕΙΑ ΦΟΙΤΗΤΩΝ

ΜΕΛΗ ΟΜΑΔΑΣ	ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ
Φίλιππος Δουραχαλής	3170045
Γεωργία Ζαχαροπούλου	3170049
Μαρία Πανοπούλου	3170129

ΔΙΔΑΣΚΩΝ:

Γκρίτζαλης Δημήτρης

Αθήνα, 25 Απριλίου, 2022

Περιεχόμενα

ΕΙΣΑΓΩΓΗ 2
ΚΥΡΙΟ ΜΕΡΟΣ 3
1. ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΔΡΑΣΤΗΡΙΟΠΟΙΗΣΗΣ ΟΡΓΑΝΙΣΜΟΥ – ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ 3
2. ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ - ΗΠΑ 3
2.1 Νομοθεσία περί κυβερνοασφάλειας και προστασία προσωπικών δεδομένων στις Η.Π.Α. 3
2.2 Σημαντικότερες επιθέσεις - Εύρος Απειλής 4
2.3 Περιορισμοί 5
2.4 Δυνατότητες και τρόποι αντιμετώπισης 5
3. ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ - ΧΟΝΓΚ ΚΟΝΓΚ 6
3.1 Εισαγωγικά Στοιχεία 6
3.2 Περιβάλλον δράσης των Μ.Κ.Ο. 6
3.3 Εύρος της απειλής 7
3.4 Περιορισμοί 9
3.5 Δυνατότητες και τρόποι αντιμετώπισης 9
4. ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ 10
4.1 Συμβουλές για τη δραστηριοποίηση στις Η.Π.Α. 11
4.2 Συμβουλές για τη δραστηριοποίηση στο Χονγκ Κονγκ 12
ΒΙΒΛΙΟΓΡΑΦΙΑ 13

Σύνολο λέξεων (δεν περιλαμβάνει βιβλιογραφία και πίνακες): 2.682

ΕΙΣΑΓΩΓΗ

Στην παρούσα αναφορά αναλύουμε την κατάσταση που επικρατεί σε κάθε χώρα συγκεκριμένα στο Χονγκ Κονγκ και στις Η.Π.Α. αναφορικά με το ιομορφικό λογισμικό, λαμβάνοντας υπόψιν τις τεχνολογικές, κοινωνικές και πολιτικές διαφορές. Βάσει αυτών, προτείνουμε κατάλληλα και αναλογικά μέτρα που πρέπει να λάβει για να δραστηριοποιηθεί σε καθεμιά.

ΚΥΡΙΟ ΜΕΡΟΣ

1. ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΔΡΑΣΤΗΡΙΟΠΟΙΗΣΗΣ ΟΡΓΑΝΙΣΜΟΥ – ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

Σχετικά με τη νομοθεσία της Ευρωπαϊκής Ένωσης, ισχύει η οδηγία 2016/679/Ε.Ε. (Γενικός Κανονισμός Προστασίας Δεδομένων - Γ.Κ.Π.Δ.)[1] σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα, ενώ όλα τα κράτη μέλη πρέπει να ακολουθούν και να έχουν ενσωματώσει στην νομοθεσία τους την οδηγία 2016/1148/Ε.Ε. (Οδηγία Ν.Ι.S.)[2], καθώς και την οδηγία 2013/40/Ε.Ε.[3].

2. ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ - ΗΠΑ

2.1 Νομοθεσία περί κυβερνοασφάλειας και προστασία προσωπικών δεδομένων στις Η.Π.Α.

Στις Η.Π.Α. δεν υπάρχει κάποιος καθολικός και ολοκληρωμένος νόμος για την προστασία των προσωπικών δεδομένων και της κυβερνοασφάλειας, αλλά αντίθετα ισχύουν διαφορετικές ομοσπονδιακές νομοθεσίες που καλύπτουν διαφορετικά δικαιώματα και υποχρεώσεις. Αυτές είναι οι εξής:

Ομοσπονδιακοί Νόμοι προστασίας δεδομένων
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Children's Online Privacy Act (COPPA)
Electronic Communications Privacy Act (ECPA)

Πίνακας 1 Ομοσπονδιακοί νόμοι περί Κυβερνοασφάλειας και Προστασίας Προσωπικών Δεδομένων στις ΗΠΑ

Οι νόμοι κάθε πολιτείας, μπορούν να επιβάλλουν πρόσθετες υποχρεώσεις σε οργανισμούς που χειρίζονται προσωπικά δεδομένα (Microsoft Corporation, 2017).[4]

[1] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434
[2] https://www.enisa.europa.eu/topics/nis-directive?tab=details
[3] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32013L0040
[4] https://www.councilofnonprofits.org/sites/default/files/documents/nonprofit-guidelines-for-cybersecurity-and-privacy.pdf

Από τις πολιτείες των Η.Π.Α. εκείνες που έχουν θεσπίσει ολοκληρωμένους και εκτενείς νόμους για το απόρρητο των δεδομένων των καταναλωτών είναι η Καλιφόρνια, το Κολοράντο και η Βιρτζίνια (National Conference of State Legislature (NCSL), 2022) [5]. Οι νόμοι συνοψίζονται στον παρακάτω πίνακα:

Πολιτεία	Νόμος περί ιδιωτικότητας προσωπικών δεδομένων
Καλιφόρνια	California Consumer Privacy Act of 2018 – CCPA & California Consumer Privacy Rights Act – CCPRA (επέκταση)
Κολοράντο	Colorado Privacy Act - CPA
Βιρτζίνια	Virginia Consumer Data Protection Act - VCDPA

Πίνακας 2 Ειδικοί νόμοι Προστασίας Προσωπικών Δεδομένων ανά πολιτεία

2.2 Σημαντικότερες επιθέσεις - Εύρος Απειλής

Σύμφωνα με το Κέντρο Στρατηγικής και Διεθνούς Μελέτης (Centre for Strategic and International Studies - CSIS) (2022), από το 2020 έως σήμερα σημειώθηκαν 26 σημαντικά περιστατικά ασφαλείας που αφορούν επιθέσεις με ιομορφικό λογισμικό εναντίον κυβερνητικών οργανισμών και εταιρίες τεχνολογίας[6]. Μεταξύ αυτών ήταν η επίθεση σε κυβερνητικά και εταιρικά δίκτυα μέσω της εισαγωγής μιας κερκόπορτας στο λογισμικό Orion της εταιρίας SolarWinds, που καταλογίζεται ως μια από τις πιο σοβαρές επιθέσεις εναντίον των Η.Π.Α. τα τελευταία χρόνια.[7]

Ακόμη, το Touro College Illinois (2021) αναφέρει πως υπάρχει αύξηση τα τελευταία χρόνια επιθέσεων λυτρισμικού, μερικές από τις οποίες αποτελούν επίσης επιθέσεις υψηλού προφίλ[8]εναντίον εταιρειών και οργανισμών των Η.Π.Α. και οδήγησαν στη διακοπή της λειτουργίας υποδομών που έχουν ζωτική σημασία.

Μερικές από τις μεγαλύτερες επιθέσεις λυτρισμικού που έλαβαν χώρα το 2021 αφορούσαν τις παρακάτω εταιρίες και υποδομές των Η.Π.Α.:

- Colonial Pipeline
- Steamship Aythority of Massachusetts
- JBS Food
- Washington DC Metropolitan Police Department

[5] https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx
[6] https://csis-website-prod.s3.amazonaws.com/s3fs-public/220404_Significant_Cyber_Incidents.pdf?6baqc92oMg0w.0wCwZLP6OATs9MmMmLG
[7] https://www.tandfonline.com/doi/epub/10.1080/00396338.2021.1906001?needAccess=true
[8] https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php

Ιδιαίτερα για τις Μ.Κ.Ο., εκείνες που συγκεντρώνουν μεγάλα χρηματικά ποσά και αποθηκεύουν προσωπικά δεδομένα μπορεί συχνά να φαίνονται ως «εύκολοι στόχοι» λόγω των ελλιπών μέτρων ασφαλείας που εφαρμόζουν[9] (Mierzwa και Scott, 2017) και επομένως να δεχθούν κυβερνοεπιθέσεις που έχουν χρηματικά κίνητρα, όπως αναφέρει η Stéphane Duguin (2022).[10]

2.3 Περιορισμοί

Η νομοθεσία των Η.Π.Α. δεν περιορίζει τις Μ.Κ.Ο. να ασκήσουν κριτική σε πολιτικά ζητήματα ή την ίδια την κυβέρνηση. Επακολούθως, εκείνες έχουν την ελευθερία να υπερασπίζονται ανοικτά τα δικαιώματα που θεωρούν οι ίδιες κρίσιμα και να εκφράζουν τις απόψεις τους πάνω σε σχετικά ζητήματα, με προϋπόθεση την απόκτηση άδειας σε κάθε πολιτεία που δραστηριοποιείται ο οργανισμός και την περιοδική αναφορά των δράσεων, των σχέσεων και των χρηματοδοτήσεών του (Bureau of Democracy, Human Rights, and Labor, 2021).[11]

Σύμφωνα με το Εθνικό Συμβούλιο των Μ.Κ.Ο. (National Council of Nonprofits) (2017) ο οργανισμός χρειάζεται να λάβει σημαντικά μέτρα κυβερνοασφάλειας εάν οι δραστηριότητες του περιλαμβάνουν κάτι από τα ακόλουθα:

- E-commerce, όπως για παράδειγμα επεξεργασία δωρεών και εγγραφές εκδηλώσεων.
- Αποθήκευση και μεταφορά (για παράδειγμα αποστολή στο cloud) προσωπικών στοιχεία ταυτοποίησης για οποιονδήποτε, συμπεριλαμβανομένων και των δωρητών.
- Συλλογή πληροφοριών για τις προτιμήσεις και τις συνήθειες των δωρητών, των θαμώνων, των συνδρομητών.

Καθίσταται σαφές πως όταν υπάρχει παραβίαση του απορρήτου των προσωπικών δεδομένων, που συλλέγουν και αποθηκεύουν οι Μ.Κ.Ο., η κατάσταση είναι ιδιαίτερα κρίσιμη. Υπάρχει κίνδυνος τόσο για τα υποκείμενα των οποίων τα δεδομένα αποκαλύφθηκαν όσο και για τον Μ.Κ.Ο. που θα έχει ευθύνη για την παραβίαση[12] (Shavell, 2021).

2.4 Δυνατότητες και τρόποι αντιμετώπισης

Στις Η.Π.Α. υπάρχουν διάφοροι οργανισμοί που δραστηριοποιούνται στον τομέα των μη κερδοσκοπικών οργανισμών και μέλημά τους είναι να παρέχουν συμβουλές προς

[9] https://www.researchgate.net/profile/Stan-Mierzwa/publication/314096686_Cybersecurity_in_Non-Profit_and_Non-Governmental_Organizations/links/58b5672f92851ca13e52a312/Cybersecurity-in-Non-Profit-and-Non-Governmental-Organizations.pdf
[10] https://reliefweb.int/report/world/cyberattacks-real-threat-ngos-and-nonprofits
[11] https://www.state.gov/non-governmental-organizations-ngos-in-the-united-states/
[12] https://philanthropynewsdigest.org/features/the-sustainable-nonprofit/it-s-time-for-ngos-and-nonprofits-to-tighten-their-cybersecurity-standards

αυτούς. Αρχικά, υπάρχει το Εθνικό Συμβούλιο των Μ.Κ.Ο., το οποίο παρέχει συμβουλές στους οργανισμούς που επεξεργάζονται δεδομένα για το πως μπορούν να προστατευτούν[13]. Επίσης, υπάρχει ο μη κερδοσκοπικός οργανισμός NTEN (Non profit Technology Enterprise Network), ο οποίος επίσης παρέχει τεχνολογική υποστήριξη σε μη κερδοσκοπικούς οργανισμούς.[14] Τέλος, το NIST Cybersecurity Framework μπορεί να χρησιμοποιηθεί από τον Μ.Κ.Ο. ώστε να αποκτήσει μεγαλύτερη ανθεκτικότητα στον κυβερνοχώρο, καθώς αποτελείται από ένα σύνολο προτύπων της βιομηχανίας και βέλτιστων πρακτικών που βοηθούν τους οργανισμούς να διαχειρίζονται τους κινδύνους με έναν οικονομικά αποδοτικό τρόπο ανάλογα με τις επιχειρηματικές τους ανάγκες.[15]

3. ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΒΑΛΛΟΝΤΟΣ - ΧΟΝΓΚ ΚΟΝΓΚ

3.1 Εισαγωγικά Στοιχεία

Το Χονγκ Κονγκ ως Ειδική Διοικητική Περιοχή της Λαϊκής Δημοκρατίας της Κίνας (Λ.Δ.Κ.) διαθέτει τον υψηλότερο βαθμό αυτονομίας από την ηπειρωτική χώρα (mainland) και επιτρέπεται να διατηρεί το δικό του οικονομικό και πολιτικό σύστημα υπό το υπόδειγμα «Μια χώρα, Δύο συστήματα»[16] (Leung, et al., 2021). Ωστόσο παρατηρείται σταδιακά μια εντατική προσπάθεια μετατόπισης στο υπόδειγμα «Μια χώρα, Ένα σύστημα», δηλαδή την προσαρμογή του συστήματος του Χονγκ Κονγκ σε αυτό της ηπειρωτικής χώρας, που είχε ήδη ξεκινήσει με τον σχεδιασμό και στη συνέχεια την υιοθέτηση του Βασικού Νόμου (Basic Law). Εκείνος θεσπίστηκε από το Εθνικό Λαϊκό Κογκρέσο, το οποίο είναι και καθόλα υπεύθυνο μαζί με την Μόνιμη Επιτροπή του, για την αναθεώρηση των παραρτημάτων του (Gittings, 2013)[17].

3.2 Περιβάλλον δράσης των Μ.Κ.Ο.

Σε αντίθεση με τις Η.Π.Α., η ασταθής πολιτική κατάσταση που επικρατεί στο Χονγκ Κονγκ μπορεί να χαρακτηριστεί ως εχθρική προς τις ακτιβιστικές ομάδες και οργανώσεις. Οι κάτοικοι του Χονγκ Κονγκ έχουν περισσότερα κατοχυρωμένα δικαιώματα και ελευθερίες από τους κατοίκους της ηπειρωτικής χώρας (όπως ελευθερία του λόγου και του τύπου και το δικαίωμα του συνέρχεσθαι και συνεταιρίζεσθαι), εντούτοις παρατηρείται μια σταδιακή υπονόμευση αυτών από την Κυβέρνηση της Κίνας μέσω της θέσπισης νόμων για την διαφύλαξη των συμφερόντων της χώρας. Παράδειγμα αποτελεί ο Νόμος περί Εθνικής Ασφάλειας (National Security

[13] https://www.councilofnonprofits.org/
[14] https://www.nten.org/
[15] https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework
[16] https://www.britannica.com/place/Hong-Kong/Government-and-society

[17]https://books.google.gr/books?hl=el&lr=&id=R5mXSCQXHysC&oi=fnd&pg=PR5&dq=hong+kong+basic+law&ots=HrgbVoUvR6&sig=Oly2xo1rv74b-ABhChY0uqpzB0A&redir_esc=y#v=onepage&q=hong%20kong%20basic%20law&f=false

Law 2020), ο οποίος ήταν η αφορμή αρκετές ανθρωπιστικές οργανώσεις να σταματήσουν τις δραστηριότητές τους στο Χονγκ Κονγκ λόγω φόβων δίωξης από την κεντρική κυβέρνηση (Amnesty International, 2021)[18]. Ταυτόχρονα έχουν αναφερθεί περιστατικά όπου οι κάτοικοι της περιοχής δεν μπορούσαν να προσπελάσουν ιστοσελίδες φιλοδημοκρατικού ή και ακτιβιστικού περιεχομένου καθώς αυτές είχαν αποκλειστεί από τους παρόχους υπηρεσιών (Pomfret and Kwok, 2022)[19].

3.3 Εύρος της απειλής

Η πολιτική αστάθεια που επικρατεί στην περιοχή καθιστά δύσκολη την εξαγωγή ενός βέβαιου και καθολικά ορθού συμπεράσματος. Σύμφωνα με τα τελευταία στατιστικά της Ομάδας Έκτακτης Ανταπόκρισης του Χονγκ Κονγκ (HKCERT), τη περίοδο 2020 Q4 – 2021 Q3 υπήρξε μια ραγδαία μείωση των καταγεγραμμένων περιστατικών κυβερνοασφάλειας σε σχέση με τη περίοδο 2020 Q3 – 2019 Q4, από 17.919 σε 4.079. Από τα 4.079, μόλις τα 10 συνδέονται με επιθέσεις ιομορφικού λογισμικού, σε αντίθεση με το προηγούμενο έτος, όπου παρατηρήθηκαν 11.898 περιστατικά (HKCERT, 2019; 2020; 2021)[20]. Αντίστοιχα αποτελέσματα κατεγράφησαν σε έρευνα που πραγματοποίησε η Microsoft (2019)[21], ενώ η πιο διαδεδομένη μορφή ιομορφικού λογισμικού την ίδια περίοδο, σύμφωνα με την εταιρία PWC (2020) ήταν το λυτρισμικό[22]. Οι επιθέσεις αυτές μπορεί να μην έχουν πάντα στόχο την διατάραξη των δραστηριοτήτων του οργανισμού, αλλά την παρακολούθησή του με σκοπό τη συλλογή πληροφοριών για τους εργαζομένους και την δράση του.

Θεωρούμε ότι τα ανωτέρω νούμερα δεν θα πρέπει απαραίτητα να θεωρηθούν καθησυχαστικά, διότι η αύξηση των κρουσμάτων μπορεί να αποδοθεί εν μέρει στις κοινωνικές αναταραχές, όπως αυτές που προξένησε στα τέλη Μαρτίου του 2019 η πρόταση ψήφισης του νομοσχεδίου σχετικά με τη Φυγή Εγκληματιών και την Νομοθεσία για Αμοιβαία Νομική Υποστήριξη σε Θέματα Ποινικού Δικαίου (Fugitive Offenders and Mutual Legal Assistance in Criminal Matters Legislation (Amendment) Bill 2019)[23]. Παράδειγμα αυτού αποτελεί η κατανεμημένη επίθεση άρνησης υπηρεσιών (DDoS) εναντίων της εφαρμογής ανταλλαγής μηνυμάτων «Telegram», την οποία χρησιμοποιεί πληθώρα ακτιβιστών και διαδηλωτών στο Χονγκ Κονγκ λόγω της υποστήριξης κρυπτογράφησης από άκρο σε άκρο (end-to-end encryption)[24](Urman, Chun-ting Ho and Katz, 2020). Η επίθεση σύμφωνα με αναλυτές σκόπευε να περιορίσει τους τρόπους επικοινωνίας των ομάδων αυτών, αλλά και να τις οδηγήσει στην εύρεση διαφορετικών, λιγότερο ασφαλών λύσεων. Ένα πιο πρόσφατο παράδειγμα αποτελεί η

[18] https://www.amnesty.org/en/latest/news/2021/10/amnesty-international-to-close-its-hong-kong-offices/
[19] https://www.reuters.com/world/china/hong-kong-rights-group-says-website-not-accessible-through-some-networks-2022-02-15/
[20] https://www.hkcert.org/watch-report
[21] https://news.microsoft.com/wp-content/uploads/prod/sites/570/2020/02/Microsoft-Security-Endpoint-Threat-Summary-2019-Updated.pdf
[22] https://www.pwchk.com/en/issues/cybersecurity-and-privacy/cyber-threats-to-hk-an-incident-response-rerspective.html
[23] https://www.legco.gov.hk/yr18-19/english/bills/b201903291.pdf
[24] https://osf.io/preprints/socarxiv/ueds4/

ανακάλυψη μιας νέας ευπάθειας τον Αύγουστο του 2021 από ερευνητές της Ομάδας Ανάλυσης Απειλών της Google (Threat Analysis Group - TAG) (2021), που στοχοποιούσε ακτιβιστές στο Χονγκ Κονγκ μέσω κακόβουλων ιστοσελίδων με φιλοδημοκρατικό περιεχόμενο[25] και οι οποίες επέτρεπαν την εγκατάσταση ιομορφικού λογισμικού σε συσκευές με λειτουργικά MacOS και iOS[26] (M. Léveillé and Cherepanov, 2022). Οι ίδιοι ερευνητές υποθέτουν πως η επίθεση προήλθε από παράγοντες που δρούσαν εκ μέρους της Λ.Δ.Κ., λόγω του τρόπου με τον οποίο διεξάχθηκε.

Ένας τέτοιος state actor πιστεύεται από ερευνητές πως είναι η ομάδα BRONZE PRESIDENT, η οποία στα μέσα του 2018 παρατηρήθηκε να επιτίθεται με ιομορφικό λογισμικό σε M.K.O. με σκοπό την παρακολούθησή τους και την υποκλοπή σημαντικών αρχείων τους[27] (Counter Threat Unit Research Team, 2019).

Από τα ανωτέρω συμπεραίνουμε πως ο κίνδυνος των επιθέσεων ιομορφικού λογισμικού εναντίον του οργανισμού είναι αυξημένος, ιδιαίτερα σε περιόδους έντονων κοινωνικοπολιτικών συγκρούσεων (κατά τις οποίες πληθαίνουν οι επιθέσεις). Αυτό οφείλεται καταρχάς στην ίδια την πολιτική κατάσταση που επικρατεί αυτή τη στιγμή στην περιοχή και κατά δεύτερον στη φύση του οργανισμού, που τον καθιστά στόχο επιθέσεων που έχουν πολιτικά κίνητρα. Κατ' επέκταση, τα μέτρα που προτείνουμε στη συνέχεια ελήφθησαν με γνώμονα τη χειρότερη περίπτωση, λαμβάνοντας υπόψιν και το ενδεχόμενο μιας μελλοντικής αναζωπύρωσης των πολιτικών συγκρούσεων που θα οδηγήσει σε εκ νέου αύξηση των επιθέσεων.

Περιστατικό Ασφάλειας	**2019 Q2**	**2019 Q3**	**2019 Q4**	**2020 Q1**	**2020 Q2**	**2020 Q3**	**2020 Q4**	**2021 Q1**	**2021 Q2**	**2021 Q3**
Βανδαλισμός ιστοσελίδων	532	1120	591	572	1062	571	305	295	476	445
Phising	1306	849	257	399	2017	552	395	495	665	993
Φιλοξενία Ιομορφικού λογισμικού	48892	17273	1185	5.445	4334	934	2	0	8	0
Σύνολο	50730	19242	2033	6416	7413	2057	702	790	1149	1438

Πίνακας 3 Περιστατικά ασφαλείας ανά τρίμηνο σύμφωνα με το HKCERT για το 2019, 2020 και 2021

[25] https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/
[26] https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/
[27] https://www.secureworks.com/research/bronze-president-targets-ngos

3.4 Περιορισμοί

Για την δραστηριοποίηση του οργανισμού στο Χονγκ Κονγκ, πρέπει να ληφθούν υπόψιν οι περιορισμοί που επιφέρει το περιβάλλον και οι νόμοι της περιοχής σχετικά με την προστασία των προσωπικών δεδομένων και την αντιμετώπιση του ιομορφικού λογισμικού.

Αρχικά το Διάταγμα περί Ιδιωτικότητας των Προσωπικών Δεδομένων (Personal Data (Privacy) (Amendment) Ordinance 2021 - PDPO) ορίζει τις αρχές που θα πρέπει να διέπουν την επεξεργασία των προσωπικών δεδομένων ενός υποκειμένου. Τα περιεχόμενα του είναι σε μεγάλο βαθμό όμοια με τον αντίστοιχο ευρωπαϊκό κανονισμό (ΓΚΠΔ) και αναφέρει μεταξύ άλλων ότι τα υποκείμενα των δεδομένων πρέπει να δώσουν τη συγκατάθεσή τους για την επεξεργασία των δεδομένων τους για έναν συγκεκριμένο σκοπό, ενώ αντίστοιχα ο εκτελών την επεξεργασία πρέπει να λάβει τα απαραίτητα οργανωτικά και λειτουργικά μέτρα για την προστασία της ασφάλειας των δεδομένων αυτών[28]. Στην ενότητα 33 του ίδιου νόμου (που δεν έχει τεθεί ακόμα σε εφαρμογή), αναφέρεται πως σε περίπτωση μεταβίβασης των δεδομένων σε κάποια περιοχή εκτός του Χονγκ Κονγκ πρέπει να ισχύει κάποια αντίστοιχη νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα[29].

Συνεχίζοντας, ο Νόμος περί Εθνικής Ασφάλειας ορίζει ότι είναι υποχρέωση της Ε.Δ.Π. του Χονγκ Κονγκ (HKSAR) να προστατεύει την εθνική ασφάλεια της χώρας και να «αποτρέπει, καταστέλλει και να επιβάλλει ποινές για κάθε πράξη ή δραστηριότητα που θέτει σε κίνδυνο την εθνική ασφάλεια»[30]. Παρότι στο κείμενο ορίζεται ότι θα πρέπει να προστατεύονται τα ανθρώπινα δικαιώματα που διαφυλάσσονται και με τον Βασικό Νόμο, τμήματα αυτού είναι ασαφώς διατυπωμένα ως προς το «τι» μπορεί να θεωρηθεί κίνδυνος για την εθνική ασφάλεια της Λ.Δ.Κ. με αποτέλεσμα την ποινικοποίηση δράσεων που αντιτίθενται στην κυβέρνηση και προωθούν την ανεξαρτητοποίηση του Χονγκ Κονγκ.

Ένα σημαντικό σημείο που επηρεάζει τις δραστηριότητες του οργανισμού στην περιοχή είναι το γεγονός ότι οι αρχές μπορούν να αφαιρούν διαδικτυακό περιεχόμενο που κρίνουν ότι παραβιάζει τον νόμο καθώς και να αποκτούν πρόσβαση σε δεδομένα χρηστών χωρίς την έκδοση εντάλματος (Amnesty International, 2020)[31].

3.5 Δυνατότητες και τρόποι αντιμετώπισης

Οι νόμοι που διαθέτει το Χονγκ Κονγκ σχετικά με την ασφάλεια πληροφοριακών συστημάτων, στους οποίους ορίζονται οι ποινές για τα εγκλήματα που σχετίζονται με αυτά, αλλά και οι τρόποι αντιμετώπισης και προστασίας από κυβερνοεπιθέσεις (The

[28] https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html
[29] https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf
[30] https://www.elegislation.gov.hk/doc/hk/a406/eng_translation_(a406)_en.pdf
[31] https://www.amnesty.org/en/latest/news/2020/07/hong-kong-national-security-law-10-things-you-need-to-know/

Hong Kong University of Science and Technology, n.d.)[32], παρουσιάζονται στον παρακάτω πίνακα.

Νόμος
Διάταγμα περί Ιδιωτικότητας των Προσωπικών Δεδομένων - PDPO
Διάταγμα περί Υποκλοπής των Τηλεπικοινωνιών και Παρακολούθησης (Ενότητα 27Α)
Διάταγμα περί Εγκλημάτων (Ενότητες 59 και 161)
Διάταγμα περί Κλοπής (Ενότητες 9, 11 και 23)

Πίνακας 4 Νόμοι περί Ασφάλειας Πληροφοριακών Συστημάτων στο Χονγκ Κονγκ σύμφωνα με το HKUST

Δεν επιβάλλεται κανένας περιορισμός ως προς τα μέτρα προστασίας που μπορεί να λάβει ο οργανισμός, όσο αυτά είναι σύμφωνα με τους ανωτέρω νόμους και δεν αποτελούν παράβαση των δικαιωμάτων των υποκειμένων όπως αυτά ορίζονται στο Βασικό Νόμο και το PDPO (Bower, Cheung, Chan and Huang, 2021)[33].

Πληροφορούμαστε επίσης πως σε περίπτωση ανίχνευσης κάποιου περιστατικού μόλυνσης από ιομορφικό λογισμικό, δεν υπάρχει νομική υποχρέωση αναφοράς του στις αρχές, ακόμα και αν θέτονται σε κίνδυνο προσωπικά δεδομένα. Συνίσταται παρ' όλα αυτά ο οργανισμός να ακολουθήσει τις Οδηγίες Χειρισμού Παραβίασης Δεδομένων (Data Breach Guidance) (Privacy Commissioner for Personal Data, 2019)[34], βάσει των οποίων θα πρέπει να συλλέξει πληροφορίες σχετικά με την παραβίαση.

4. ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

[32] https://itsc.hkust.edu.hk/it-policies-guidelines/related-laws
[33] https://www.allenovery.com/germany/-/media/allenovery/2_documents/news_and_insights/publications/2021/06/a_guide_to_hong_kongs_cyber_security_laws_and_practices_june_2021.pdf
[34] https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

Από την έρευνα που πραγματοποιήσαμε, υπάρχουν ορισμένες συμβουλές και μέτρα τα οποία θεωρούμε ότι ισχύουν από κοινού και στις δύο νέες χώρες που θέλει να δραστηριοποιηθεί ο οργανισμός. Αυτά είναι τα εξής:

- Σωστή και πλήρης εκπαίδευση των εργαζομένων πάνω σε θέματα κυβερνοασφάλειας για αποφυγή επιθέσεων social engineering και phising, που αποτελούν ίσως το πιο διαδεδομένο τρόπο επίθεσης (attack vector).

- Τακτική ενημέρωση του λογισμικού που χρησιμοποιεί ο οργανισμός, καθώς, πολλές επιθέσεις με ιομορφικό λογισμικό εκμεταλλεύονται ευπάθειες που δεν έχουν διορθωθεί.

- Χρήση λογισμικού antivirus και τείχους προστασίας (firewall).

- Αποφυγή λήψης αρχείων και προγραμμάτων όταν το περιεχόμενο τους δεν μπορεί να θεωρηθεί έμπιστο και ασφαλές.

- Τήρηση αντιγράφων ασφαλείας με σκοπό την προστασία της διαθεσιμότητας των δεδομένων (φερειπείν σε περίπτωση μόλυνσης από λυτρισμικό).

4.1 Συμβουλές για τη δραστηριοποίηση στις Η.Π.Α.

Σε γενικές γραμμές η μελέτη μας έδειξε πως το περιβάλλον των Η.Π.Α. παρουσιάζει αρκετές ομοιότητες με την Ε.Ε., όπου δραστηριοποιείται ήδη ο οργανισμός, όσον αφορά τις επιθέσεις ιομορφικού λογισμικού που δέχονται οι Μ.Κ.Ο., οι εταιρίες και οι κυβερνητικοί οργανισμοί σε ένα δεδομένο χρονικό διάστημα, αλλά και αναφορικά με την κοινωνικοπολιτική κατάσταση που επικρατεί στις δύο περιοχές.

Η μεγαλύτερη απειλή στις Η.Π.Α., με βάση τα δεδομένα που παρουσιάστηκαν στην ενότητα 2.2, φαίνεται πως είναι το λυτρισμικό, καθώς ο οργανισμός κινδυνεύει όχι μόνο λόγω των επιθέσεων εναντίον στόχων υψηλού προφίλ, οι οποίες δύναται να τον επηρεάσουν άμεσα, αλλά και επειδή υπάρχουν επιτιθέμενοι που στοχεύουν απευθείας τους Μ.Κ.Ο. με λυτρισμικό, ελπίζοντας να λάβουν ένα μέρος του χρηματικού ποσού που διαθέτουν από δωρεές και άλλες πηγές χρηματοδότησης. Καταλήγουμε στο συμπέρασμα πως ο κίνδυνος που διατρέχει από τη συγκεκριμένη απειλή δεν είναι απαραίτητα υψηλότερος από εκείνον που ήδη αντιμετωπίζει, συνεπώς ο οργανισμός δεν χρειάζεται να μεταβάλει σε σημαντικό βαθμό την πολιτική κυβερνοασφάλειας που ακολουθεί ήδη, αλλά θα χρειαστεί να λάβει ιδιαίτερη μέριμνα για την αντιμετώπιση των επιθέσεων τέτοιου είδους.

Τέλος, τα δεδομένα που διαχειρίζεται ο οργανισμός μπορεί να είναι ιδιαίτερα ευαίσθητα γι’ αυτό και η τυχόν διαρροή τους ύστερα από μια επίθεση ιομορφικού λογισμικού θα επέφερε σοβαρές συνέπειες τόσο στους ανθρώπους των οποίων τα δεδομένα διέρρευσαν, όσο και στον ίδιο τον οργανισμό. Έτσι λοιπόν, με βάση στοιχεία που υποστηρίζονται και από το National Council of Nonprofits προτείνουμε στον

οργανισμό να υλοποιήσει τα ακόλουθα μέτρα, τα οποία θα τον βοηθήσουν να προστατεύσει τα δεδομένα που αποθηκεύει και επεξεργάζεται.[35]

1. Όπως συμβουλεύει και ο οργανισμός NTEN, θα πρέπει να πραγματοποιήσει ένα είδος Ελέγχου Επικινδυνότητας (Risk Assessment). Πιο συγκεκριμένα, να απαντηθούν ερωτήσεις σχετικά με το τι είδους δεδομένα είναι, που βρίσκονται και πόσο ευαίσθητα θεωρούνται (Rivas, 2016).[36]

2. Το συμβούλιο προτρέπει επίσης τους οργανισμούς να γνωρίζουν αν τα δεδομένα που συλλέγουν και διατηρούν καλύπτονται από ομοσπονδιακούς ή πολιτειακούς κανονισμούς ως ”στοιχεία προσωπικής ταυτοποίησης”.

3. Να κάνει χρήση του NIST Cybersecurity Framework.

4. Να κρυπτογραφεί τις βάσεις δεδομένων προκειμένου να προστατεύσει την εμπιστευτικότητα των δεδομένων σε περίπτωση επίθεσης με ιομορφικό λογισμικό.

4.2 Συμβουλές για τη δραστηριοποίηση στο Χονγκ Κονγκ

Όπως προαναφέρθηκε, η επ’ αριθμόν ένα απειλή στο Χονγκ Κονγκ για τις Μ.Κ.Ο. και τις ακτιβιστικές ομάδες είναι οι κυβερνοεπιθέσεις πολιτικών οργανώσεων και παραγόντων που δρουν προς όφελος κάποιας κυβέρνησης προκειμένου να αλλοιώσουν, να υποκλέψουν ή να καταστρέψουν τα δεδομένα του οργανισμού και να εμποδίσουν την πρόσβαση στο περιεχόμενο που κάνει διαθέσιμο στο κοινό. Θεωρούμε πως ο αντίκτυπος που ενδεχομένως να έχει μια επιτυχής επίθεση θα είναι επίσης αυξημένος, διότι εκείνη δύναται να προέρχεται από state actors οι οποίοι διαθέτουν μεγάλη τεχνογνωσία και περισσότερους πόρους που μπορούν να αξιοποιήσουν για να πλήξουν τον στόχο τους.

Τα μέτρα που προτείνουμε να λάβει ο οργανισμός σε τεχνολογικό και κοινωνικό επίπεδο είναι τα εξής:

1. Κρίνουμε πως η κρυπτογράφηση των βάσεων δεδομένων θα πρέπει να εφαρμοστεί οπωσδήποτε σε συνδυασμό με το αμέσως επόμενο μέτρο, επειδή σε κάθε άλλη περίπτωση οι αρχές μπορούν να απαιτήσουν την παράδοση των αποκρυπτογραφημένων δεδομένων των χρηστών ανά πάσα στιγμή (βάσει του Νόμου Εθνικής Ασφάλειας), πράγμα που παραβιάζει την αρχή της εμπιστευτικότητας και καθιστά το μέτρο ανούσιο.

2. Μεταφορά των διακομιστών του οργανισμού σε χώρα εκτός του Χονγκ Κονγκ με σκοπό την παράκαμψη του Νόμου Εθνικής Ασφάλειας. Τονίζουμε ότι θα

[35] https://www.councilofnonprofits.org/tools-resources/cybersecurity-nonprofits
[36] https://www.nten.org/article/assessing-risk-protect-valuable-data/

πρέπει να υπάρχει στη χώρα προορισμού κάποια νομοθεσία αντίστοιχη του PDPO και για τον λόγο αυτό προτείνουμε κάποιο κράτος μέλος της Ε.Ε. όπου ήδη είναι σε εφαρμογή ο GDPR. Αναφέρουμε επίσης πως η εφαρμογή αυτού του μέτρου μπορεί, με μεγάλη πιθανότητα, να επιφέρει μπλοκάρισμα του περιεχομένου για τους κατοίκους εντός του Χονγκ Κονγκ.

3. Χρήση ειδικού δικτυακού εξοπλισμού ή υπηρεσιών για την μετρίαση του αντικτύπου μιας επίθεσης DDoS, η οποία όπως έγινε σαφές αποτελεί κίνδυνο για τον οργανισμό, αφού αποτρέπει τους χρήστες από την προσπέλαση του διαδικτυακού περιεχομένου του και μπορεί στη χειρότερη περίπτωση να επηρεάσει ολόκληρη τη λειτουργία του.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Amnesty International, 2020. *Hong Kong's national security law: 10 things you need to know.* [Ηλεκτρονικό]
Available at: https://www.amnesty.org/en/latest/news/2020/07/hong-kong-national-security-law-10-things-you-need-to-know/
[Πρόσβαση 5 4 2022].

Amnesty International, 2021. *Amnesty International to close its Hong Kong offices.* [Ηλεκτρονικό]
Available at: https://www.amnesty.org/en/latest/news/2021/10/amnesty-international-to-close-its-hong-kong-offices/
[Πρόσβαση 3 4 2022].

ΟΔΗΓΊΑ 2013/40/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ, 2013 [Ηλεκτρονικό]
Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32013L0040
[Πρόσβαση 27 3 2022].

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ, 2016 [Ηλεκτρονικό]
Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434
[Πρόσβαση 3 4 2022].

Fugitive Offenders and Mutual Legal Assistance in Criminal Matters Legislation (Amendment) Bill 2019*, 2019* [pdf]
Available at: https://www.legco.gov.hk/yr18-19/english/bills/b201903291.pdf

[Πρόσβαση 12 4 2022]

Guidance on Data Breach Handling and the Giving of Breach Notifications [pdf]
Available at:
https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHand

ling2015_e.pdf
[Πρόσβαση 15 4 2022].

The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region, 2020 [Ηλεκτρονικό].

Available at:
https://www.elegislation.gov.hk/doc/hk/a406/eng_translation_(a406)_en.pdf

[Πρόσβαση 5 4 2022]

Bower, M., Cheung, F. H., Chan, K. & Huang, J., 2021. *A guide to Hong Kong's cyber security laws and practices.* [Ηλεκτρονικό]
Available at: https://www.allenovery.com/germany/-/media/allenovery/2_documents/news_and_insights/publications/2021/06/a_guide_to_hong_kongs_cyber_security_laws_and_practices_june_2021.pdf
[Πρόσβαση 9 4 2022].

Bureau of Democracy, Human Rights, and Labor, 2021. *Non-Governmental Organizations (NGOs) in the United States.* [Ηλεκτρονικό]
Available at: https://www.state.gov/non-governmental-organizations-ngos-in-the-united-states/
[Πρόσβαση 8 4 2022].

Center for Strategic and International Studies (CSIS), 2022. *Significant Cyber Incidents Since 2006.* [Ηλεκτρονικό]
Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/220404_Significant_Cyber_Incidents.pdf?6baqc92oMg0w.0wCwZLP6OATs9MmMmLG
[Πρόσβαση 15 4 2022].

Counter Threat Unit Research Team , 2019. *BRONE PRESIDENT Targets NGOs.* [Ηλεκτρονικό]
Available at: https://www.secureworks.com/research/bronze-president-targets-ngos
[Πρόσβαση 14 4 2022].

Duguin, S., 2022. *Cyberattacks: a real threat to NGOs and nonprofits.* [Ηλεκτρονικό]
Available at: https://reliefweb.int/report/world/cyberattacks-real-threat-ngos-and-nonprofits
[Πρόσβαση 7 4 2022].

ENISA, n.d. [Ηλεκτρονικό]
Available at: https://www.enisa.europa.eu/topics/nis-directive?tab=details
[Πρόσβαση 27 3 2022].

Gittings, D., 2013. *Introduction to the Hong Kong Basic Law.* [e-book]
Available at:
https://books.google.gr/books?hl=el&lr=&id=R5mXSCQXHysC&oi=fnd&pg=PR5&dq=hong+kong+basic+law&ots=HrgbVoUvR6&sig=Oly2xo1rv74b-ABhChY0uqpzB0A&redir_esc=y#v=onepage&q=hong%20kong%20basic%20law&f

=false
[Πρόσβαση 25 3 2022].

Google, 2021. *Analyzing a watering hole campaign using macOS exploits.* [Ηλεκτρονικό]
Available at: https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/
[Πρόσβαση 3 4 2022].

Hong Kong Computer Emergency Response Team, 2019-2021. *HK Security Watch Report.* [Ηλεκτρονικό]
Available at: https://www.hkcert.org/watch-report

Hong Kong University of Science and Technology, n.d. *Laws Related to Misuse of Computer and Data Privacy.* [Ηλεκτρονικό]
Available at: https://itsc.hkust.edu.hk/it-policies-guidelines/related-laws
[Πρόσβαση 15 4 2022].

Leung, C.-K., 2021. *Hong Kong.* [Ηλεκτρονικό]
Available at: https://www.britannica.com/place/Hong-Kong/Government-and-society
[Πρόσβαση 22 3 2022].

M.Léveillé, M.-E. & Cherepanov, A., 2022. *Watering hole deploys new macOS malware, DazzleSpy, in Asia.* [Ηλεκτρονικό]
Available at: https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/
[Πρόσβαση 3 4 2022].

Microsoft Corporation, 2017. *Nonprofit Guidelines for Cybersecurity and Privacy.* [pdf]
Available at:
https://www.councilofnonprofits.org/sites/default/files/documents/nonprofit-guidelines-for-cybersecurity-and-privacy.pdf
[Πρόσβαση 10 4 2022].

Microsoft Corporation, 2020. *Microsoft Security Endpoint Threat Summary 2019.* [pdf]
Available at: https://news.microsoft.com/wp-content/uploads/prod/sites/570/2020/02/Microsoft-Security-Endpoint-Threat-Summary-2019-Updated.pdf
[Πρόσβαση 8 4 2022].

Mierzwa, S. & Scott, J., 2017. *Cybersecurity in Non-Profit and Non-Governmental Organizations.* [Ηλεκτρονικό]
Available at:
https://www.researchgate.net/publication/314096686_Cybersecurity_in_Non-Profit_and_Non-Governmental_Organizations
[Πρόσβαση 12 4 2022].

National Conference of State legislature, 2022. *State Laws Related to Digital Privacy.* [Ηλεκτρονικό]

Available at: https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx
[Πρόσβαση 9 4 2022].

National Council for Nonprofits, n.d. *Cybersecurity for Nonprofits.* [Ηλεκτρονικό]
Available at: https://www.councilofnonprofits.org/tools-resources/cybersecurity-nonprofits
[Πρόσβαση 12 4 2022].

National Insitute of Standards and Technology (NIST), 2017. *NIST Releases Update to Cybersecurity Framework.* [Ηλεκτρονικό]
Available at: https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework
[Πρόσβαση 15 4 2022].

Pomfret, J. & Kwok, D., 2022. *Hong Kong rights group says website not accessible through some networks.* [Ηλεκτρονικό]
Available at: https://www.reuters.com/world/china/hong-kong-rights-group-says-website-not-accessible-through-some-networks-2022-02-15/Jam
[Πρόσβαση 16 4 2022].

Privacy Commissioner for Personal Data, n.d. *The Personal Data (Privacy) Ordinance.* [Ηλεκτρονικό]
Available at:
https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html
[Πρόσβαση 7 4 2022].

PWC, 2020. *Cyber threats to Hong Kong: An incident response perspective.* [Ηλεκτρονικό]
Available at: https://www.pwchk.com/en/issues/cybersecurity-and-privacy/cyber-threats-to-hk-an-incident-response-rerspective.html
[Πρόσβαση 14 4 2022].

Rivas, D., 2016. *Assessing risk: How to protect your most valuable data.* [Ηλεκτρονικό]
Available at: https://www.nten.org/article/assessing-risk-protect-valuable-data/
[Πρόσβαση 14 4 2022].

Shavell, R., 2021. *It's time for NGOs and nonprofits to tighten their cybersecurity standards.* [Ηλεκτρονικό]
Available at: https://philanthropynewsdigest.org/features/the-sustainable-nonprofit/it-s-time-for-ngos-and-nonprofits-to-tighten-their-cybersecurity-standards
[Πρόσβαση 9 4 2022].

Touro College Illinois, 2021. *The 10 Biggest Ransomware Attacks of 2021.* [Ηλεκτρονικό]
Available at: https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php
[Πρόσβαση 7 4 2022].

Urman, A., Ho, J. C.-T. & Katz, S., 2020. *No Central Stage: Telegram-based activity during the 2019 protests in Hong Kong. [pdf]*

Available at: https://osf.io/preprints/socarxiv/ueds4/

[Πρόσβαση 6 4 2022]

Willett, M., 2021. Lessons of the SolarWinds Hack. *Survival*, 23(2), pp. 7-26.