ΕΛΛΑΔΑ–ΕΕ
πιο δυνατοί μαζί

Η ΔΗΜΟΚΡΑΤΙΑ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΠΟΧΗ

Κυβερνοασφάλεια

Μια αξιόπιστη και κυβερνοασφαλής Ευρώπη

Γιούχαν **Λεπασάρ**
Εκτελεστικός Διευθυντής του Ευρωπαϊκού Οργανισμού για την Κυβερνοασφάλεια (ENISA)

ΜΙΑ ΑΠΟ ΤΙΣ ΚΟΙΝΩΝΙΚΕΣ ΙΔΕΕΣ που έχουν ασκήσει τη μεγαλύτερη επίδραση στην εξέλιξη της ανθρώπινης ιστορίας είναι η δημοκρατία. Θεσπίστηκε στην αρχαία Ελλάδα με τη συγκρότηση των πόλεων-κρατών, τη διαμόρφωση του πολίτη και της «ελεύθερης πολιτείας» και στο διάβα του χρόνου εξελίχθηκε ώστε να μπορέσει να ανταποκριθεί στις συνθήκες της κάθε εποχής. Ο όρος «κυβερνητική» επινοήθηκε για πρώτη φορά από τον Γάλλο φυσικό Αντρέ-Μαρί Αμπέρ, ο οποίος πρότεινε «η μελλοντική επιστήμη της διακυβέρνησης να ονομαστεί “cybernétique”». Τη δεκαετία του ’40, ο όρος χρησιμοποιήθηκε από τον Νόρμπερτ Βίνερ, ο οποίος ονόμασε «cybernetics» την «επιστήμη του ελέγχου και της επικοινωνίας ζώου και μηχανής». Σε μια δημοκρατική κοινωνία, οφείλει να συμβάλει στην οικοδόμηση εμπιστοσύνης όχι μόνο για ψηφιακές λύσεις, αλλά γενικότερα για την ψηφιακή κοινωνία.

Το διαδίκτυο αυτό καθαυτό αποτελεί ένα μηχανισμό δημιουργίας τεράστιου πλούτου, μια δύναμη ελευθερίας, ανοίγματος, διαφάνειας και καινοτομίας. Ωστόσο, χωρίς την κυβερνοασφάλεια, τα τηλέφωνα και οι υπολογιστές σιωπούν, οι γεννήτριες ακινητοποιούνται, κρίσιμα αγαθά και υπηρεσίες δεν μπορούν να διαδοθούν στους πολίτες. Εάν δεν υπάρχει εμπιστοσύνη στην ακεραιότητα των δεδομένων μας, όπως π.χ. των χρηματοπιστωτικών δεδομένων ή των δεδομένων υγείας, η οικονομία κλονίζεται. Εδώ στην Ελλάδα, τη χώρα που φιλοξενεί τον ENISA, όλο και περισσότερες δημόσιες υπηρεσίες είναι διαθέσιμες μέσω διαδικτύου. Η κυβερνοασφάλεια είναι βασική αρχή για τη διασφάλιση της ανθεκτικότητας αυτών των διαδικτυακών δημόσιων υπηρεσιών.

Το 2020, λόγω της πανδημίας του κορωνοϊού, γίναμε μάρτυρες ενός πρωτόγνωρου ψηφιακού μετασχηματισμού. Την ίδια στιγμή, κακόβουλοι παράγοντες κατάφεραν να προσαρμόσουν άμεσα τις επιθετικές τακτικές τους, ώστε να εκμεταλλευτούν αυτή τη νέα απομακρυσμένη πραγματικότητα. Στην πρώτη καραντίνα καταγράφηκε απότομη αύξηση στις απάτες μέσω εταιρικού ηλεκτρονικού ταχυδρομείου, στις επιθέσεις με θέμα τον κορωνοϊό, στις απάτες που σχετίζονται με ηλεκτρονικές αγορές και στις επιθέσεις μέσω αυτόματης συμπλήρωσης διαπιστευτηρίων.

Στη διάρκεια της πανδημίας βρήκαν γόνιμο έδαφος επιθέσεις μέσω κοινωνικής μηχανικής για την κλοπή στοιχείων των χρηστών, όπως διαπιστευτηρίων σύνδεσης, πληροφοριών πιστωτικών καρτών ή ακόμη και χρημάτων. Αξίζει να σημειωθεί ότι, στους πρώτους μήνες της πανδημίας, η εξελισσόμενη ψηφιακή επανάσταση επηρεάζει τον τρόπο λειτουργίας της κοινωνίας και της δημοκρατίας μας. Βιώνουμε μεγάλο μέρος της πραγματικότητας πλέον μέσα από αναρτήσεις στα κοινωνικά δίκτυα και συχνά εισπνέουμε μια εικόνα διαστρεβλωμένη, ψεύτικη, ύποπτη. Μια εικόνα τόσο απλοϊκή, που φαντάζει πιστευτή, ή τόσο εντυπωσιακή, που μαζεύει χιλιάδες like και retweet, απέναντι σε μια αλήθεια που καλείται να δώσει την άνιση μάχη για το αυτονόητο: πίστευε μεν, ερεύνα δε.

Η Αντιπροσωπεία της Ευρωπαϊκής Επιτροπής στην Ελλάδα, με τη Realnews και σε συνεργασία με το Democracy & Culture Foundation κηρύττουν τον πόλεμο στην παραπληροφόρηση και ανοίγουν μια δημόσια συζήτηση περί «Δημοκρατίας στην ψηφιακή εποχή» με τέσσερα διαδοχικά αφιερώματα από τις 9 έως τις 30 Μαΐου.

Γιώργος Μοσχόβης -
Αν. Επικεφαλής της Αντιπροσωπείας της Ευρωπαϊκής Επιτροπής στην Ελλάδα

Η κυβερνοασφάλεια είναι ευθύνη όλων μας

Κωνσταντίνος **Ζανετόπουλος**
Senior Manager στην Accenture

ΤΟΝ ΤΕΛΕΥΤΑΙΟ ΧΡΟΝΟ, η τηλεργασία έχει θέσει ενώπιον πολλαπλών προκλήσεων την παρακολούθηση της ασφάλειας των επιχειρήσεων, από τις πλατφόρμες που χρησιμοποιούνται για την επικοινωνία έως τις συσκευές και τα δίκτυα μέσω των οποίων μεταδίδονται τα δεδομένα. Οι περισσότερες επιχειρήσεις σε όλο τον κόσμο αναγκάστηκαν να περάσουν γρήγορα στην τηλεργασία. Κάποιες το έπραξαν σύμφωνα με συγκεκριμένο σχέδιο, άλλες αντέδρασαν, αλλά όχι σύμφωνα με το σχέδιό τους, ενώ ακόμη περισσότερες δεν διέθεταν καν σχέδιο.

Οι ευκαιρίες για κοινωνική μηχανική αυξάνονται, καθώς η κυβερνοκατασκοπεία και ομάδες κυβερνοεγκλήματος προσπαθούν να εκμεταλλευτούν ευάλωτους υπαλλήλους που δεν είναι εξοικειωμένοι με τη διαχείριση των τεχνολογικών περιβαλλόντων εργασίας τους. Οι παγκόσμιοι οικονομικοί και επιχειρηματικοί κλυδωνισμοί έχουν θέσει επιχειρήσεις και κυβερνήσεις ενώπιον τεράστιων οικονομικών προκλήσεων. Οι πιέσεις αυτές αναπόφευκτα μεταφράζονται σε μέτρα για την ασφάλεια των πληροφοριών, ώστε να διατηρηθεί ή να αυξηθεί η κάλυψη, υπό διαρκώς σφιχτότερους δημοσιονομικούς περιορισμούς.

Οι κυβερνοεγκληματίες εργάζονται, συχνότερα από ό,τι στο παρελθόν, για να αποκομίσουν κέρδη από την πρόσβαση σε δεδομένα και δίκτυα, καθώς η οικονομία γίνεται ολοένα και πιο ψηφιακή, αλλά και πιο ευάλωτη.

Εν τω μεταξύ, οι παράγοντες κυβερνοαπειλών βρίσκουν νέους τρόπους να πείσουν τα θύματά τους να πληρώσουν. Τον Νοέμβριο του 2019, το νέο, εξελιγμένο στέλεχος λυτρισμικού Maze μόλυνε μια μεγάλη εταιρεία προσωπικού ασφαλείας, έκλεψε δεδομένα της, ειδοποίησε τα μέσα ενημέρωσης και τελικά, όταν δεν πληρώθηκαν τα λύτρα, δημοσιοποίησε 700 MB δεδομένων. Αυτή η προσέγγιση «κατονομασίας και στιγματισμού» ασκεί επιπλέον πίεση στα θύματα να πληρώσουν, παρόλο που οι Αρχές επιβολής του νόμου και ο κλάδος της κυβερνοασφάλειας ανέκαθεν συνιστούσαν να μην πληρώνονται λύτρα. Αξίζει να σημειωθεί ότι στο δεύτερο τρίμηνο του 2020 το μέσο ποσό των καταβαλλόμενων λύτρων διαμορφώθηκε περίπου στα 180.000 δολάρια ΗΠΑ, αυξημένο κατά 60 % σε σχέση με το πρώτο τρίμηνο του 2020. Η κατάσταση μπορεί να επιδεινωθεί ακόμη περισσότερο, καθώς αυξάνονται τα κέρδη που αποκομίζουν οι παράγοντες απειλής, με αποτέλεσμα να μπορούν να καινοτομήσουν και να επενδύσουν σε πιο προηγμένα λυτρισμικά και να εκμεταλλευτούν τις μεγαλύτερες τρωτότητες της τηλεργασίας.

Η Accenture πιστεύει ότι στο μέλλον οι παράγοντες απειλής που χρησιμοποιούν αυτές τις τακτικές θα συνεχίσουν να εξελίσσονται και να πολλαπλασιάζονται.

Οι επιχειρήσεις χρησιμοποιούν όλο και περισσότερες συσκευές με κενά ασφαλείας ή που δεν έχουν δοκιμαστεί και οι οποίες αποτελούν πολύ πιο εύκολο στόχο για δυνητικούς δράστες επιθέσεων. Οι συσκευές που συνδέονται σε υπολογιστικά νέφη και στο διαδίκτυο γνωρίζουν μεγάλη διάδοση. Οι πρωτοπόροι της κυβερνοασφάλειας αντεπιτίθενται χρησιμοποιώντας προγράμματα επικήρυξης σφαλμάτων («bug bounty») και πλαίσια ανίχνευσης, αλλά οι απειλές κατά των τεχνολογιών παραγωγικών λειτουργικών («ΟΤ») καθιστούν αναγκαία τη βελτίωση της αποτελεσματικότητας των ελέγχων ασφαλείας. Οι δοκιμές ασφαλείας πολλές φορές είναι δαπανηρές. Είναι δύσκολο να εκτιμηθεί ο κίνδυνος που ενέχει η κάθε συσκευή, καθώς οι διαφορές στις δοκιμές ασφαλείας μεταξύ των συσκευών μικρών και μεγάλων κατασκευαστών είναι τεράστιες. Αργά αλλά σταθερά, οι πωλητές εντοπίζουν και αντιμετωπίζουν τις απειλές με ενημερώσεις ασφαλείας. Με την έλευση των τεχνολογιών 5G, ο πολλαπλασιασμός των συσκευών του διαδικτύου των πραγμάτων καθιστά τις προκλήσεις ακόμη μεγαλύτερες. Οι πρωτοπόροι της κυβερνοασφάλειας πρέπει να μοιραστούν τις γνώσεις τους και να αναπτύξουν τυποποιημένα συστήματα που να είναι απλά και εύκολο να ενσωματωθούν.

Ο κορωνοϊός επιταχύνει την ανάγκη για μια νέα προσέγγιση ασφαλείας. Η Accenture έχει εντοπίσει τέσσερα στοιχεία:

- Ασφαλής νοοτροπία. Ο ανθρώπινος παράγοντας είναι πολύ σημαντικός για την οικοδόμηση ενός ασφαλούς και προστατευμένου περιβάλλοντος.
- Ασφαλής πρόσβαση στο δίκτυο μέσω συνεχών δοκιμών παρείσφρυσης και αναβάθμισης των πληροφοριών για απειλές.
- Ασφαλή εργασιακά περιβάλλοντα μέσω της αναβάθμισης των υποδομών των επιχειρήσεων και της μόχλευσης των ικανοτήτων υπολογιστικού νέφους.
- Ασφαλής συνεργασία, όπου οι ομάδες διαθέτουν εργαλεία για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας.

Η πανδημία άνοιξε τον δρόμο σε καιροσκοπικές απειλές, καθώς δημιούργησε ευκαιρίες κοινωνικής μηχανικής, όπως νέες εκστρατείες ηλεκτρονικού ψαρέματος. Καθώς τα δεδομένα παραμένουν ένα περιζήτητο εμπόρευμα υψηλής αξίας, οι πρωτοπόροι της κυβερνοασφάλειας θα πρέπει να εξετάσουν το ενδεχόμενο να υιοθετήσουν την προσαρμόσιμη ασφάλεια, θέτοντας σε εφαρμογή κατάλληλους ελέγχους και παρακολούθηση, ώστε να συμβάλουν στη δημιουργία ενός ασφαλούς και προστατευμένου εργασιακού περιβάλλοντος για την επιχείρησή τους.

Οι κυβερνητικοί οργανισμοί σε όλα τα επίπεδα θα πρέπει να συνεχίσουν να συνεργάζονται με τον ιδιωτικό τομέα, την κοινωνία των πολιτών και τους ιδιώτες, ώστε να προγραμματίσουν, να προετοιμαστούν και να εξασκηθούν με στόχο την ενίσχυση της ανθεκτικότητας της κυβερνοασφάλειας, υποστηριζόμενοι από τους κατάλληλους πόρους και επενδύσεις. Η Accenture πιστεύει η ανθεκτικότητα της κυβερνοασφάλειας μπορεί να επιτευχθεί μέσω μιας πολυδιάστατης στρατηγικής διαχείρισης κρίσεων, με πολλαπλές ροές εργασίας και ομάδες που συνεργάζονται στενά, συχνά σε καθημερινή βάση, και ότι μια τέτοια στρατηγική μπορεί να συμβάλει στην προστασία του κράτους, των πολιτών και των επιχειρήσεων.

Σε συνεργασία με
THE DEMOCRACY & CULTURE FOUNDATION
ΔΙΟΡΓΑΝΩΤΗΣ ΤΟΥ ATHENS DEMOCRACY FORUM