Κυβερνοασφάλεια

Εισαγωγή στην Κυβερνοασφάλεια

Φαντάσου το Διαδίκτυο σαν μια τεράστια, αχανή πόλη. Όπως σε κάθε μεγάλη πόλη, υπάρχουν υπέροχα μέρη για να επισκεφτείς, βιβλιοθήκες με ατελείωτη γνώση και πλατείες για να συναντήσεις φίλους. Δυστυχώς, όμως, υπάρχουν και γειτονιές όπου παραμονεύουν επιτήδειοι, έτοιμοι να εκμεταλλευτούν την απροσεξία μας. **Κυβερνοασφάλεια** είναι όλα εκείνα τα μέτρα που παίρνουμε για να προστατεύσουμε τον εαυτό μας, το «σπίτι» μας (τον υπολογιστή, το κινητό) και τα «υπάρχοντά» μας (τα δεδομένα, τις φωτογραφίες, τους κωδικούς) ενώ περιηγούμαστε σε αυτή την ψηφιακή πόλη.

Οι τρεις θεμελιώδεις στόχοι της κυβερνοασφάλειας παραμένουν ίδιοι, όπως σωστά αναφέρει το βιβλίο σου, και τους λέμε και **τριάδα CIA**:

- **Εμπιστευτικότητα (Confidentiality):** Μόνο εσύ και όποιος εσύ επιτρέπεις μπορείτε να βλέπετε τα μηνύματα και τα αρχεία σου. Είναι σαν να στέλνεις ένα γράμμα σε έναν φίλο μέσα σε κλειστό φάκελο, και όχι σε ανοιχτή κάρτα.
- **Ακεραιότητα (Integrity):** Σημαίνει ότι τα δεδομένα σου είναι ακέραια και δεν έχουν αλλοιωθεί στην πορεία. Είναι σαν να στέλνεις μια φωτογραφία και ο φίλος σου να την βλέπει ακριβώς όπως την τράβηξες, χωρίς κάποιος να έχει ζωγραφίσει πάνω της.
- **Διαθεσιμότητα (Availability):** Όταν θέλεις να έχεις πρόσβαση σε ένα αρχείο σου ή σε μια υπηρεσία (π.χ. να μπεις στο e-mail σου), αυτή να είναι διαθέσιμη και να λειτουργεί. Σαν να θέλεις να ανοίξεις την ντουλάπα σου και να μην είναι σφηνωμένη η πόρτα.

---

1. Έννοιες-Κλειδιά: Αγαθό, Απειλή, Ζημία

Το βιβλίο σου εισάγει τρεις πολύ βασικές έννοιες. Ας τις δούμε με σύγχρονα παραδείγματα:

- **Αγαθό (Asset):** Είναι **οτιδήποτε έχει αξία για εσένα** και θες να προστατεύσεις.
  - *Παραδείγματα:* Ο προσωπικός σου υπολογιστής, το κινητό τηλέφωνο, οι οικογενειακές φωτογραφίες, τα βίντεο από τις διακοπές, οι κωδικοί για τα social media (Instagram, TikTok), ο λογαριασμός σου σε ένα online παιχνίδι, ακόμα και η ίδια σου η "ψηφιακή φήμη".
- **Απειλή (Threat):** Είναι **οτιδήποτε μπορεί να προκαλέσει ζημιά** στο «αγαθό» σου.
  - *Παραδείγματα:* Ένας ιός, ένα μήνυμα ηλεκτρονικού "ψαρέματος" (phishing) που προσπαθεί να σου κλέψει τον κωδικό, ένας χάκερ, αλλά και μια φυσική καταστροφή (π.χ. πτώση του κινητού στο νερό) ή μια διακοπή ρεύματος.
- **Ζημία (Harm):** Είναι η **πραγματική συνέπεια** αν μία απειλή γίνει πραγματικότητα.
  - *Παραδείγματα:* Να χάσεις όλες σου τις φωτογραφίες γιατί έσπασε το κινητό σου, να σου "κλέψουν" τον λογαριασμό στο παιχνίδι, να διαρρεύσουν προσωπικά σου μηνύματα ή να κολλήσει ο υπολογιστής του σπιτιού έναν ιό και να γίνει πιο αργός.

---

2. Μέτρα Ασφάλειας σε Επίπεδο Υπολογιστή & Κινητού

Εδώ το βιβλίο σου έχει πολύ σωστές βάσεις, αλλά η τεχνολογία προχωράει. Ας δούμε τι ισχύει σήμερα:

1. **Ενημερώσεις Λογισμικού (Software Updates):** Το βιβλίο σωστά αναφέρει τις ενημερώσεις του λειτουργικού. Σήμερα, είναι πιο κρίσιμες από ποτέ. Δεν φέρνουν μόνο νέες λειτουργίες, αλλά κλείνουν «τρύπες ασφαλείας» που ανακαλύπτονται συνεχώς.

    - **Σύγχρονο παράδειγμα:** Το 2025, η Microsoft σταμάτησε την υποστήριξη των Windows 10 . Αν κάποιος συνεχίσει να χρησιμοποιεί Windows 10 χωρίς να πληρώσει για **Εκτεταμένες Ενημερώσεις Ασφαλείας (ESU)** ή χωρίς να αναβαθμίσει σε Windows 11, ο υπολογιστής του γίνεται πολύ πιο ευάλωτος σε νέες επιθέσεις, γιατί δεν θα διορθώνονται πια τα κενά ασφαλείας που ανακαλύπτονται . Το ίδιο ισχύει για το κινητό σου: πρέπει να το ενημερώνεις πάντα στην τελευταία έκδοση!
2. **Αντιικό Λογισμικό (Antivirus):** Παραμένει απαραίτητο, αλλά πια δεν είναι η μοναδική άμυνα. Τα σύγχρονα προγράμματα προστατεύουν από ένα τεράστιο φάσμα απειλών:
    - **Ransomware:** Είναι σαν να μπαίνει κάποιος στο σπίτι σου και να κλειδώνει όλα τα δωμάτια, ζητώντας λύτρα για να σου δώσει τα κλειδιά . Σήμερα, οι επιθέσεις αυτές στοχεύουν ακόμα και σπίτια, όχι μόνο εταιρείες.
    - **Malvertising:** Είναι κακόβουλες διαφημίσεις. Μπορεί να σου εμφανιστεί μια διαφήμιση που υπόσχεται δωρεάν diamonds για ένα παιχνίδι, αλλά κρύβει έναν ιό.
3. **Τείχος Προστασίας (Firewall):** Λειτουργεί σαν ένας αυστηρός πορτιέρης που ελέγχει ποια δεδομένα μπαίνουν και βγαίνουν από τον υπολογιστή σου. Είναι πλέον ενεργοποιημένο από προεπιλογή σε όλα τα λειτουργικά συστήματα.

---

3. Μέτρα Ασφάλειας σε Επίπεδο Δικτύου & Υπηρεσιών

Εδώ μπαίνουμε στην καρδιά της σύγχρονης προστασίας, ειδικά τώρα που όλοι είμαστε συνδεδεμένοι.

1. **Ασφαλή Πρωτόκολλα (HTTPS, SSL/TLS):** Το βιβλίο αναφέρει τη μετάβαση από **http** σε **https**. Το "s" σημαίνει "ασφαλές" (secure). Σήμερα, το βλέπεις παντού. Η τεχνολογία πίσω από αυτό ονομάζεται **SSL/TLS** και δημιουργεί ένα κρυφό, προστατευμένο τούνελ για τα δεδομένα σου, ώστε κανείς να μην μπορεί να τα υποκλέψει . Για αυτό, όταν μπαίνεις στο gov.gr ή στο e-banking σου, βλέπεις πάντα HTTPS.
2. **Ταυτοποίηση Δύο Παραγόντων (2FA) - OTP:** Το βιβλίο αναφέρει το **OTP (One Time Password)**. Αυτή είναι μια από τις σημαντικότερες σύγχρονες συνήθειες ασφαλείας. Ακόμα κι αν κάποιος μάθει τον κωδικό σου, δεν μπορεί να μπει στον λογαριασμό σου, γιατί θα χρειαστεί και έναν μοναδικό κωδικό που στέλνεται στο κινητό σου. Χρησιμοποίησέ το παντού: Instagram, TikTok, e-mail, τράπεζες.
3. **Εθνική Στρατηγική και Νέοι Νόμοι:** Σήμερα, η κυβερνοασφάλεια είναι τόσο σημαντική που οι χώρες φτιάχνουν ολόκληρες στρατηγικές γι' αυτήν. Η Ελλάδα, για παράδειγμα, έχει την **Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030** και μια ειδική αρχή, την **Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ)** . Αυτό δείχνει πόσο σοβαρά αντιμετωπίζεται πια το θέμα, με στόχο την προστασία κρίσιμων υποδομών όπως τα νοσοκομεία, οι τράπεζες και τα δίκτυα ενέργειας από επιθέσεις .

---

4. Κρυπτογράφηση: Η Μαγεία της Ασφάλειας

Το βιβλίο σου εξηγεί τέλεια τη διαφορά. Απλά να θυμάσαι:

- **Συμμετρική Κρυπτογράφηση:** Ένα κλειδί για να κλειδώσεις και να ξεκλειδώσεις. Σαν το συρτάρι του γραφείου σου. Το πρόβλημα; Πώς θα στείλεις με ασφάλεια αυτό το κλειδί στον φίλο σου;

- **Ασύμμετρη Κρυπτογράφηση (ή Κρυπτογράφηση Δημοσίου Κλειδιού):** Εδώ λύνεται το πρόβλημα. Χρησιμοποιείς δύο κλειδιά: ένα **Δημόσιο** (που μπορείς να το στείλεις σε όλο τον κόσμο, σαν μια ανοιχτή κλειδαριά) και ένα **Ιδιωτικό** (που το κρατάς μυστικό, σαν το μοναδικό κλειδί που ξεκλειδώνει αυτήν την κλειδαριά).
    - **Πώς λειτουργεί:** Θέλεις να σου στείλω ένα μυστικό μήνυμα. Εσύ μου δίνεις πρώτα την ανοιχτή σου κλειδαριά (το δημόσιο κλειδί). Εγώ κλειδώνω το μήνυμα σε ένα κουτί με αυτήν και στο στέλνω. Μόνο εσύ, με το δικό σου μυστικό κλειδί (το ιδιωτικό), μπορείς να το ανοίξεις .
    - Το βιβλίο αναφέρει τον αλγόριθμο **RSA**, που είναι ο πιο διάσημος για αυτή τη δουλειά.

---

5. Ψηφιακά Πιστοποιητικά και Υπογραφές

- **Ψηφιακό Πιστοποιητικό:** Σκέψου το σαν μια **ταυτότητα** ή ένα **διαβατήριο** για έναν ιστότοπο. Εκδίδεται από μια επίσημη, αξιόπιστη Αρχή (π.χ. η Αρχή Πιστοποίησης Ελληνικού Δημοσίου) και βεβαιώνει ότι "αυτό το site (π.χ. της τράπεζάς σου) είναι γνήσιο και δεν είναι απάτη" .
- **Ψηφιακή Υπογραφή:** Είναι σαν την κανονική σου υπογραφή, αλλά σε ψηφιακή μορφή. Είναι μοναδική και εξασφαλίζει ότι ένα έγγραφο που στέλνεις (π.χ. μια υπεύθυνη δήλωση) προέρχεται πράγματι από εσένα και δεν άλλαξε στην πορεία. Βασίζεται στην ασύμμετρη κρυπτογράφηση.

---

6. Σύγχρονες Τεχνολογίες: Πέρα από το Βιβλίο

Το βιβλίο σου κλείνει με μια μικρή αναφορά στο Blockchain. Ας το δούμε λίγο πιο αναλυτικά, καθώς είναι η βάση για τα κρυπτονομίσματα.

- **Τεχνολογία Blockchain:** Φαντάσου ένα **ψηφιακό καθολικό (βιβλίο καταγραφής)** όπου κάθε σελίδα είναι ένα "μπλοκ". Αυτό το βιβλίο, όμως, δεν βρίσκεται σε ένα μέρος, αλλά υπάρχουν χιλιάδες πανομοιότυπα αντίγραφά του σε χιλιάδες υπολογιστές σε όλο τον κόσμο. Κάθε φορά που γίνεται μια νέα συναλλαγή (π.χ. αγορά ενός Bitcoin), γράφεται σε μια καινούρια σελίδα. Για να προστεθεί αυτή η σελίδα, όλοι οι υπολογιστές πρέπει να συμφωνήσουν ότι είναι σωστή. Αν κάποιος προσπαθήσει να αλλάξει μια παλιά σελίδα, θα πρέπει να την αλλάξει σε όλα τα αντίγραφα ταυτόχρονα, κάτι που είναι πρακτικά αδύνατο. Αυτό κάνει το Blockchain εξαιρετικά ασφαλές και διαφανές .

Συμπέρασμα & Συμβουλές για την Ψηφιακή σου Ζωή

Όπως λέει και η Εθνική Αρχή Κυβερνοασφάλειας, η βασική οδηγία είναι: **«Παραμένετε πάντα υποψιασμένοι όσο είστε συνδεδεμένοι σε δίκτυα»** .

Τρεις χρυσοί κανόνες για σένα:

1. **Σκέψου πριν κάνεις κλικ:** Μην ανοίγεις περίεργα links, ακόμα κι αν σου τα στείλει "φίλος" (μπορεί να τον έχουν χακάρει).
2. **Προστάτεψε τους κωδικούς σου:** Χρησιμοποίησε διαφορετικούς κωδικούς για κάθε λογαριασμό και ενεργοποίησε την **επιβεβαίωση δύο παραγόντων (2FA)** παντού.
3. **Ενημέρωσε τις συσκευές σου:** Ναι, είναι βαρετό, αλλά οι ενημερώσεις σε κρατάνε ασφαλή από τους τελευταίους ιούς.

Η τεχνολογία εξελίσσεται, αλλά η βασική αρχή παραμένει: η ασφάλεια εξαρτάται περισσότερο από τις δικές σου συνήθειες παρά από τα εργαλεία που χρησιμοποιείς