ΕΝΣΩΜΑΤΩΣΗ ΤΗΣ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΥΓΕΙΑΣ ΣΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Σύνοψη

Το παρόν έγγραφο αναλύει μια νέα οπτική, διερευνώντας τη σχέση μεταξύ των απειλών για την κυβερνοασφάλεια και της υγείας και ασφάλειας των εργαζομένων. Αυτό απαιτεί υπέρβαση της παραδοσιακής θεώρησης της κυβερνοασφάλειας, που εστιάζει μόνο στις τεχνικές πτυχές, και επέκταση του προβληματισμού στις ανθρώπινες και κοινωνικές συνέπειες των κυβερνοεπιθέσεων.

Λαμβάνοντας υπόψη την αυξανόμενη χρήση της ψηφιακής τεχνολογίας σε όλους τους οργανισμούς και της αύξησης των επιθέσεων κατά των συστημάτων υπολογιστών και των δικτύων τους, πρέπει να εξεταστούν οι νέοι αναδυόμενοι κίνδυνοι για την υγεία και την ασφάλεια των εργαζομένων. Η επαγγελματική ασφάλεια και υγεία (ΕΑΥ) πρέπει να αντιμετωπίσει νέες ανάγκες και προκλήσεις τα επόμενα χρόνια.

Το σενάριο της κυβερνοασφάλειας

Τα τελευταία χρόνια, η ασφάλεια στον κυβερνοχώρο έχει αναδειχθεί σε φλέγον θέμα για όλες τις επιχειρήσεις και σε όλους τους κλάδους οικονομικής δραστηριότητας. Το έγκλημα στον κυβερνοχώρο καθίσταται ολοένα και πιο εξελιγμένο, και οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται τις κάθε είδους τρωτότητες για να πραγματοποιήσουν τις επιθέσεις τους, είτε φυσικές είτε τεχνικές, είτε ανθρώπινες.

Το λεξικό του Cambridge ορίζει την κυβερνοεπίθεση ως «παράνομη απόπειρα πρόκλησης ζημίας σε ένα σύστημα υπολογιστή ή στις πληροφορίες που περιέχονται σε αυτό, με χρήση του διαδικτύου»[1]. Ειδικότερα, σύμφωνα με το NIST (Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ), κυβερνοεπίθεση είναι «μια επίθεση, μέσω του κυβερνοχώρου, η οποία στοχεύει στη χρήση του κυβερνοχώρου από μια επιχείρηση με σκοπό τη διατάραξη, την απενεργοποίηση, την καταστροφή, ή τον κακόβουλο έλεγχο ενός υπολογιστικού περιβάλλοντος/υποδομής ή την καταστροφή της ακεραιότητας των δεδομένων ή την κλοπή ελεγχόμενων πληροφοριών»[2].

Σε έναν ολοένα και περισσότερο ψηφιακό κόσμο, κάθε επιχείρηση κινδυνεύει να δεχθεί κυβερνοεπίθεση. Ειδικότερα, το 2020 αποτέλεσε ορόσημο τόσο για τα ζητήματα ψηφιακής μετάβασης όσο και κυβερνοασφάλειας. Οι επιχειρήσεις έχουν αυξήσει την εφαρμογή οργανωτικών προσεγγίσεων που βασίζονται στην ευελιξία και την αξιοποίηση της τεχνολογίας για εξ αποστάσεως εργασία, κυρίως λόγω της πανδημίας COVID-19, αλλά αυτό έχει αποτελέσει επίσης πρόσφορο έδαφος για τους εγκληματίες του κυβερνοχώρου, σε σημείο που 78 % των οργανισμών έχουν αντιμετωπίσει αυξημένο όγκο κυβερνοεπιθέσεων λόγω της μεταστροφής προς την εξ αποστάσεως εργασία[3].

Παγκοσμίως, το 87 % των οργανισμών έχουν υποστεί απόπειρα εκμετάλλευσης μιας υπάρχουσας τρωτότητας, ενώ το 71 % των επαγγελματιών του τομέα της ασφάλειας έχουν αναφέρει αύξηση των απειλών για την κυβερνοασφάλεια (ηλεκτρονικό ψάρεμα/phishing, κακόβουλο λογισμικό/malware, λυτρισμικό λογισμικό/ransomware για την απαίτηση πληρωμής λύτρων μέσω της κρυπτογράφησης των δεδομένων ή του κλειδώματος του προσωπικού υπολογιστή του θύματος) από τότε που άρχισε η έξαρση της πανδημίας του κορωνοϊού[4].

Γενικά, οι επιθέσεις κατά της κυβερνοασφάλειας εξακολουθούν να αυξάνονται όχι μόνο αριθμητικά, αλλά και όσον αφορά τον αντίκτυπό τους (ENISA, 2021a), ενώ οι χώρες διαθέτουν διαφορετικούς πόρους και εργαλεία για τη διαχείριση της κυβερνοασφάλειας. Για παράδειγμα, με βάση συγκεκριμένους παράγοντες, όπως η δέσμευση ως προς την κυβερνοασφάλεια και τη νομοθεσία,

[1] https://dictionary.cambridge.org/dictionary/english/cyberattack
[2] https://csrc.nist.gov/glossary/term/cyber_attack
[3] https://atlasvpn.com/blog/cyberattack-volume-grew-in-78-of-businesses-globally
[4] https://www.checkpoint.com/pages/cyber-security-report-2021/

τρεις ευρωπαϊκές χώρες (Πορτογαλία, Λιθουανία και Σλοβακία) θεωρείται ότι έχουν τον καλύτερο δείκτη κυβερνοασφάλειας[5].

Το διευρυνόμενο τοπίο απειλών έχει αναδείξει την επείγουσα ανάγκη να εφαρμόσει η Ευρωπαϊκή Επιτροπή μια αποτελεσματική στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία,[6] με σκοπό να διασφαλίσει την ασφαλή ψηφιακή εποχή, βελτιώνοντας την ανθεκτικότητα, αναπτύσσοντας την ικανότητα πρόληψης και αντιμετώπισης των περιστατικών κυβερνοασφάλειας, και καθορίζοντας μια συνεκτική διεθνή πολιτική για τον κυβερνοχώρο. Επιπλέον, αυτή η στρατηγική υπογραμμίζει τη σημασία ενός προγράμματος ευαισθητοποίησης ως προς την κυβερνοασφάλεια για όλα τα θεσμικά και λοιπά όργανα της ΕΕ, προκειμένου να αναπτυχθεί μια αποτελεσματική νοοτροπία κυβερνοασφάλειας.

Τρέχουσες και μελλοντικές απειλές

Το κόστος του εγκλήματος στον κυβερνοχώρο αναμένεται να φτάσει το ποσό των 10,5 τρισεκατομμυρίων USD ετησίως έως το 2025[7] Στην πραγματικότητα, διάφοροι παράγοντες χρησιμοποιούν τον κυβερνοχώρο για κακόβουλους σκοπούς και με διάφορα κίνητρα, από εγκληματίες του κυβερνοχώρου που έχουν ως βασικό κίνητρο το οικονομικό κέρδος, έως τρομοκράτες του κυβερνοχώρου που εμπνέονται από πολιτικούς και ιδεολογικούς σκοπούς. Το πεδίο του εγκλήματος στο διαδίκτυο είναι ιδιαίτερα ευρύ και περιλαμβάνει πολλές παράνομες πράξεις –ήδη γνωστές στον πραγματικό κόσμο– όπως κλοπή ταυτότητας, απάτη, κατασκοπεία, έγκλημα διανοητικής ιδιοκτησίας, καθώς και διάφορες μορφές διαδικτυακής βίας (όπως παρενοχλητική παρακολούθηση ή εκφοβισμός). Αυτές οι πράξεις βασίζονται στα ισχυρά τεχνικά μέσα που παρέχει το ψηφιακό πλαίσιο, και λόγω του ολοένα και περισσότερο διασυνδεδεμένου κόσμου, το κυβερνοέγκλημα αποτελεί έναν από τους σημαντικότερους κινδύνους για τις δύο επόμενες δεκαετίες[8].

Οι απειλές για την κυβερνοασφάλεια αποτελούν υψηλή προτεραιότητα για κάθε οργανισμό και κάθε χώρα λόγω της πολυμορφίας και της σοβαρότητας των συνεπειών: από απώλεια πολύτιμων πληροφοριών έως παράλυση των συστημάτων υπολογιστών και των σχετικών υπηρεσιών, καθώς και σοβαρούς κινδύνους για την υγεία και ασφάλεια των ατόμων.

Παρότι είναι γνωστοί εδώ και χρόνια, ορισμένοι συνήθεις τύποι απειλών για την κυβερνοαφάλεια (πίνακας 1), όπως το ηλεκτρονικό ψάρεμα (phishing) και το λυτρισμικό λογισμικό (ransomware), εξακολουθούν να αυξάνονται[9]. Στην πραγματικότητα, είναι ιδιαίτερα επικερδείς για τους εγκληματίες του κυβερνοχώρου, και το κόστος της εκτέλεσής τους είναι πολύ χαμηλό σε σύγκριση με τον κίνδυνο να συλληφθούν οι επιτιθέμενοι (Hernandez-Castro et al., 2020). Το ηλεκτρονικό ψάρεμα παραμένει μια από τις κύριες τακτικές παραβίασης της ασφάλειας (Verizon, 2021), αλλά οι διάφορες μορφές κυβερνοεπιθέσεων καταδεικνύουν την πολυπλοκότητα του τοπίου των κυβερνοαπειλών. Οι επιθέσεις σε αλυσίδες εφοδιασμού, για παράδειγμα, παρουσιάζουν ανοδική τάση και αποτελούν μείζονα λόγο ανησυχίας για τους οργανισμούς στο μέλλον (ENISA, 2021β)[10].

Πίνακας 1: Ορισμένες από τις συνηθέστερες απειλές για την κυβερνοασφάλεια[11]

Τύπος	Περιγραφή
Ηλεκτρονικό ψάρεμα και στοχευμένο	Το ηλεκτρονικό ψάρεμα (phishing) είναι η πρακτική αποστολής δόλιων μηνυμάτων που φαίνεται να προέρχονται από αξιόπιστη πηγή, συνήθως μέσω ηλεκτρονικού ταχυδρομείου. Στόχος του είναι η κλοπή ευαίσθητων

[5] https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/
[6] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[7] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[8] https://www.weforum.org/agenda/2020/12/3-disruptive-frontier-risks-that-could-strike-by-2040/
[9] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[10] Αλυσίδα εφοδιασμού είναι «ο συνδυασμός του οικοσυστήματος πόρων που χρειάζονται για τον σχεδιασμό, την παραγωγή και τη διανομή ενός προϊόντος». Όσον αφορά την κυβερνοασφάλεια, μια αλυσίδα εφοδιασμού περιλαμβάνει εξοπλισμό και λογισμικό, αποθήκευση σε υπολογιστικό νέφος ή τοπική αποθήκευση, και μηχανισμούς διανομής. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
[11] Αυτές είναι ορισμένες από τις συνηθέστερες απειλές για την κυβερνοασφάλεια σύμφωνα με τον ENISA (2020·2021). Για την περιγραφή των απειλών, βλ. επίσης https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks and https://www.itgovernance.co.uk/cyber-threats

Τύπος	Περιγραφή
ηλεκτρονικό ψάρεμα	δεδομένων, όπως στοιχεία πιστωτικών καρτών και διαπιστευτήρια σύνδεσης, ή η εγκατάσταση κακόβουλου λογισμικού στη συσκευή του θύματος. Υπάρχουν διάφορες μορφές ηλεκτρονικού ψαρέματος, όπως το στοχευμένο ηλεκτρονικό ψάρεμα (spear phishing), μια πιο εξελιγμένη παραλλαγή του ηλεκτρονικού ψαρέματος που στοχεύει σε συγκεκριμένο άτομο ή οργανισμό.
Κακόβουλο λογισμικό και λυτρισμικό λογισμικό	Το κακόβουλο λογισμικό (malware) είναι ένας ευρύς όρος που χρησιμοποιείται για να περιγράψει το λογισμικό κακόβουλης λειτουργίας, όπως κατασκοπευτικό λογισμικό, λυτρισμικό λογισμικό, ιούς και σκουλήκια υπολογιστών. Το λυτρισμικό λογισμικό (ransomware), για παράδειγμα, είναι μια μορφή κακόβουλου λογισμικού που κρυπτογραφεί τις πληροφορίες των θυμάτων και απαιτεί πληρωμή λύτρων ως αντάλλαγμα για το κλειδί αποκρυπτογράφησης. Είναι ένας από τους πιο επικερδείς τύπους κυβερνοεπίθεσης.
Κοινωνική μηχανική	Η κοινωνική μηχανική είναι μια τεχνική που χρησιμοποιείται για την εξαπάτηση και τη χειραγώγηση ατόμων με σκοπό την απόκτηση εμπιστευτικών πληροφοριών ή την εξασφάλιση πρόσβασης στον υπολογιστή τους. Το ηλεκτρονικό ψάρεμα είναι ένα παράδειγμα κοινωνικής μηχανικής.
Άρνηση υπηρεσίας (DoS)	Αυτός ο τύπος επίθεσης πλημμυρίζει τα συστήματα, τους διακομιστές ή τα δίκτυα με τόσο πολλή κίνηση ώστε το σύστημα αδυνατεί να ανταποκριθεί στα νόμιμα αιτήματα. Οι επιτιθέμενοι μπορεί επίσης να χρησιμοποιούν πολλαπλές παραβιασμένες συσκευές για να εξαπολύσουν αυτήν την επίθεση (DDos – κατανεμημένη άρνηση υπηρεσίας)
Παραβίαση δεδομένων	Η παραβίαση δεδομένων είναι ένα περιστατικό κυβερνοασφάλειας κατά το οποίο γίνεται κλοπή πληροφοριών, οι οποίες λαμβάνονται από ένα σύστημα ή χρησιμοποιούνται χωρίς άδεια.
Κυβερνοκατασκοπεία	Ο στόχος των δραστηριοτήτων κυβερνοκατασκοπείας είναι η κλοπή ευαίσθητων ή διαβαθμισμένων δεδομένων ή διανοητικής ιδιοκτησίας για την εξασφάλιση πλεονεκτήματος έναντι μιας ανταγωνιστικής επιχείρησης ή μιας κυβερνητικής οντότητας.
Εκστρατείες παραπληροφόρησης και εσφαλμένης πληροφόρησης	Η παραπληροφόρηση συνίσταται στην εσκεμμένη δημιουργία και κοινοποίηση ψευδών πληροφοριών με σκοπό την πρόκληση ζημίας. Η εσφαλμένη πληροφόρηση συνίσταται στην τυχαία διάδοση ψευδών ή ανακριβών πληροφοριών. Και οι δύο αυτές πρακτικές μπορεί να προετοιμάζουν άλλες επιθέσεις (όπως κοινωνική μηχανική και ηλεκτρονικό ψάρεμα) και να χρησιμοποιούνται παράλληλα με άλλες απειλές για την κυβερνοασφάλεια.

Το παράδοξο είναι ότι, αφενός, οι καινοτόμες τεχνολογίες μπορούν να χρησιμοποιούνται με σκοπό τη δημιουργία νέων λύσεων για τη βελτίωση της κυβερνοασφάλειας και, αφετέρου, οι ίδιες τεχνολογίες παρέχουν περαιτέρω ευκαιρίες για τους εγκληματίες του κυβερνοχώρου. Ως εκ τούτου, παράλληλα με τη θετική χρήση της τεχνητής νοημοσύνης (ΤΝ/AI), όπως για την ανίχνευση εισβολών και την αναγνώριση κακόβουλου λογισμικού (Truong κ.α., 2020), αναπτύσσονται νέες απειλές και ενισχύονται οι παραδοσιακές απειλές (Brundage κ.α., 2018). Για παράδειγμα, οι τεχνολογίες τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν για την αυτοματοποίηση των επιθέσεων κοινωνικής μηχανικής, καθώς

και για την αύξηση της αποτελεσματικότητας του κακόβουλου λογισμικού. Επιπλέον, ο πολλαπλασιασμός των συσκευών του Διαδικτύου των Πραγμάτων (IoT) επιφέρει περαιτέρω τρωτότητες που πρέπει να αντιμετωπιστούν, εφόσον οι συσκευές αυτές έχουν ασθενέστερες ικανότητες επεξεργασίας και αποθήκευσης, οπότε περιορίζονται οι εφαρμογές ασφάλειας για την προστασία τους[12]

Συγκεκριμένες συνθήκες εργασίας έχουν αυξήσει τις ευκαιρίες για τους εγκληματίες του κυβερνοχώρου. Η εξ αποστάσεως εργασία, για παράδειγμα, που υιοθετήθηκε ευρέως το 2020 λόγω της πανδημίας COVID-19, έχει δημιουργήσει νέες προκλήσεις για την ασφάλεια των επιχειρήσεων, όπως τη δημιουργία περισσότερων τελικών σημείων που μπορεί να είναι ευάλωτα σε παραβιάσεις της ασφάλειας, και τη χρήση προσωπικών συσκευών για επαγγελματικές δραστηριότητες (BYOD - «Φέρε τη δική σου συσκευή»)[13]. Στην πραγματικότητα, η άνεση του να βρίσκεις τα πάντα σε μία συσκευή συνδέεται με σημαντικούς κινδύνους ασφάλειας, όταν, για παράδειγμα, η απερίσκεπτη συμπεριφορά στην ιδιωτική χρήση ψηφιακών συσκευών επεκτείνεται στην επαγγελματική χρήση (Disterer και Kleiner, 2013). Εξάλλου, η απώλεια μιας ψηφιακής συσκευής θέτει σε κίνδυνο όχι μόνο τις προσωπικές αλλά και τις επαγγελματικές πληροφορίες. Η εξ αποστάσεως εργασία αποτελεί, συνεπώς, μια πρόκληση για την ασφάλεια των επιχειρήσεων, οι οποίες καλούνται να αναθεωρήσουν τις εταιρικές πολιτικές τους και να επενδύσουν στην άρτια κατάρτιση των τηλεργαζομένων (Borkovich και Skovira, 2020).

Είναι επίσης ενδιαφέρον να παρατηρήσουμε ότι οι ίδιοι οι εργαζόμενοι που χρησιμοποιούν φορετές συσκευές (όπως ακουστικά wi-fi ή “έξυπνα” ρολόγια) μπορεί να γίνουν ακούσιοι ξενιστές για τους εγκληματίες του κυβερνοχώρου. Οι τεχνολογίες φορετών συσκευών παρουσιάζουν ορισμένους κινδύνους για την κυβερνοασφάλεια, όπως στην περίπτωση συσκευών συνδεδεμένων με έναν εταιρικό φορητό υπολογιστή που μπορούν να εισαγάγουν ιούς στο σύστημα της εταιρείας, καθώς και κινδύνους για την ιδιωτικότητα που προκαλούνται από μη εξουσιοδοτημένη πρόσβαση (Heembrock, 2015).

Άλλες αναδυόμενες απειλές για την κυβερνοασφάλεια εγείρουν περαιτέρω ανησυχίες τόσο για τα άτομα όσο και για τις επιχειρήσεις, εξαιτίας των πολλαπλασιαστικών αποτελεσμάτων των μέσων κοινωνικής δικτύωσης. Τα deep fake βίντεο, για παράδειγμα, είναι ψηφιακά αλλοιωμένα αρχεία βίντεο ή ήχου όπου εμφανίζονται άτομα –συχνά διασημότητες ή πολιτικοί– για κακόβουλους σκοπούς, όπως η διάδοση ψευδών πληροφοριών και η δυσφήμιση αυτών των ατόμων. Ωστόσο, η ανησυχία για αυτές τις απειλές επεκτείνεται πέρα από την προπαγάνδα και τις πολιτικές εκλογές, καθώς μπορούν επίσης να πλήξουν επιχειρήσεις μέσω χειραγώγησης της αγοράς, σαμποτάζ εμπορικών σημάτων, εκβιασμού και ψηφιακής αντιποίησης ταυτότητας στελεχών (Westerlund, 2019).

Τέλος, λαμβάνοντας υπόψη την εντυπωσιακή πρόοδο της τεχνολογικής καινοτομίας, εκτιμάται ότι η κβαντική πληροφορική, που μπορεί να επεξεργαστεί πληροφορίες πολύ πιο αποτελεσματικά από τις παραδοσιακές μεθόδους, μπορεί να είναι διαθέσιμη έως το 2025[14] Θεωρητικά, αυτοί οι υπολογιστές θα μπορούσαν να παραβιάσουν πολλά από τα σημερινά συστήματα κρυπτογράφησης ασφαλείας, αλλά απαιτείται σημαντική τεχνολογική πρόοδος[15] για να τεθεί πρακτικά σε χρήση αυτή η τεχνολογία.

Με βάση το σενάριο που μόλις περιγράφηκε, καθίσταται σαφές γιατί οι κίνδυνοι για την κυβερνοασφάλεια κατατάσσονται σε υψηλή θέση μεταξύ των άλλων παγκόσμιων κινδύνων (Παγκόσμιο Οικονομικό Φόρουμ, 2021).

Ο αντίκτυπος των κυβερνοεπιθέσεων στην ΕΑΥ

Οι κυβερνοεπιθέσεις κατά επιχειρήσεων και οργανισμών αναλύονται πάντα από τεχνολογική σκοπιά, παρότι ο ανθρώπινος παράγοντας αποτελεί εξίσου σημαντικό μέρος του ζητήματος της κυβερνοασφάλειας (Corradini κ.α., 2020). Παρομοίως, όταν εξετάζεται ο αντίκτυπος των κυβερνοεπιθέσεων, δίνεται έμφαση κυρίως στις οικονομικές πτυχές (Cashell κ.α., 2004· Anderson κ.α., 2013), και σπάνια στην υγεία και ασφάλεια των εργαζομένων. Στην πραγματικότητα, ο αντίκτυπος μετράται κυρίως ως προς το υλικό κόστος, όπως η απώλεια δεδομένων και η διακοπή των

[12] https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/
[13] https://www.techrepublic.com/article/how-to-combat-the-security-challenges-of-a-remote-workforce/
[14] https://builtin.com/founders-entrepreneurship/quantum-computing-revolution
[15] https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat

επιχειρηματικών δραστηριοτήτων, και ως προς το άυλο κόστος, όπως η απώλεια του ανταγωνιστικού πλεονεκτήματος λόγω της απώλειας στοιχείων πνευματικής ιδιοκτησίας, και η δυσφήμιση του εμπορικού σήματος[16].

Ωστόσο, οι κυβερνοεπιθέσεις μπορούν δυνητικά να καταλήξουν σε τραυματισμούς, ψυχολογικά προβλήματα ή και απώλεια ζωής, είναι συνεπώς σαφές ότι η αξιολόγηση των κινδύνων για την κυβερνοασφάλεια και η αξιολόγηση των κινδύνων για την ΕΑΥ στους χώρους εργασίας δεν μπορούν να θεωρούνται χωριστές δραστηριότητες, αλλά πρέπει να διενεργούνται μαζί (Izuakor, 2016). Κατά συνέπεια, οι επιχειρήσεις θα πρέπει να λαμβάνουν υπόψη διάφορες επιπτώσεις των απειλών για την κυβερνοασφάλεια και να υιοθετούν μια πιο ολοκληρωμένη προσέγγιση για τη βελτιστοποίηση της διαχείρισης των κινδύνων για την κυβερνοασφάλεια (Couce-Vieira κ.α., 2020) όπως, για παράδειγμα, περιγράφεται στον πίνακα 2.

Πίνακας 2: Οι ποικίλες επιπτώσεις εξαιτίας των κινδύνων κυβερνοασφάλειας

Κατηγορίες	Επιπτώσεις
Επιχείρηση/Οργανισμός	Οικονομικές ζημίες (όπως μικρότερη παραγωγικότητα λόγω μη διαθεσιμότητας υπηρεσίας, απώλεια μεριδίου της αγοράς ή απώλεια ανταγωνιστικού πλεονεκτήματος)
	Δυσφήμιση (ζημία στην αξιοπιστία των ενδιαφερόμενων μερών)
	Άλλες οικονομικές πτυχές (όπως ασφάλιση έναντι κινδύνων για την κυβερνοασφάλεια)
Εργαζόμενοι	Σωματικές βλάβες (όπως απώλεια ζωής λόγω βλάβης ενός κυβερνοφυσικού συστήματος)
	Ψυχικές βλάβες (όπως άγχος ή απογοήτευση)
	Αντίκτυπος στα ατομικά δικαιώματα (παραβίαση ιδιωτικότητας λόγω παραβίασης προσωπικών δεδομένων)
	Προσωπική οικονομική ζημία
Άλλοι συναφείς οργανισμοί	Ζημία λόγω διατάραξης διασυνδέσεων παγκόσμιων αλυσίδων εφοδιασμού
Περιβάλλον	Αντίκτυπος στο φυσικό περιβάλλον (όπως ρύπανση εδάφους λόγω κυβερνοπεριστατικού)

Προσαρμογή από Couce-Vieira κ.α. 2020

Αυτές οι επιπτώσεις μπορούν να συνδεθούν με κόστος μετρήσιμο με χρηματικούς όρους, όπως η απώλεια μεριδίου της αγοράς, και με μη χρηματικό κόστος, όπως οι σωματικές ή ψυχικές βλάβες.

Στην ακόλουθη ενότητα θα εξετασθεί η σημασία των πιθανών σωματικών και ψυχολογικών επιπτώσεων στην υγεία και ασφάλεια των εργαζομένων.

Πτυχές ασφάλειας που σχετίζονται με την κυβερνοασφάλεια

Η ελλιπής συνεκτίμηση των πτυχών ασφάλειας που σχετίζονται με την κυβερνοασφάλεια μπορεί να αποδοθεί στο γεγονός ότι οι κίνδυνοι για την κυβερνοασφάλεια θεωρούνται εξωτερικές απειλές, ενώ τα ζητήματα υγείας και ασφάλειας αντιμετωπίζονται εντός των επιχειρήσεων και των οργανισμών[17]. Ωστόσο, η εξέλιξη των κυβερνοαπειλών και η αυξανόμενη έκθεση επιχειρήσεων και οργανισμών σε

[16] https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/cyber-security-is-your-organisation-under-threat-of-a-cyber-attack.html
[17] https://donesafe.com/2017/06/why-cybersecurity-should-factor-into-every-health-and-safety-plan/

κυβερνοεπιθέσεις απαιτεί την υιοθέτηση μιας ολιστικής προσέγγισης για την αποτελεσματική τους διαχείριση, που θα περιλαμβάνει την προστασία της υγείας και ασφάλειας των εργαζομένων.

Οι κυβερνοεπιθέσεις μπορούν όχι μόνο να θέσουν σε κίνδυνο τους πληροφοριακούς πόρους μιας επιχείρησης ή ενός οργανισμού, αλλά και να απειλήσουν τη σωματική και ψυχική υγεία των εργαζομένων, όταν οι χάκερ επιτίθενται σε κρίσιμες υποδομές[18] ή αποκτούν τον έλεγχο των τεχνολογικών συσκευών των εργαζομένων. Η παραβίαση μιας συσκευής, για παράδειγμα, μπορεί να προκαλέσει σωματική βλάβη σε άτομα και να θέσει σε κίνδυνο τις προσωπικές πληροφορίες τους (Loukas, 2019).

Ορισμένα παραδείγματα μπορούν να αποσαφηνίσουν αυτό το ζήτημα. Το 2014 στη Γερμανία, μια χαλυβουργία δέχθηκε επίθεση χάκερ και οι επιτιθέμενοι κατάφεραν να διακόψουν τη λειτουργία της καμίνου[19]. Ο κίνδυνος να μετατραπεί η κυβερνοεπίθεση σε κρίσιμο συμβάν για την ασφάλεια των εργαζομένων ήταν πολύ υψηλός, λόγω της φύσης των υλικών.

Το 2017, η Υπηρεσία Τροφίμων και Φαρμάκων (FDA) των ΗΠΑ απέσυρε περίπου 465 000 βηματοδότες λόγω τρωτοτήτων ασφαλείας. Οι συσκευές ήταν ευάλωτες σε παραβιάσεις ασφαλείας, θέτοντας επομένως σε κίνδυνο τη ζωή των ασθενών[20].

Οι κυβερνοεπιθέσεις σε βιομηχανικά συστήματα ελέγχου που περιλαμβάνουν τόσο ηλεκτρονικά όσο και φυσικά στοιχεία αποτελούν επικίνδυνη απειλή για την ανθρώπινη ζωή. Για παράδειγμα, το Stuxnet[21], ένα σκουλήκι υπολογιστών που δημιουργήθηκε το 2010 για να αποκτήσει τον έλεγχο των ιρανικών φυγοκεντριστών που χρησιμοποιούνταν για τον εμπλουτισμό ουρανίου· ή το κακόβουλο λογισμικό Triton[22], που το 2017 εισέβαλε σε πετροχημική βιομηχανία στη Μέση Ανατολή και, ευτυχώς, απέτυχε. Αυτά τα είδη επιθέσεων μπορούν επίσης να προκαλέσουν σοβαρές επιπτώσεις στο περιβάλλον.

Η εξ αποστάσεως χρήση εξοπλισμού σε επικίνδυνες καταστάσεις μπορεί να θέσει την ασφάλεια των εργαζομένων σε κίνδυνο, όπως στην περίπτωση οχημάτων ή μηχανημάτων που λειτουργούν ανεξέλεγκτα λόγω διακοπής των ασύρματων σημάτων ή λόγω επιθέσεων από χάκερ (Steijn κ.α., 2016).

Στον μεταποιητικό τομέα, όταν άνθρωποι και ρομπότ συνεργάζονται σε γραμμές παραγωγής, οι κυβερνοεπιθέσεις μπορούν να διακόψουν τις φυσικές βιομηχανικές διαδικασίες και να προκαλέσουν τραυματισμούς εργαζομένων (Perales Gómez κ.α., 2020).

Σύμφωνα με την Gartner, οι κυβερνοεπιτιθέμενοι θα μπορούν ενδεχομένως έως το 2025 να χρησιμοποιούν επιτυχώς ως όπλο την τεχνολογία παραγωγικών λειτουργιών (OT) και άλλα κυβερνοφυσικά συστήματα με σκοπό να βλάπτουν ή να σκοτώνουν ανθρώπους[23].

Όταν εξαπολύουν μια κυβερνοεπίθεση κατά νοσοκομείων, οι χάκερ μπορούν να αποκτήσουν πρόσβαση στις ευαίσθητες πληροφορίες όλων των ασθενών και εργαζομένων,αυτό όμως που μπορεί να τεθεί σε σοβαρό κίνδυνο είναι η δυνατότητα των ασθενών να λάβουν την κατάλληλη περίθαλψη και να υποβληθούν στις απαραίτητες ιατρικές επεμβάσεις (Argaw κ.α., 2020)[24]. Η ανάλυση της παγκόσμιας επίθεσης με το λυτρισμικό λογισμικό «WannaCry», τον Μάιο του 2017, κατέδειξε σημαντικές αρνητικές επιπτώσεις στο εθνικό σύστημα υγείας της Βρετανίας (Ghafur κ.α., 2019).

Κατά τη διάρκεια της πανδημίας COVID-19, τα αμερικανικά νοσοκομεία αποτέλεσαν στόχο ενός κύματος επιθέσεων με λυτρισμικό λογισμικό που διέκοψαν την παροχή υγειονομικής περίθαλψης σε

[18] Οι κρίσιμες υποδομές είναι ζωτικής σημασίας για τη λειτουργία μιας χώρας, δεδομένου ότι περιλαμβάνουν κλάδους όπως η ενέργεια, η δημόσια υγεία, οι τηλεπικοινωνίες, ο τραπεζικός και χρηματοοικονομικός κλάδος.
[19] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/
[20] https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362
[21] https://spectrum.ieee.org/the-real-story-of-stuxnet
[22] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/
[23] https://www.thehindubusinessline.com/info-tech/cyber-attackers-could-weaponise-tech-to-kill-humans-by-2025-gartner/article35519872.ece
[24] Το 2020, ένα γερμανικό νοσοκομείο έπεσε θύμα κυβερνοεπίθεσης, με αποτέλεσμα να μην μπορεί να δεχθεί εισερχόμενους ασθενείς. Μια γυναίκα που διακομίστηκε εκεί προκειμένου να λάβει περίθαλψη, πέθανε καθ' οδόν προς το κοντινότερο νοσοκομείο, που ήταν πάνω από 30 χιλιόμετρα μακριά. Μετά την έρευνα που διενεργήθηκε, οι εισαγγελείς αποφάνθηκαν ότι τα στοιχεία ήταν ανεπαρκή, αλλά είναι γνωστό ότι μια επίθεση με λυτρισμικό λογισμικό ήταν υπεύθυνη για το κλείσιμο του τμήματος επειγόντων περιστατικών του νοσοκομείου. https://www.wired.co.uk/article/ransomware-hospital-death-germany

αρκετά νοσοκομεία, απειλώντας σοβαρά τη ζωή των ασθενών[25]. Έρευνες που εστιάζουν στη χρήση λυτρισμικού λογισμικού κατά οργανισμών υγειονομικής περίθαλψης, δείχνουν πώς αυτές οι κυβερνοαπειλές μπορεί να έχουν συνέπειες ζωής και θανάτου (Ponemon, 2021).

Κοινωνικές και ψυχολογικές επιπτώσεις

Οι κυβερνοεπιθέσεις μπορούν να συνδεθούν με κοινωνικές επιπτώσεις, όπως απώλεια εμπιστοσύνης στην ψηφιακή τεχνολογία, και ψυχολογικές επιπτώσεις, όπως άγχος, θυμός και κατάθλιψη (Bada και Nurse, 2020). Οι εργαζόμενοι που έχουν υποστεί κυβερνοεπιθέσεις μπορεί να καταλήξουν να αισθανθούν ντροπή, ενοχή, σύγχυση ή απελπισία, ειδικά στην περίπτωση διαρροής ψηφιακών πληροφοριών, και η βαρύτητα αυτών των επιπτώσεων εξαρτάται από το περιβάλλον που εμπλέκεται στην κυβερνοεπίθεση (Αγραφιώτης κ.α., 2018). Για παράδειγμα, σε ένα χρηματοπιστωτικό ίδρυμα, όπου οι συνέπειες μιας παραβίασης δεδομένων είναι πιθανόν περισσότερο σοβαρές από ό,τι σε ένα άλλο ίδρυμα παροχής υπηρεσιών, η ψυχολογική βλάβη στους εργαζομένους μπορεί να είναι μεγαλύτερη. Σε πιο ακραίες περιπτώσεις, μια διαρροή δεδομένων μπορεί να καταλήξει στην αυτοκτονία των ατόμων που επηρεάζονται –καθώς αισθάνονται μεγάλη ντροπή λόγω της δημόσιας έκθεσης των πληροφοριών που τους αφορούν[26] – και η ψυχολογική επιβάρυνση που αισθάνονται οι εργαζόμενοι μπορεί να είναι ιδιαίτερα δυσβάστακτη.

Ως εκ τούτου, η ιδιωτικότητα και η ασφάλεια αλληλοσυνδέονται ολοένα και περισσότερο, και ενώ η ιδιωτικότητα αφορά τη συλλογή και χρήση προσωπικών δεδομένων, η ασφάλεια στοχεύει στη διασφάλιση της προστασίας αυτών των δεδομένων[27]. Ο γενικός κανονισμός για την προστασία των προσωπικών δεδομένων (ΓΚΠΔ), που τέθηκε σε ισχύ στις 25 Μαΐου 2018, υποχρεώνει τους οργανισμούς της ΕΕ να προστατεύουν τα δεδομένα και την ιδιωτική ζωή[28], και σε περίπτωση παραβίασης δεδομένων που θέτει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των χρηστών, οι επιχειρήσεις έχουν προθεσμία 72 ωρών να ειδοποιήσουν όσους επηρεάζονται από την παραβίαση.

Είναι ενδιαφέρον να παρατηρήσουμε πώς η παραβίαση της ιδιωτικότητας μπορεί να έχει αρνητικές επιπτώσεις για την ψυχική υγεία των ατόμων. Η ιδιωτικότητα αποτελεί μια ψυχολογική ανάγκη που σχετίζεται αυστηρά με την ανάπτυξη της προσωπικής ταυτότητας (Aboujaoude, 2019).

Οι έρευνες σχετικά με τη θυματοποίηση του κυβερνοεγκλήματος υπογραμμίζουν τις αρνητικές εμπειρίες τόσο για τις επιχειρήσεις όσο και για τα άτομα (για παράδειγμα, Augustina, 2015 και McGuire και Dowling, 2013). Ειδικά όταν οι οργανισμοί υφίστανται επιθέσεις λυτρισμικού λογισμικού, οι ομάδες τεχνολογίας των πληροφοριών (ΤΠ) πλήττονται όσον αφορά την επαγγελματική αξιοπιστία και την υψηλή εκτίμηση του εξειδικευμένου προσωπικού[29]. Επιπλέον, οι επιθέσεις με λυτρισμικό λογισμικό είναι πιθανό να έχουν μεγαλύτερο ψυχολογικό αντίκτυπο στους εργαζομένους από ό,τι άλλα περιστατικά ασφαλείας, καθώς, όταν οι επιχειρήσεις πληρώνουν τα λύτρα, «ανταμείβουν» τους επιτιθέμενους αντί να επενδύουν χρήματα στο προσωπικό τους[30].

Περαιτέρω προβληματισμοί μπορούν να διατυπωθούν σχετικά με το ανθρώπινο λάθος, που θεωρείται η κύρια αιτία του 90 % των παραβιάσεων της κυβερνοασφάλειας[31]. Τα λάθη αυτά, όπως το άνοιγμα μηνυμάτων email ηλεκτρονικού ψαρέματος ή η παραμέληση της διαχείρισης των κωδικών πρόσβασης μπορούν να εκθέσουν τους οργανισμούς σε σοβαρές συνέπειες, όπως κατά λάθος εγκατάσταση κακόβουλου λογισμικού στο δίκτυο μιας επιχείρησης ή ενός οργανισμού. Μπορεί εύκολα να φανταστεί κανείς το αίσθημα της αποτυχίας που νιώθουν οι εργαζόμενοι οι οποίοι είναι υπεύθυνοι

25 https://www.technologyreview.com/2020/10/29/1011436/a-wave-of-ransomware-hits-us-hospitals-as-coronavirus-spikes/

26 Ο ιστότοπος γνωριμιών Ashley Madison, που δέχθηκε επίθεση από χάκερ τον Ιούλιο του 2015, αποτελεί μια δραματική περίπτωση από πλευράς συνεπειών. Τα δεδομένα που δημοσιοποίησαν οι χάκερ περιλάμβαναν ονόματα, κωδικούς πρόσβασης, διευθύνσεις, αλλά και πληροφορίες για τις σεξουαλικές επιθυμίες των πελατών. Μετά από αυτήν την παραβίαση δεδομένων, ακολούθησαν παραιτήσεις, διαζύγια και αυτοκτονίες. https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked
https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/CYB-ET/Pres/8-4%20Waleed%20Hagag_PrivacyVSSecurity.pdf

28 https://gdpr.eu/tag/gdpr/

29 https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx

30 https://securityintelligence.com/posts/ransomware-response-beyond-money-to-morale/

31 https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

για το συμβάν, σε βαθμό που μπορεί επίσης να τους αποτρέψει να αναφέρουν το λάθος στην επιχείρηση ή τον οργανισμό όπου απασχολούνται.

Όσον αφορά τα ανθρώπινα λάθη, είναι σημαντικό να εξεταστούν οι ψυχολογικοί παράγοντες που εμπλέκονται στα περιστατικά κυβερνοασφάλειας: Το 52 % των εργαζομένων είναι πιθανότερο να κάνουν λάθη όταν είναι αγχωμένοι, το 43 % όταν είναι κουρασμένοι και το 26 % όταν αισθάνονται εξαντλημένοι[32]. Εξάλλου, οι επαγγελματίες του τομέα της κυβερνοασφάλειας βιώνουν υψηλά επίπεδα άγχους ή εξάντλησης καθώς εργάζονται για να εμποδίζουν ή να μετριάζουν τις κυβερνοεπιθέσεις[33].

Τέλος, ως υποσημείωση, είναι σημαντικό να παρατηρήσουμε πως η διάσταση του κυβερνοχώρου επηρεάζει επίσης τα φαινόμενα βίας. Ο διαδικτυακός εκφοβισμός, για παράδειγμα, είναι η πλέον γνωστή μορφή διαδικτυακής παρενόχλησης (Notar κ.α., 2013) με σκοπό την ταπείνωση, την καταδίωξη και τον έλεγχο ενός ατόμου με χρήση ψηφιακών μέσων. Αν και αυτό το φαινόμενο δεν εντάσσεται αυστηρά στο πεδίο της κυβερνοασφάλειας, οι επιθέσεις με κακόβουλο λογισμικό και κλοπή ταυτότητας μπορούν να χρησιμοποιηθούν προκειμένου να βλάψουν άτομα. Η διαδικτυακή παρενόχληση μπορεί να προκαλέσει σοβαρές ψυχοσωματικές, κοινωνικές και ψυχικές επιπτώσεις (Dressing κ.α., 2014· Betts, 2016). Συνεπώς, δεδομένου ότι ο διαδικτυακός εκφοβισμός στην εργασία (Corradini, 2019· Farley κ.α., 2021) μπορεί να θέσει σε κίνδυνο την υγεία και ασφάλεια των εργαζομένων, αυτό το ζήτημα θα πρέπει να αντιμετωπιστεί σωστά.

Στόχος των κυβερνοεπιθέσεων

Η καινοτόμος τεχνολογία έχει διεισδύσει σε κάθε εργασιακό τομέα. Όλοι οι οργανισμοί –οι πολύ μικρές, μικρές και μεσαίες επιχειρήσεις (ΜΜΕ), καθώς και οι μεγάλου μεγέθους επιχειρήσεις– μπορεί να αποτελέσουν στόχο των εγκληματιών του κυβερνοχώρου, οπότε κινδυνεύουν να δεχθούν κυβερνοεπίθεση. Πολλές πολύ μικρές και μικρές επιχειρήσεις δεν διαθέτουν τους απαραίτητους πόρους για την άμυνά τους, όπως καταδεικνύει το γεγονός ότι το 43 % όλων των παραβιάσεων δεδομένων αφορούν πολύ μικρές και μικρές επιχειρήσεις (Verizon, 2019).

Είναι σαφές ότι σε έναν ολοένα και περισσότερο ψηφιακό κόσμο, οι επιχειρήσεις και οι οργανισμοί αλληλοσυνδέονται ολοένα και περισσότερο, επεκτείνοντας επομένως την επιφάνεια έκθεσης σε πιθανές επιθέσεις.

Εξετάζοντας τους περισσότερο ευάλωτους τομείς σε κυβερνοεπιθέσεις, σύμφωνα με την έκθεση για την ασφάλεια που δημοσίευσε η IBM το 2021, ο χρηματοοικονομικός και ο ασφαλιστικός κλάδος υπέστησαν τις περισσότερες επιθέσεις το 2020 (23 % των επιθέσεων), ακολουθούμενοι από τον κλάδο της βιομηχανίας (17,7 %), της ενέργειας (11,1 %), του λιανεμπορίου (10,2 %), των επαγγελματικών υπηρεσιών (8,7 %), των κυβερνητικών υπηρεσιών (7,9 %), της υγειονομικής περίθαλψης (6,6 %), των μέσων ενημέρωσης (5,7 %), των μεταφορών (5,1 %), της εκπαίδευσης (4,0 %).

Παρατηρώντας την εξέλιξη των κλάδων που δέχονται κυβερνοεπιθέσεις, οι μελέτες υπογραμμίζουν ότι ο κλάδος της υγειονομικής περίθαλψης γίνεται πολύ ελκυστικός στόχος για τους εγκληματίες του κυβερνοχώρου[34], ιδίως λόγω των ευαίσθητων πληροφοριών που αποθηκεύονται στα ιατρικά αρχεία (Martin κ.α., 2017). Η πανδημία COVID-19 έχει επιδεινώσει την κατάσταση, καθώς οι εγκληματίες του κυβερνοχώρου έχουν στρέψει την προσοχή τους στην πνευματική ιδιοκτησία όσον αφορά στην ανάπτυξη εμβολίων (Muthuppalaniappan και Stevenson, 2021) και χρησιμοποιούν μηνύματα email ηλεκτρονικού ψαρέματος με θέμα τη νόσο COVID-19[35]. Ωστόσο, ο κλάδος της υγειονομικής περίθαλψης έχει μετασχηματιστεί σε μεγάλο βαθμό από τον αγώνα του κατά της πανδημίας, και σύμφωνα με τις μελλοντικές προοπτικές θα πρέπει να ενισχύσει την άμυνά του έναντι των κινδύνων για την ασφάλεια[36].

Ακόμα και οι εκπαιδευτικοί οργανισμοί γίνονται ελκυστικός στόχος για τους εγκληματίες του κυβερνοχώρου, δεδομένου ότι το 44 % δέχθηκαν επίθεση με λυτρισμικό λογισμικό το 2020 και το 35 % από αυτούς πλήρωσαν τα λύτρα για να πάρουν πίσω τα δεδομένα τους[37]. Οι αιτίες αποδίδονται

[32] https://www.tessian.com/research/the-psychology-of-human-error/
[33] https://news.vmware.com/security/hacking-burnout-for-cybersecurity-awareness-month-2021
[34] https://cybersecurityguide.org/industries/healthcare/
[35] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home
[36] https://www.protiviti.com/US-en/insights/whitepaper-top-risks-2021-and-2030-healthcare-industry-perspective
[37] https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/

κατά βάση στους περιορισμένους προϋπολογισμούς για την κυβερνοασφάλεια και στη μεγάλη βάση χρηστών, όπως σπουδαστές και προσωπικό, που μπορούν να αυξήσουν την έκθεση σε επιθέσεις. Επιπλέον, η έλλειψη ψηφιακής ευαισθητοποίησης των διδασκόντων και των σπουδαστών απαιτεί την υλοποίηση προγραμμάτων κατάρτισης για την υπεύθυνη χρήση των ψηφιακών τεχνολογιών (Corradini και Nardelli, 2020).

Η τρέχουσα κατάσταση όσον αφορά τις κυβερνοεπιθέσεις συνεχώς εξελίσσεται, οπότε είναι σημαντικό να παρακολουθούνται οι εξελίξεις χρόνο με τον χρόνο. Εν τω μεταξύ, αναδύεται μια ακόμα πιο ανησυχητική εικόνα. Οι επιτιθέμενοι με λυτρισμικό λογισμικό δοκιμάζουν νέες μεθόδους εκβιασμού, αναγκάζοντας τους οργανισμούς να συνεργαστούν και να κοινοποιήσουν πληροφορίες για να αντιμετωπίσουν την απειλή[38].

Παράγοντες κινδύνου θυματοποίησης

Οι εγκληματίες του κυβερνοχώρου ενδιαφέρονται περισσότερο για επιθέσεις σε επιχειρήσεις με χρήση κλεμμένων κωδικών πρόσβασης παρά για την εξαπόλυση μαζικών επιθέσεων με σκοπό την υποκλοπή πληροφοριών καταναλωτών[39]. Ωστόσο, 330 εκατομμύρια ενήλικοι σε 10 χώρες ήρθαν αντιμέτωποι με το κυβερνοέγκλημα το 2020[40], και εξάλλου η στόχευση συγκεκριμένων εργαζομένων, για παράδειγμα μέσω στοχευμένου ηλεκτρονικού ψαρέματος, μπορεί να αποτελέσει αποτελεσματική στρατηγική για την απόκτηση πρόσβασης στον οργανισμό τους.

Ο κίνδυνος να πέσει κανείς θύμα των διαφόρων μορφών κυβερνοεγκλήματος εξαρτάται τόσο από προσωπικούς όσο και από περιβαλλοντικούς παράγοντες (Jansen κ.α., 2017), και η μελέτη των προφίλ των θυμάτων μπορεί να συμβάλει στην καλύτερη κατανόηση της σχέσης μεταξύ κυβερνοεπιθέσεων και υποβάθρου των θυμάτων.

Από τη διαγενεακή ανάλυση των θυμάτων κυβερνοεγκλήματος, προκύπτει ότι οι νέοι ενήλικοι (κάτω των 25 ετών) και οι πιο ηλικιωμένοι (75 και άνω) είναι περισσότερο ευάλωτοι σε κυβερνοεπιθέσεις[41] Το φύλο αποτελεί σημαντικό παράγοντα που επηρεάζει τη συμπεριφορά ως προς την κυβερνοασφάλεια (Anwar κ.α., 2017), παρότι η περαιτέρω έρευνα σε αυτόν τον τομέα όσον αφορά τα δημογραφικά χαρακτηριστικά, μπορεί να έχει μεγάλο ενδιαφέρον για τον προσδιορισμό των κατάλληλων δράσεων πρόληψης. Ορισμένες μελέτες έχουν δείξει ότι οι γυναίκες είναι πιθανότερο να αποτελέσουν στόχο επιθέσεων ηλεκτρονικού ψαρέματος (Darwish κ.α., 2012), ενώ άλλες αποκαλύπτουν ότι οι γυναίκες ενδιαφέρονται περισσότερο για την προστασία της ιδιωτικότητας στους ιστοτόπους κοινωνικής δικτύωσης σε σχέση με τους άνδρες (Tifferet, 2019).

Τέλος, με δεδομένη την ανάγκη ενίσχυσης των περιβαλλόντων εργασίας έναντι των απειλών για την κυβερνοασφάλεια, φαίνεται ενδιαφέρον να αναλυθεί πώς οι οργανωτικοί παράγοντες, όπως οι κανόνες και οι ρουτίνες, επηρεάζουν την ευαλωτότητα των εργαζομένων σε μηνύματα email ηλεκτρονικού ψαρέματος και στοχευμένου ηλεκτρονικού ψαρέματος (Williams κ.α., 2018). Μια τέτοια ευρεία ανάλυση θα μπορούσε να παράσχει χρήσιμα στοιχεία για τη βελτίωση του σχεδιασμού των συστημάτων/εφαρμογών διεπαφής (interface design) και των προγραμμάτων ευαισθητοποίησης των εργαζομένων.

Για μια ολοκληρωμένη προσέγγιση της κυβερνοασφάλειας: ο ρόλος της ευαισθητοποίησης

Η σχέση μεταξύ κυβερνοαπειλών και υγείας και ασφάλειας αποτελεί μια ιδιαίτερα δυναμική πρόκληση για τις επιχειρήσεις και τους οργανισμούς, οι οποίοι καλούνται να λάβουν κάθε αναγκαίο μέτρο για μια συνολική εταιρική προσέγγιση της κυβερνοασφάλειας[42].

Αυτή η οπτική απαιτεί συνδυασμό των πτυχών της ασφάλειας στην εργασία και της κυβερνοασφάλειας, που συνήθως εξετάζονται ως χωριστές έννοιες, λόγω των διαφορετικών νομοθετικών ορίων, συμφερόντων και πρακτικών ζητημάτων (Μπούστρας και Waring, 2020).

[38] https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021
[39] https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/?utm_source=email&utm_medium=TMIEmail012821&utm_campaign=2020DBRReport
[40] https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf
[41] https://risk.lexisnexis.co.uk/about-us/press-room/press-release/20200223-biannual-cybercrime-report
[42] https://app.croneri.co.uk/feature-articles/health-safety-and-cyber-threats?topic=3682&product=154&section=3511

Για την επίτευξη αυτού του στόχου, ο ρόλος της ευαισθητοποίησης των διαφόρων ενδιαφερόμενων μερών είναι θεμελιώδης, επομένως θα πρέπει να προωθηθεί από τη σκοπιά τόσο της κυβερνοασφάλειας όσο και της ΕΑΥ, στενά συνδεόμενων μεταξύ τους.

Όσον αφορά τα ζητήματα κυβερνοασφάλειας, οι μελέτες υπογραμμίζουν πως η ελλιπής συμμόρφωση με τους κανόνες ασφάλειας και άλλοι οργανωτικοί παράγοντες, όπως τα ανεπαρκή μέτρα αντίδρασης, καθιστούν τους οργανισμούς ευάλωτους σε κυβερνοεπιθέσεις (Hart, 2019). Επιπλέον, ανεξάρτητα από την πολυμορφία των εργασιακών κλάδων, η έλλειψη ευαισθητοποίησης των εργαζομένων ως προς την κυβερνοασφάλεια είναι υπεύθυνη για πολλά περιστατικά κυβερνοασφάλειας[43]. Επομένως, τα προγράμματα ευαισθητοποίησης ως προς την κυβερνοασφάλεια μπορούν να διαδραματίσουν σημαντικό ρόλο στην ανάπτυξη μιας αποτελεσματικής νοοτροπίας κυβερνοασφάλειας στις επιχειρήσεις και στους οργανισμούς (Corradini, 2020), καθώς και στην πρόληψη των κυβερνοεπιθέσεων (Aldawood και Skinner, 2018).

Η ανάπτυξη της ευαισθητοποίησης για τις πιθανές συνέπειες των κυβερνοεπιθέσεων στον τομέα της ΕΑΥ απαιτεί να επεκταθεί η εστίαση σε πηγές κινδύνου που παραδοσιακά δεν εξετάζονται σε σχέση με την υγεία και ασφάλεια των εργαζομένων. Οι θετικές εμπειρίες από τη διαχείριση κινδύνων ΕΑΥ μπορούν επίσης να αποτελέσουν σημαντική πηγή έμπνευσης, δεδομένου ότι το θέμα της υγείας και ασφάλειας στους χώρους εργασίας βασίζεται σε πολλά έτη εμπειρίας, σε σύγκριση με τον τομέα της κυβερνοασφάλειας, και πολλές εφαρμογές και προγράμματα για την ανάπτυξη ασφαλέστερων περιβαλλόντων εργασίας εξακολουθούν να εφαρμόζονται με επιτυχία. Επιπλέον, η διαχείριση της ανθρώπινης αποτυχίας θεωρείται ζωτικής σημασίας για την πρόληψη των ατυχημάτων στον τομέα της ΕΑΥ.

Επιπλέον, δεδομένου ότι οι υπηρεσίες/τα τμήματα/οι εμπειρογνώμονες του τομέα της ασφάλειας ΤΠ δεν είναι συνήθως εξοικειωμένοι με την ΕΑΥ και, παρομοίως, η κοινότητα ΕΑΥ δεν είναι εξοικειωμένη με τις απειλές για την κυβερνοασφάλεια, η συνεργασία μεταξύ των δύο αυτών τομέων είναι απαραίτητη. Για παράδειγμα, η συνεργασία μεταξύ τμημάτων ΕΑΥ, ανθρώπινου δυναμικού και ασφάλειας ΤΠ σε μια επιχείρηση ή έναν οργανισμό, όπου είναι δυνατόν, μπορεί να επιτρέψει την εξέταση του ζητήματος των κυβερνοαπειλών από διαφορετικές οπτικές, και την εφαρμογή αποτελεσματικότερων, καινοτόμων λύσεων πρόληψης.

Αύξηση της ευαισθητοποίησης των ενδιαφερόμενων μερών

Λαμβάνοντας υπόψη όσα συζητήθηκαν ανωτέρω, το πρώτο βήμα είναι να ευαισθητοποιηθούν τα διάφορα ενδιαφερόμενα μέρη σχετικά με τους κινδύνους για την ΕΑΥ που σχετίζονται με τις κυβερνοαπειλές ώστε να μπορούν να ενεργούν υπεύθυνα.

Τα προγράμματα ευαισθητοποίησης μπορεί να είναι εξαιρετικά χρήσιμα, αλλά για να είναι αποτελεσματικά πρέπει να είναι σωστά σχεδιασμένα και προσαρμοσμένα στις ειδικές συνθήκες, ώστε να είναι κατάλληλα για τα διάφορα ενδιαφερόμενα μέρη. Θα πρέπει επίσης να περιλαμβάνουν μια σειρά εργαλείων και μεθοδολογιών, όπως εκστρατείες, εργαστήρια, διασκέψεις, εκπαιδευτικό υλικό και άλλες δράσεις επικοινωνίας. Επιπλέον, λαμβάνοντας υπόψη τα χαρακτηριστικά και τους περιορισμένους πόρους των πολύ μικρών επιχειρήσεων και των ΜΜΕ, θα πρέπει να αναπτυχθούν ειδικές πρωτοβουλίες προκειμένου να βοηθηθούν αυτές οι επιχειρήσεις.

Τα προγράμματα ευαισθητοποίησης θα πρέπει να περιλαμβάνουν τουλάχιστον τα εξής εσωτερικά και εξωτερικά ενδιαφερόμενα μέρη:

- Οι **εργοδότες**, που είναι νομικά υπεύθυνοι για την ασφάλεια και υγεία των εργαζομένων τους, καθώς και η **διοίκηση/διοικητικά στελέχη**, είναι βασικοί παράγοντες λόγω του ηγετικού ρόλου τους στις επιχειρήσεις και τους οργανισμούς. Με βάση τη νομοθεσία περί υγείας και ασφάλειας, οι εργοδότες έχουν εκτεταμένα καθήκοντα για να προστατεύουν τους εργαζομένους τους από κάθε εργασιακό κίνδυνο και να διαχειρίζονται αποτελεσματικά αυτούς τους κινδύνους. Καθώς οι κυβερνοαπειλές μπορούν να έχουν αντίκτυπο στην υγεία και ασφάλεια των εργαζομένων, θα πρέπει να λαμβάνονται ρητώς υπόψη στις δραστηριότητες πρόληψης και διαχείρισης κινδύνων ΕΑΥ.

[43] https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers/

- Οι **εργαζόμενοι** πρέπει να είναι ενημερωμένοι σχετικά με τους κινδύνους για την ασφάλεια και την υγεία τους που ενδέχεται να αντιμετωπίσουν κατά τις εργασιακές τους δραστηριότητες, και οι κίνδυνοι του κυβερνοχώρου θα πρέπει να συμπεριλαμβάνονται σε αυτούς. Είναι, επομένως, σαφές ότι η παροχή πληροφόρησης και κατάρτισης στους εργαζομένους για το συγκεκριμένο ζήτημα αποτελεί απαραίτητο μέτρο πρόληψης.
- Οι **επαγγελματίες του τομέα της ΕΑΥ** θα πρέπει να συμμετέχουν στις πρωτοβουλίες ευαισθητοποίησης, καθώς γενικά είναι ελλιπώς ευαισθητοποιημένοι ως προς την κυβερνοασφάλεια. Οι εν λόγω επαγγελματίες μπορούν να αναλάβουν καίριο ρόλο στην πρόληψη των επιπτώσεων των κυβερνοεπιθέσεων στην υγεία και ασφάλεια των εργαζομένων, και θα πρέπει να είναι ενημερωμένοι για την εξέλιξη των οργανωτικών πλαισίων και για τους σχετικούς κινδύνους για την κυβερνοασφάλεια.
- **Επιθεωρήσεις εργασίας** Οι νέες προκλήσεις που θέτουν οι κυβερνοαπειλές όσον αφορά την ΕΑΥ θα επιβάλουν πιθανότατα τη χρήση νέων μεθόδων και εργαλείων για τα καθήκοντα που ασκούν οι επιθεωρήσεις εργασίας. Ως εκ τούτου, η ευαισθητοποίηση σχετικά με τους κινδύνους που σχετίζονται με τις κυβερνοαπειλές είναι θεμελιώδους σημασίας τόσο για τον ελεγκτικό όσο και για τον προληπτικό ρόλο των επιθεωρήσεων εργασίας.
- **Υπεύθυνοι ασφάλειας ΤΠ**. Συχνά δεν είναι εξοικειωμένοι με τις πτυχές επαγγελματικής ασφάλειας της κυβερνοασφάλειας, δεδομένου ότι, από τη φύση της εργασίας τους, εστιάζουν κατά βάση στην ασφάλεια δικτύων και δεδομένων, και στον σχεδιασμό και τη διαχείριση μιας αποτελεσματικής πολιτικής ΤΠ για τον οργανισμό τους. Η ενίσχυση της ευαισθητοποίησής τους σχετικά με αυτό το θέμα θα συνέβαλλε στην ενθάρρυνση της συνεργασίας με εμπειρογνώμονες σε θέματα ΕΑΥ και θα ενσωμάτωνε μια επιπλέον οπτική στον καθορισμό των κανόνων και πρακτικών ασφαλείας των οργανισμών.

Με δεδομένη τη μελλοντική επέκταση των σχετικών με την κυβερνοασφάλεια κινδύνων στην ασφάλεια στον χώρο εργασίας, και άλλες κατηγορίες ενδιαφερομένων θα πρέπει να γνωρίζουν τις επιπτώσεις της κυβερνοασφάλειας στην ΕΑΥ και να συμβάλλουν στις στρατηγικές πρόληψης. Μεταξύ αυτών, για παράδειγμα, είναι οι εμπειρογνώμονες στην αλληλεπίδραση ανθρώπων-υπολογιστών (Human-Computer Interaction - HCI) και οι κατασκευαστές λογισμικού.

Η **HCI** είναι ένα πολυεπιστημονικό πεδίο μελέτης, που αρχικά εστίαζε στην αλληλεπίδραση μεταξύ των υπολογιστών και των χρηστών τους, ενώ σήμερα καλύπτει πολλές μορφές σχεδιασμού της τεχνολογίας των πληροφοριών[44]. Λαμβάνοντας υπόψη ότι ο εργασιακός εξοπλισμός θα βασίζεται ολοένα και περισσότερο στη δικτύωση, ο κατάλληλος σχεδιασμός των διεπαφών HCI από εμπειρογνώμονες του τομέα αυτού, θα είναι καίριας σημασίας για την ελαχιστοποίηση του αντικτύπου στην κυβερνοασφάλεια και την ΕΑΥ (Korfmacher, 2019).

Παρομοίως, οι **υπεύθυνοι ανάπτυξης λογισμικού** μπορούν να διαδραματίσουν σημαντικό ρόλο, δεδομένου ότι ένα ολοένα και μεγαλύτερο ποσοστό του εργαζόμενου πληθυσμού, είτε εντός οργανισμού είτε εξ αποστάσεως, εκτελεί τις εργασιακές δραστηριότητές του μέσω ψηφιακών συστημάτων και λογισμικού. Συνεπώς, είναι σημαντικό να ενισχυθεί η ευαισθητοποίηση των υπεύθυνων για την ανάπτυξη λογισμικού ως προς τις επιπτώσεις των κυβερνοεπιθέσεων στην ασφάλεια και υγεία των εργαζομένων, ώστε να εξασφαλίζεται ο προσεκτικός σχεδιασμός και η υλοποίηση αυτών των συστημάτων, όσον αφορά στην ικανότητά τους να προστατεύονται από τους κινδύνους για την κυβερνοασφάλεια. Το γεγονός αυτό θα έχει θετικό αντίκτυπο στην ευημερία των εργαζομένων, βοηθώντας τους να αισθάνονται προστατευμένοι έναντι των επιθέσεων.

Συμπερασματικά, μια βασική σύσταση είναι να συμμετέχουν οι **εμπειρογνώμονες που ασχολούνται με την ανθρώπινη συμπεριφορά** στον σχεδιασμό και την εφαρμογή προγραμμάτων ευαισθητοποίησης ως προς την κυβερνοασφάλεια. Στην πραγματικότητα, η επιτυχία αυτών των πρωτοβουλιών εξαρτάται από τα κίνητρα των συμμετεχόντων, καθώς και από τις μεθόδους και τα εργαλεία που χρησιμοποιούνται για την υλοποίησή τους. Χρειάζονται, επομένως, επαρκείς ικανότητες και γνώσεις για την ανθρώπινη συμπεριφορά.

[44] https://www.interaction-design.org/literature/topics/human-computer-interaction

Τέλος, η κυβερνοασφάλεια είναι, πάνω από όλα, ανθρώπινο ζήτημα. Ως εκ τούτου, οι διεπιστημονικές ομάδες –που συνδυάζουν τεχνικές δεξιότητες με ανθρώπινες και κοινωνικές δεξιότητες– θα είναι ολοένα και περισσότερο απαραίτητες για την αποτελεσματική της διαχείριση.

Επόμενα βήματα

Οι μελλοντικές μελέτες θα πρέπει να εστιάσουν στις διασυνδέσεις μεταξύ των δύο τομέων που εξετάζονται, της κυβερνοασφάλειας και της ΕΑΥ. Ο εντοπισμός των αναγκών και των κενών θα συμβάλει στον προσδιορισμό των πιθανών κινδύνων των κυβερνοεπιθέσεων για τους εργαζόμενους, καθώς και στον καθορισμό των κατάλληλων πολιτικών και στρατηγικών πρόληψης στις επιχειρήσεις και στους οργανισμούς. Ενδιαφέρουσες συνδέσεις μεταξύ εργασιακής ασφάλειας και κυβερνοασφάλειας έχουν ήδη εξετασθεί στη βιβλιογραφία, όπως η θετική σχέση μεταξύ νοοτροπίας ασφάλειας, ικανοποίησης από την εργασία και συμπεριφοράς συμμορφούμενης με τους κανόνες ασφάλειας (Green και D'Arcy, 2010).

Οι υπάρχουσες έρευνες για τη σχέση μεταξύ κυβερνοασφάλειας και κινδύνων για την ασφάλεια στην εργασία εστιάζουν κυρίως στον τομέα της υγειονομικής περίθαλψης (για παράδειγμα, Martin κ.α., 2017) και στα αυτόνομα οχήματα (για παράδειγμα, Taeihagh και Lim, 2019), ενώ χρειάζονται περισσότερες μελέτες προκειμένου να διευκρινιστούν όλες οι πιθανές επιπτώσεις των κυβερνοεπιθέσεων στην υγεία και ασφάλεια των εργαζομένων σε κάθε εργασιακό κλάδο.

Επιπλέον, λαμβάνοντας υπόψη ότι τα ενσωματωμένα συστήματα θα είναι ολοένα και περισσότερο διαδεδομένα στο μέλλον, θα είναι αναγκαίο να εξασφαλιστεί επαρκής ενοποίηση μεταξύ κυβερνοασφάλειας και επαγγελματικής ασφάλειας. Τα συστήματα αυτά θα μπορούσαν να σχεδιαστούν κατά τρόπο ώστε να ανταποκρίνονται στους στόχους κυβερνοασφάλειας (όπως επιθέσεις από χάκερ), αλλά και να διασφαλίζουν τις λειτουργίες ασφάλειας στην εργασία, αποτρέποντας την πρόκληση βλάβης στους χρήστες (εργαζόμενοι). Η ενοποίηση επαγγελματικής ασφάλειας και κυβερνοασφάλειας αποτελεί φλέγον θέμα στην ανάπτυξη κρίσιμων συστημάτων[45], και τα διεθνή πρότυπα μπορούν να προσφέρουν χρήσιμη υποστήριξη στους οργανισμούς[46].

Τέλος, μπορούμε να υποθέσουμε ότι οι υβριδικές μορφές εργασίας –που συνδυάζουν εργασία από το σπίτι και εργασία στο γραφείο– θα είναι ακόμα πιο διαδεδομένες στο μέλλον, όπως και τα "έξυπνα" περιβάλλοντα εργασίας που βασίζονται στις τεχνολογίες του Διαδικτύου των Πραγμάτων και στα κυβερνοφυσικά συστήματα (Podgórski κ.α., 2017). Συνεπώς, οι επιχειρήσεις και οι οργανισμοί θα χρειαστεί να επικαιροποιήσουν την αξιολόγηση των επαγγελματικών κινδύνων τους ώστε να αναγνωρίζουν κάθε πιθανό σχετικό κίνδυνο για τους εργαζομένους τους και να λαμβάνουν τα κατάλληλα μέτρα. Για τον σκοπό αυτόν, θα πρέπει να εφαρμοστούν νέες μέθοδοι και εργαλεία.

Συμπερασματικές παρατηρήσεις

Ο ψηφιακός μετασχηματισμός αποτελεί μια ασταμάτητη διαδικασία, που συνοδεύεται από αρκετές προκλήσεις τις οποίες πρέπει να αντιμετωπίσει κάθε χώρα. Σήμερα, η κυβερνοασφάλεια αποτελεί μείζονα πηγή ανησυχίας για τις επιχειρήσεις και τους οργανισμούς κάθε μεγέθους και σε κάθε κλάδο οικονομικής δραστηριότητας, η οποία αναμένεται να διευρυνθεί στο μέλλον.

Ωστόσο, η διαχείριση της κυβερνοασφάλειας δεν μπορεί να περιοριστεί στην απλή τεχνολογική προστασία των συστημάτων και των πληροφοριών. Καθώς οι κυβερνοεπιθέσεις μπορούν να επηρεάσουν επίσης την υγεία και ασφάλεια των εργαζομένων, οι επιχειρήσεις και οι οργανισμοί θα πρέπει να εφαρμόζουν μια ολιστική προσέγγιση της κυβερνοασφάλειας. Προκειμένου να επιτευχθεί αυτός ο στόχος, απαιτείται **υιοθέτηση ενός διεπιστημονικού οράματος που ενσωματώνει τις τεχνικές και κοινωνικές ικανότητες** για την αντιμετώπιση των διαφόρων επιπτώσεων των κυβερνοαπειλών.

[45] https://insights.sei.cmu.edu/blog/integrating-safety-and-security-engineering-for-mission-critical-systems/

[46] Βλ. για παράδειγμα, ISO/TR 22100-4, Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects [Ασφάλεια των μηχανημάτων – Σχέση με το ISO 12100 – Μέρος 4: Καθοδήγηση των κατασκευαστών μηχανημάτων ως προς τη συνεκτίμηση των σχετικών πτυχών της ασφάλειας ΤΠ (κυβερνοασφάλεια)]· IEC TR 63074:2019 «Safety of machinery – Security aspects related to functional safety of safety-related control systems» [Ασφάλεια των μηχανημάτων – Πτυχές ασφάλειας που σχετίζονται με τη λειτουργική ασφάλεια των σχετικών με την ασφάλεια συστημάτων ελέγχου].

Όσον αφορά τις μεγάλου μεγέθους επιχειρήσεις και τους οργανισμούς, η συνεργασία μεταξύ υπευθύνων ασφάλειας ΤΠ και ΕΑΥ συνιστάται ιδιαίτερα για τον καθορισμό μιας καινοτόμου διαδικασίας αξιολόγησης των επαγγελματικών κινδύνων, ώστε να προστατεύονται τα υλικά και άυλα στοιχεία ενεργητικού και, πάνω από όλα, οι άνθρωποι. Συγχρόνως, φλέγον θέμα αποτελεί το πώς θα εφαρμοστούν αποτελεσματικές στρατηγικές για τις πολύ μικρές επιχειρήσεις και τις ΜΜΕ, που συχνά δεν διαθέτουν ειδικούς εσωτερικούς πόρους[47], αλλά παρόλα αυτά είναι εκτεθειμένες στις συνέπειες των κυβερνοαπειλών.

Η πρόκληση για το μέλλον είναι εξαιρετικά μεγάλη. Προκειμένου να τεθούν σωστές βάσεις, απαιτείται καταρχάς ένα ισχυρό και ευρύ πρόγραμμα ευαισθητοποίησης σχετικά με αυτά τα θέματα ώστε να προετοιμαστούν οι εργοδότες, οι εργαζόμενοι και η κοινότητα ΕΑΥ, καθώς και οι υπεύθυνοι ασφάλειας ΤΠ και οι λοιποί αρμόδιοι παράγοντες –όπως οι εμπειρογνώμονες σε θέματα HCI, οι κατασκευαστές λογισμικού και οι εμπειρογνώμονες σε θέματα ανθρώπινης συμπεριφοράς– για το σενάριο της ολοένα μεγαλύτερης υιοθέτησης και εφαρμογής ψηφιακών τεχνολογιών και συστημάτων/μέσων και της εξέλιξης των κυβερνοαπειλών.

Συντάκτες: Isabella Corradini, επιστημονική διευθύντρια του ερευνητικού κέντρου Themis (Ιταλία),

Διαχείριση έργου: Emmanuelle Brun, Annick Starren, με τη συμβολή της Ana Cayuela, Ευρωπαϊκός Οργανισμός για την Ασφάλεια και την Υγεία στην Εργασία (EU-OSHA).

[47] https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

Βιβλιογραφικές πηγές

Aboujaoude, E. (2019). Protecting privacy to protect mental health: The new ethical imperative [Προστασία της ιδιωτικότητας για την προστασία της ψυχικής υγείας: Η νέα ηθική επιταγή]. *Journal of Medical Ethics*. *45*(9), 604–607.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. και Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate [Ταξινόμηση των κινδύνων στον κυβερνοχώρο: Ορισμός των επιπτώσεων των κυβερνοεπιθέσεων και κατανόηση του τρόπου επέκτασής τους]. *Journal of Cybersecurity*, *4*(1).

Aldawood, H. and Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review [Εκπαίδευση και ευαισθητοποίηση σχετικά με την κοινωνική μηχανική της κυβερνοασφάλειας: Βιβλιογραφική επισκόπηση]. Σε IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). IEEE, 62–68.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. και Savage, S. (2013). Measuring the cost of cybercrime [Μέτρηση του κόστους του κυβερνοεγκλήματος]. Σε R. Böhme (επιμ.) *The economics of information security and privacy [Η οικονομία της ασφάλειας των πληροφοριών και της ιδιωτικότητας]* (265–300). Springer-Verlag.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. και Xu, L. (2017). Gender difference and employees' cybersecurity behaviors [Διαφορές μεταξύ των φύλων και συμπεριφορές των εργαζομένων ως προς την κυβερνοασφάλεια]. *Computers in Human Behavior*, 69, 437–443.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. και Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks [Η κυβερνοασφάλεια των νοσοκομείων: Ανάλυση των προκλήσεων και προσπάθεια μετριασμού των κινδύνων]. *BMC Medical Informatics and Decision Making, 20*(146).

Augustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect [Κατανόηση της θυματοποίησης στον κυβερνοχώρο: Ψηφιακές αρχιτεκτονικές και φαινόμενο της άρσης των αναστολών]. *International Journal of Cyber Criminology*. *9*(1), 35–54.

Bada, M. και Nurse, J. R. C. (2020). The social and psychological impact of cyber-attacks, psychology [Οι κοινωνικές και ψυχολογικές επιπτώσεις των κυβερνοεπιθέσεων]. Σε V. Benson και J. Mcalaney (επιμ.), *Emerging cyber threats and cognitive vulnerabilities* [Αναδυόμενες κυβερνοαπειλές και γνωστικές τρωτότητες] (σ. 73–92). Academic Press.

Betts, L. R. (2016). Cyberbullying: Approaches, consequences, and interventions [Διαδικτυακός εκφοβισμός: Προσεγγίσεις, συνέπειες και παρεμβάσεις]. Σε J. Binder (επιμ.), *Palgrave studies in Cyberpsychology*. Palgrave Macmillan.

Borkovich, D. J. και Skovira, R. J. (2020). Working from home: Cybersecurity in the age of covid-19 [Εργασία από το σπίτι: Η κυβερνοασφάλεια στην εποχή της covid-19]. *Issues in Information Systems*. *21*(4), 234–236.

Boustras, G. και Waring, A. (2020). Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context [Προς έναν επαναπροσδιορισμό της έννοιας της ασφάλειας στην εργασία και της ασφάλειας στον κυβερνοχώρο, των μεταξύ τους αλληλεπιδράσεων και των απαιτήσεων πολιτικής στο πλαίσιο του 21ου αιώνα]. *Safety Science*, 132.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B. κ.α. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation* [Η κακόβουλη χρήση της τεχνητής νοημοσύνης: Πρόβλεψη, πρόληψη και μετριασμός].https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Cashell, B., Jackson, W. D., Jickling, M. και Webel, B. (2004). The Economic Impact of Cyber-Attacks [Ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων]. *CRS Report for Congress*.

Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology [Ανάπτυξη μιας νοοτροπίας κυβερνοασφάλειας στους οργανισμούς: Πώς θα γεφυρωθεί το χάσμα μεταξύ ανθρώπων και ψηφιακής τεχνολογίας].* Springer.

Corradini, I. (2019). *Crimini relazionali nell'era digitale. Conoscere per prevenire. Cyber-bullismo-mobbing-stalking.* Themis.

Corradini, I., Nardelli, E. και Ahram, T. (επιμ.) (2020). *Advances in human factors in cybersecurity* [Εξελίξεις στους ανθρώπινους παράγοντες της κυβερνοασφάλειας]. AHFE 2020. Advances in Intelligent Systems and Computing [Εξελίξεις των έξυπνων συστημάτων και της πληροφορικής]. τόμος 1219, Springer.

Corradini, I. και Nardelli, E. (2020). Developing digital awareness at school: A fundamental step for cybersecurity education [Ανάπτυξη της ψηφιακής ευαισθητοποίησης στο σχολείο: Ένα θεμελιώδες βήμα για την εκπαίδευση στον τομέα της κυβερνοασφάλειας]. Σε I. Corradini, E. Nardelli και T. Ahram (επιμ.) *Advances in human factors in cybersecurity*. AHFE 2020. Advances in intelligent systems and computing. τόμος 1219, Springer.

Couce-Vieira, A., Insua, D. R. και Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts [Αξιολόγηση και πρόβλεψη των επιπτώσεων για την κυβερνοασφάλεια]. *Decision Analysis. 17*(4), 356–374.

Darwish, A., El Zarka, A. και Aloul, F. (2012). Towards understanding phishing victims' profile [Κατανόηση του προφίλ των θυμάτων ηλεκτρονικού ψαρέματος]. *International Conference on Computer Systems and Industrial Informatics*. 1–5.

Disterer, G. και Kleiner, C. (2013). BYOD - Bring Your Own Device [Φέρε τη δική σου συσκευή]. *HMD*. 50, 92–100.

Dressing, H., Bailer, J., Anders, A., Wagner, A. και Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims [Η διαδικτυακή παρενοχλητική παρακολούθηση σε μεγάλο δείγμα χρηστών κοινωνικών δικτύων: Συχνότητα, χαρακτηριστικά και επιπτώσεις στα θύματα]. *Cyberpsychology, Behavior, and Social Networking,* 17: 61–67.

ENISA. (2020). *Threat Landscape 2020* [Τοπίο απειλών 2020]. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA. (2021α). Threat Landscape 2021, 27 Οκτωβρίου 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2021β). Threat Landscape for Supply Chain Attacks [Τοπίο απειλών των επιθέσεων σε αλυσίδες εφοδιασμού], 29 Ιουλίου 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Farley, S., Coyne, I. και D'Cruz, P. (2021). Cyberbullying at Work: Understanding the influence of technology [Ο διαδικτυακός εκφοβισμός στην εργασία: Κατανόηση της επίδρασης της τεχνολογίας]. Σε P. D'Cruz, E. Noronha, G. Notelaers και C. Rayner (επιμ.), *Handbooks of workplace bullying, emotional abuse and harassment*. τόμος 1, Springer.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. και Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS [Αναδρομική ανάλυση επιπτώσεων της κυβερνοεπίθεσης WannaCry στο βρετανικό ΕΣΥ]. *NPJ Digital Medicine*. *2*(98).

Hamlyn-Harris, J. H. (2017). *Three reasons why pacemakers are vulnerable to hacking [Τρεις λόγοι για την ευαλωτότητα των βηματοδοτών σε παραβιάσεις ασφαλείας].* The Conversation. http://theconversation.com/three-reasons-why-pacemakers-are- vulnerable-to-hacking-83362

Hart, D. V. (2019). Factors influencing the adoption of cybersecurity situational awareness programs [Παράγοντες που επηρεάζουν την εφαρμογή προγραμμάτων ευαισθητοποίησης ως προς την κυβερνοασφάλεια]. *Isaca Journal*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs

Heembrock, M. (2015). The risks of wearable tech in the workplace [Οι κίνδυνοι της τεχνολογίας φορετών συσκευών στον χώρο εργασίας]. *Risk Management Magazine.* https://www.rmmagazine.com/articles/article/2015/02/02/-The-Risks-of-Wearable-Tech-in-the-Workplace-

Hernandez-Castro, J., Cartwright, A. και Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences [Μια οικονομική ανάλυση του λυτρισμικού και των συνεπειών του στην ευημερία]. Royal Society Open Science. 7(3), 190023.

Izuakor, C. (2016). Understanding the impact of cyber security risks on safety [Κατανόηση του αντικτύπου των κινδύνων κυβερνοασφάλειας στην εργασιακή ασφάλεια]. ICISSP 2016 - 2nd International Conference on Information Systems Security and Privacy.

Jansen, J., Junger, M., Kort, J., Leukfeldt, R., Veenstra, S., van Wilsem, J. και van der Zee, S. (2017). Victims [Θύματα]. Σε R. Leukfeldt (επιμ.), *Research agenda. The human factor in cybercrime and cybersecurity* [Ο ανθρώπινος παράγοντας στο κυβερνοέγκλημα και στην κυβερνοασφάλεια], Eleven International Publishing.

Kavallieratos, G., Katsikas, S. και Gkioulos, V. (2020). Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey [Συνεργασία των κυβερνοφυσικών συστημάτων στους τομείς της κυβερνοασφάλειας και της εργασιακής ασφάλειας–Μια ολοκληρωμένη έρευνα]. *Future Internet*. *12*(4), 65.

Korfmacher, S. (2019). The relevance of cybersecurity for functional safety and HCI [Η σημασία της κυβερνοασφάλειας για τη λειτουργική ασφάλεια και την HCI]. Σε V. Duffy (επιμ.), *Digital human modeling and applications in health, safety, ergonomics and risk management human body and motion HCII 2019 lecture notes in computer science*. 11581 Springer.

Loukas, G. (Νοέμβριος 2019). Cyber-physical security threats to Occupational Safety and Health (OSH) in Industry 4.0 [Κυβερνοφυσικές απειλές για την επαγγελματική ασφάλεια και υγεία (ΕΑΥ) στη Βιομηχανία 4.0]. https://www.safe-machines-at-work.org/fileadmin/user_upload/pdf/LOUKAS.pdf

Martin, G., Martin, P., Hankin, C., Darzi, A. και Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? [Κυβερνοασφάλεια και υγειονομική περίθαλψη: Πόσο ασφαλείς είμαστε;] British Medical Journal (εκδ. Clinical research), 358, j3179.

McGuire, M. και Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications [Κυβερνοέγκλημα: Επισκόπηση των στοιχείων. Περίληψη των βασικών πορισμάτων και επιπτώσεων] (Home Office Research Report, 75). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Muthuppalaniappan, M., και Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health [Κυβερνοεπιθέσεις στην υγειονομική περίθαλψη και πανδημία COVID-19: Μια επείγουσα απειλή για την παγκόσμια υγεία]. *International Journal for Quality in Health Care*, *33*(1).

Notar, C. E., Padgett, S. και Roden, J. (2013). Cyberbullying: A review of the literature [Διαδικτυακός εκφοβισμός: Βιβλιογραφική επισκόπηση]. *Universal Journal of Educational Research, 1*(1), 1–9.

Perales Gómez, Á.L., Fernández Maimó, L., Huertas Celdrán, A., García Clemente, F.J., Gil Pérez, M. και Martínez Pérez, G. (2020). SafeMan: A unified framework to manage cybersecurity and safety in manufacturing industry [SafeMan: Ένα ενιαίο πλαίσιο για τη διαχείριση της κυβερνοασφάλειας και της επαγγελματικής ασφάλειας στη μεταποιητική βιομηχανία]. *Software: Practice and Experience 51(3),* 607–627.

Podgórski, D., Majchrzycka, K., Dąbrowska, A., Gralewicz, G. και Okrasa, M. (2017). Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies [Προς ένα εννοιολογικό πλαίσιο της διαχείρισης κινδύνων ΕΑΥ σε έξυπνα εργασιακά περιβάλλοντα βασιζόμενα στα έξυπνα μέσα ατομικής προστασίας, στην περιβάλλουσα νοημοσύνη και στις

τεχνολογίες του διαδικτύου των πραγμάτων]. *International Journal of Occupational Safety and Ergonomics*, *23*(1), 1–20.

Ponemon. (2021). The impact of ransomware on healthcare during covid-19 and beyond [Ο αντίκτυπος του λυτρισμικού λογισμικού στην υγειονομική περίθαλψη κατά την πανδημία Covid-19 και μετά από αυτήν]. https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

Stacey, N., Ellwood, P., Bradbrook, S., Reynolds, J., Williams, H. και David, L. (2018). *Key trends and drivers of change in information and communication technologies and work location [Βασικές τάσεις και παράγοντες αλλαγής σε σχέση με τις τεχνολογίες των πληροφοριών και επικοινωνιών και τον τόπο εργασίας. Πρόβλεψη των νέων και αναδυόμενων κινδύνων για την επαγγελματική ασφάλεια και υγεία].* Ευρωπαϊκός Οργανισμός για την Ασφάλεια και την Υγεία στην Εργασία. https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

Steijn, W., van der Vorm, J., Luiijf, E., Gallis, R. και van der Beek, D. (6 Σεπτεμβρίου 2016). Emergent risks to workplace safety as a result of IT connections of and between work equipment [Αναδυόμενοι κίνδυνοι για την ασφάλεια στον χώρο εργασίας ως αποτέλεσμα των συνδέσεων ΤΠ και του εργασιακού εξοπλισμού]. *TNO report*.

Taeihagh, A. και Lim, H. S. M. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks [Έλεγχος των αυτόνομων οχημάτων: Αναδυόμενες απαντήσεις για τους κινδύνους όσον αφορά την επαγγελματική ασφάλεια, την ευθύνη, την ιδιωτικότητα, την κυβερνοασφάλεια και τη βιομηχανία]. *Transport Reviews*, 39, 103–128.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis [Διαφορές μεταξύ των φύλων στις τάσεις διαχείρισης της ιδιωτικότητας στους δικτυακούς τόπους κοινωνικής δικτύωσης: Μια μετα-ανάλυση. *Computers in Human Behavior*, 93: 1–12.

Truong, T. C., Diep, Q. B. και Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense [Τεχνητή νοημοσύνη στον κυβερνοχώρο: Επίθεση και άμυνα]. *Symmetry, 12*(3), 410.

Verizon. (2019). 2019 Data breach investigations report. [Έκθεση ερευνών παραβιάσεων δεδομένων 2019]. https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf

Verizon. (2021). 2021 Data breach investigations report. [Έκθεση ερευνών παραβιάσεων δεδομένων 2021] https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

Παγκόσμιο Οικονομικό Φόρουμ. (2021). These are the top cybersecurity challenges of 2021 [Αυτές είναι οι μεγαλύτερες προκλήσεις για την κυβερνοασφάλεια το 2021]. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

Westerlund, M. (2019). The emergence of deepfake technology: A review [Η ανάδυση της τεχνολογίας deepfake: Επισκόπηση]. *Technology Innovation Management Review, 9*(11), 40–53.

Williams, E. J., Hinds, J., και Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace [Διερεύνηση της ευαλωτότητας στο ηλεκτρονικό ψάρεμα στον χώρο εργασίας]. *International Journal of Human-Computer Studies*, 120, 1–13.