

Κλοπή ταυτότητας και χάκερ

- Διαδικτυακό έγκλημα
- Εγκληματίες του διαδικτύου
- Κοινές κατηγορίες διαδικτυακών εγκλημάτων

Χρόνος	Επίπεδος
2008	5,9K
2009	11,9K
2010	16,8K
2011	29,9K
2012	41,7K
2013	42,8K
2014	45,5K
2015	61,2K
2016	67,1K

Κλοπή ταυτότητας και χάκερ

Κλοπή ταυτότητας (Στόχος 9.1)

- Σημειώνεται όταν κάποιος κλέβει προσωπικές πληροφορίες και παρουσιάζεται ως κάποιος άλλος
 - Το πιο επισφαλές οικονομικά διαδικτυακό έγκλημα για τα θύματά του
- Είδη απάτης
 - Παραχάραξη πιστωτικών και χρεωστικών καρτών
 - Αίτηση για αλλαγή διεύθυνσης στην τράπεζά σας
 - Άνοιγμα νέων πιστωτικών καρτών
 - Λήψη ιατρικών υπηρεσιών
 - Αγορά σπιτιού

Κλοπή ταυτότητας και χάκερ

Χάκερ (1 από 4) (Στόχος 9.2)

- Χάκερ θεωρείται γενικά οποιοσδήποτε εισβάλλει παράνομα σε ένα σύστημα υπολογιστή
- Είδη χάκερ
 - Χάκερ με τα λευκά καπέλα (ηθικοί χάκερ)
 - Χάκερ με τα μαύρα καπέλα
 - Χάκερ με τα γκρι καπέλα
- Πρόγραμμα ανάλυσης πακέτων (sniffer)
- Keylogger

Κλοπή ταυτότητας και χάκερ

Χάκερ (2 από 4) (Στόχος 9.2)

- Οι Δούρειοι ίπποι φαίνονται χρήσιμοι αλλά λειτουργούν κακόβουλα
- Οι κερκόπορτες και τα rootkit δίνουν στους χάκερ τη δυνατότητα να προσπελαίνουν τον υπολογιστή σας
- Τα ζόμπι είναι υπολογιστές που ελέγχονται από χάκερ

Κλοπή ταυτότητας και χάκερ

Χάκερ (3 από 4) (Στόχος 9.2)

- Άρνηση εξυπηρέτησης
 - Οι νόμιμοι χρήστες αποκλείονται από την πρόσβαση σε ένα σύστημα υπολογιστή
 - Ο υπολογιστής τερματίζει τη λειτουργία του
- Κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS)
- Botnet (μια μεγάλη ομάδα προγραμμάτων λογισμικού που εκτελούνται αυτόνομα σε υπολογιστές ζόμπι)

Κλοπή ταυτότητας και χάκερ

Χάκερ (4 από 4) (Στόχος 9.2)

- Πακέτα εκμετάλλευσης - προγράμματα λογισμικού τα οποία εκτελούνται σε διακομιστές και αναζητούν ευπαθή σημεία των υπολογιστών
- Οι λογικές θύρες (logical port) είναι εικονικές – όχι φυσικές– πύλες επικοινωνίας ή διαδρομές

Ιοί υπολογιστών

Τα βασικά για τους ιούς (Στόχος 9.3)

- Πρόγραμμα υπολογιστή που προσκολλάται σε κάποιο άλλο προσπαθώντας να εξαπλωθεί σε άλλους υπολογιστές
- Ο κύριος σκοπός ενός ιού είναι να αντιγράψει τον εαυτό του και τον κώδικά του σε όσο το δυνατόν περισσότερα αρχεία φιλοξενίας
- Οι δευτερεύοντες στόχοι του μπορεί να είναι καταστροφικοί
- Τα smartphone, τα tablet και άλλες συσκευές μπορούν επίσης να μολυνθούν από ιούς

Ιοί υπολογιστών

Τύποι ιών (1 από 2) (Στόχος 9.4)

- Ιοί τομέα εκκίνησης
- Βόμβες λογικής και ωρολογιακές βόμβες
- Σκουλήκια
- Ιοί δέσμης ενεργειών και ιοί μακροεντολών
- Ιοί ηλεκτρονικού ταχυδρομείου
- Ιοί κρυπτογράφησης



Ιοί υπολογιστών

Τύποι ιών (2 από 2) (Στόχος 9.4)

- Ταξινόμηση με βάση τις μεθόδους που χρησιμοποιούν έτσι ώστε να αποφύγουν τον εντοπισμό τους
 - Οι πολυμορφικοί ιοί τροποποιούν τον κώδικά τους ή τον ξαναγράφουν σε τακτά διαστήματα, έτσι ώστε να αποφύγει τον εντοπισμό
 - Οι πολυμερείς ιοί έχουν σχεδιαστεί έτσι ώστε να μολύνουν πολλούς τύπους αρχείων
 - Οι άορατοι ιοί διαγράφουν προσωρινά τον κώδικά τους από τα αρχεία στα οποία εδρεύουν και στη συνέχεια κρύβονται στην ενεργή μνήμη του υπολογιστή

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

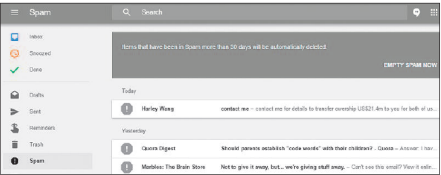
Διαδικτυακές οχλήσεις (1 από 3) (Στόχος 9.5)

- Το κακόβουλο λογισμικό έχει κακές προθέσεις
 - Το adware προβάλλει χορηγούμενες διαφημίσεις
 - Το spyware είναι ένα ανεπιθύμητο πρόγραμμα
 - Μεταδίδει πληροφορίες
 - Χρησιμοποιεί cookie παρακολούθησης
 - Ένα πρόγραμμα keylogger παρακολουθεί όσα πληκτρολογούν οι χρήστες
- Υπάρχουν πολλά προγράμματα προστασίας από spyware

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Διαδικτυακές οχλήσεις (2 από 3) (Στόχος 9.5)

- Spam (ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου)
- Τακτικές ελαχιστοποίησης των spam (φίλτρο spam)



Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Διαδικτυακές οχλήσεις (3 από 3) (Στόχος 9.5)

- Τα cookie είναι μικρά αρχεία κειμένου τα οποία αποθηκεύουν αυτόματα στον σκληρό σας δίσκο ορισμένους διαδικτυακούς τόπους όταν τους επισκέπτεστε
- Βοηθούν τις εταιρείες να καθορίσουν την αποτελεσματικότητα της στρατηγικής μάρκετινγκ που υιοθετούν
- Δεν αναζητούν προσωπικές πληροφορίες στον σκληρό σας δίσκο
- Μπορεί να παραβιάσουν την ιδιωτικότητα σας
- Δεν αποτελούν απειλή για την ασφάλεια

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

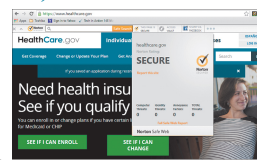
Κοινωνική μηχανική (1 από 3) (Στόχος 9.6)

- Κοινωνική μηχανική είναι οποιαδήποτε τεχνική χρησιμοποιεί κοινωνικές δεξιότητες προκειμένου να δημιουργήσει μια ανθρώπινη αλληλεπίδραση
 - Παρακινεί τα εμπλεκόμενα άτομα να αποκαλύψουν ευαίσθητες πληροφορίες
- Το pretexting περιλαμβάνει τη δημιουργία ενός σεναρίου το οποίο ακούγεται απολύτως νομότυπο

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Κοινωνική μηχανική (2 από 3) (Στόχος 9.6)

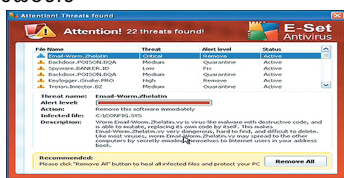
- Phishing (ψάρεμα)
 - Δελεάζει τους χρήστες ώστε να αποκαλύπτουν προσωπικές πληροφορίες
- Pharming
 - Ένας κακόβουλος κώδικας εισβάλλει στον υπολογιστή για να συλλέξει πληροφορίες
- Οδηγίες για να αποφύγετε αυτά τα συστήματα



Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Κοινωνική μηχανική (3 από 3) (Στόχος 9.6)

- Scareware
 - Είδος κακόβουλου λογισμικού
 - Προσπαθεί να σας πείσει ότι υπάρχει κάποιο πρόβλημα... και να πληρώσετε για να το διορθώσετε



Προστασία της ψηφιακής ιδιοκτησίας

- Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας
- Διατηρήστε τα δεδομένα σας ασφαλή
- Προστασία των φυσικών ψηφιακών πόρων σας

Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Στόχοι

- 9.7 Τι είναι το τείχος προστασίας και πώς προστατεύει τον υπολογιστή σας από χάκερ.
- 9.8 Προστασία υπολογιστή από μόλυνση από ιό.
- 9.9 Χρήση κωδικών πρόσβασης και βιομετρικών χαρακτηριστικών για αυθεντικοποίηση χρήστη.
- 9.10 Τρόποι ανώνυμης περιήγησης στο web.

Διατηρήστε τα δεδομένα σας ασφαλή

Στόχοι

- 9.11 Τύποι πληροφοριών που δεν πρέπει να κοινοποιείτε ποτέ στο διαδίκτυο.
- 9.12 Διάφοροι τύποι αντιγράφων ασφαλείας στις ψηφιακές συσκευές σας και τα διάφορα μέρη όπου μπορείτε να αποθηκεύετε αντίγραφα ασφαλείας.

Προστασία των φυσικών ψηφιακών πόρων σας

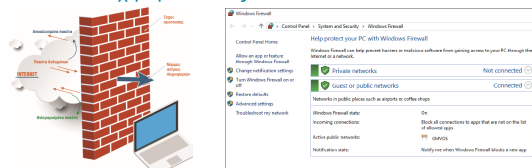
Στόχοι

- 9.13 Αρνητικές επιπτώσεις που μπορεί να έχουν το περιβάλλον και οι αυξομειώσεις της τάσης του ρεύματος σε ψηφιακές συσκευές.
- 9.14 Οι κυριότερες ανησυχίες που προκύπτουν από την κλοπή μιας συσκευής και στρατηγικές επίλυσης των προβλημάτων.

Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Τείχη προστασίας (1 από 2) (Στόχος 9.7)

- Τείχος προστασίας - πρόγραμμα λογισμικού ή συσκευή υλικού
- Τα Windows και το macOS περιλαμβάνουν αξιόπιστα τείχη προστασίας
- Τα πακέτα λογισμικού για την ασφάλεια του υπολογιστή σας διαθέτουν τείχη προστασίας



Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Τείχη προστασίας (2 από 2) (Στόχος 9.7)

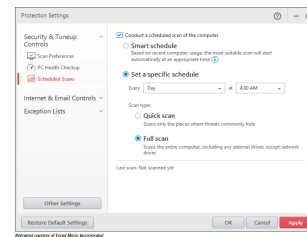
- Φιλτράρισμα πακέτων
 - Φιλτράρει τα πακέτα που αποστέλλονται σε συγκεκριμένες λογικές θύρες
- Αποκλεισμός λογικής θύρας
 - Αγνοεί το αίτημα που προέρχεται από το διαδίκτυο και ζητά πρόσβαση σε ορισμένες θύρες

Συνήθεις λογικές θύρες	
Αριθμός θύρας	Πρωτόκολλο χρήσης της θύρας
21	FTP (πρωτόκολλο μεταφοράς αρχείων)
23	Telnet (βηματοκομίες γραμμής κρυπτογράφησης κειμένου)
25	SMTP (πρωτόκολλο μεταφοράς μηνυμάτων ηλεκτρονικού ταχυδρομείου)
53	DNS (σύστημα ονομάτων τομέα)
80	HTTP (πρωτόκολλο μεταφοράς υπερκειμένου)
443	HTTPS (HTTP με κρυπτογράφηση ασφαλείας μεταφοράς επίπεδου [TLS])

Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Αποτροπή μολύνσεων από ιούς (1 από 2) (Στόχος 9.8)

- Λογισμικό προστασίας από ιούς
 - Ανίχνευση ιών και προστασία του υπολογιστή
- Δημοφιλή προγράμματα
 - Symantec
 - Kaspersky
 - AVG
 - McAfee



Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Αποτροπή μολύνσεων από ιούς (2 από 2) (Στόχος 9.8)

- Υπογραφή ιού
 - Ένα τμήμα του κώδικα του που τον χαρακτηρίζει μοναδικά
- Καραντίνα
 - Απομονώνει τον ιό σε έναν ασφαλή χώρο, έτσι ώστε να μην εξαπλωθεί σε άλλα αρχεία
- Εμβολιασμός
 - Καταγράφει τα βασικά χαρακτηριστικά των αρχείων του υπολογιστή σας και τα διατηρεί σε ασφαλές μέρος

Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Αυθεντικοποίηση (1 από 2) (Στόχος 9.9)

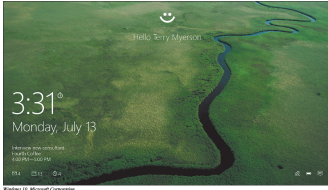
- Απαιτούνται ισχυροί κωδικοί πρόσβασης
- Προγράμματα μέτρησης της ισχύος κωδικών πρόσβασης
- Τα λειτουργικά συστήματα ενσωματώνουν προστασία με κωδικούς πρόσβασης
- Διαχείριση κωδικών πρόσβασης

Ισχυροί και ασφαλείς υποψήφιοι κωδικοί πρόσβασης			
Κωδικός πρόσβασης	Κατηγορία	Καλό σημείο	Κακό σημείο
john0h022	Απλήνης	- Περιέχει κεφαλαία και πεζά γράμματα - Περιέχει γράμματα και αριθμούς	- Απύκνωτα από 14 χαρακτήρες - Περιέχει ονόματα και ημερομηνία γέννησης
test44dine6car	Μέτριος	- 15 χαρακτήρες	- Περιέχει τρεις λέξεις που υπάρχουν σε λεξικό - Οι αριθμοί επαναλαμβάνονται
88Ran7h6ydl7H18	Καλή ποιότητα	- Καλό μήκος - Περιέχει κεφαλαία και πεζά γράμματα - Περιέχει σύμβολα	- Τα κεφαλαία και τα πεζά γράμματα επαναλαμβάνονται - Περιέχει μια λέξη που υπάρχει σε λεξικό (ραντ)
782m3mE3855ky98	Ισχυρός	- Όλα τα παραπάνω καλά σημεία - Η λέξη που υπάρχει σε λεξικό (στημεντσερ) είναι γραμμένη με 3 αντί για e	- Κανένα

Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Αυθεντικοποίηση (2 από 2) (Στόχος 9.9)

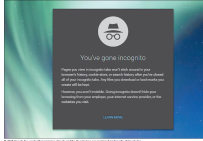
- Δακτυλικό αποτύπωμα
- Ίριδα των ματιών
- Συστήματα αναγνώρισης φωνής
- Αναγνώριση χαρακτηριστικών προσώπου
- Παρέχουν υψηλό επίπεδο ασφάλειας



Περιορισμός της πρόσβασης στους ψηφιακούς πόρους σας

Ανώνυμη περιήγηση στο web (στόχος 9.10)

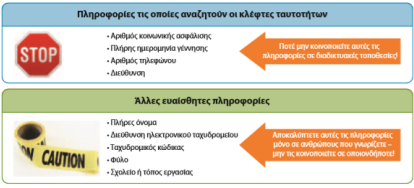
- Εργαλεία ανώνυμης περιήγησης
 - Private Browsing
 - InPrivate
 - Incognito
- Φορητές συσκευές προστασίας απορρήτου
 - IronKey Personal Flash Drives
- Εικονικά ιδιωτικά δίκτυα (VPN)
 - Ασφαλή δίκτυα που δημιουργούνται αξιοποιώντας τη δημόσια υποδομή του διαδικτύου



Διατηρήστε τα δεδομένα σας ασφαλή

Προστασία προσωπικών πληροφοριών (Στόχος 9.11)

- Να αποκαλύπτετε όσο το δυνατόν λιγότερα στοιχεία
- Στο Facebook να αλλάξετε τις επιλογές στις ρυθμίσεις απορρήτου σας



Διατηρήστε τα δεδομένα σας ασφαλή

Αντίγραφα ασφαλείας δεδομένων (1 από 2) (Στόχος 9.12)

- Τα αντίγραφα ασφαλείας είναι αντίγραφα των αρχείων τα οποία μπορείτε να χρησιμοποιήσετε ώστε να αντικαταστήσετε τα πρωτότυπα, αν χαθούν ή καταστραφούν
- Τύποι αρχείων χρειάζονται αντίγραφα ασφαλείας
 - Αρχεία δεδομένων
 - Αρχεία προγραμμάτων
- Επιλογές για τη δημιουργία αντιγράφων ασφαλείας
 - Πλήρη
 - Αυξητικό
 - Ειδώλου

Διατηρήστε τα δεδομένα σας ασφαλή

Αντίγραφα ασφαλείας δεδομένων (2 από 2) (Στόχος 9.12)

Τοποθεσία αντιγράφων ασφαλείας	Υπέρ	Κατά
Στο δίκτυο (στο cloud)	<ul style="list-style-type: none"> • Τα αρχεία φυλάσσονται σε μια ασφαλή, απομακρυσμένη τοποθεσία • Τα αρχεία και τα αντίγραφα ασφαλείας είναι προσβάσιμα από παντού μέσω του προγράμματος περιήγησης. 	<ul style="list-style-type: none"> • Τα περισσότερα δωρεάν πακέτα δεν προσφέρουν αρκετή χωρητικότητα για τα αντίγραφα ασφαλείας εσώνων συστημάτων
Εξωτερική μονάδα σκληρού δίσκου	<ul style="list-style-type: none"> • Οικονομική λύση που καταλάμβεται μόνο μία φορά • Έπιλογή αντιγραφα ασφαλείας με μια συσκευή USB 3.0, που συνδέεται απευθείας στον υπολογιστή σας. 	<ul style="list-style-type: none"> • Υπάρχει πιθανότητα η μονάδα να καταστραφεί από κάποιο συμβάν (φυσικό/πυρμαύρο) μαζί με τον υπολογιστή σας • Πιθανότητα κλοπής • Ελαφρώς πιο δύσκολη η δημιουργία αντιγράφων από πολλαπλούς υπολογιστές μόνο με μία συσκευή
Συσκευές αποθήκευσης που συνδέονται στο δίκτυο (NAS) ή οικιακοί διακομιστές	<ul style="list-style-type: none"> • Διευκολύνει τη δημιουργία αντιγράφων ασφαλείας για πολλαπλές συσκευές 	<ul style="list-style-type: none"> • Πιο ακριβή λύση από μια ανεξάρτητη εξωτερική μονάδα σκληρού δίσκου • Υπάρχουν πιθανότητες η μονάδα να καταστραφεί από κάποιο συμβάν (φυσικό/πυρμαύρο) μαζί με τον υπολογιστή σας • Πιθανότητα κλοπής

(Μικρά Φωτιά: Προσρο: Warrington/Φωτιά: Darklesign/Φωτιά)

Προστασία των φυσικών ψηφιακών πόρων σας

Περιβαλλοντικοί παράγοντες και αυξομειώσεις τάσης ρεύματος (Στόχος 9.13)

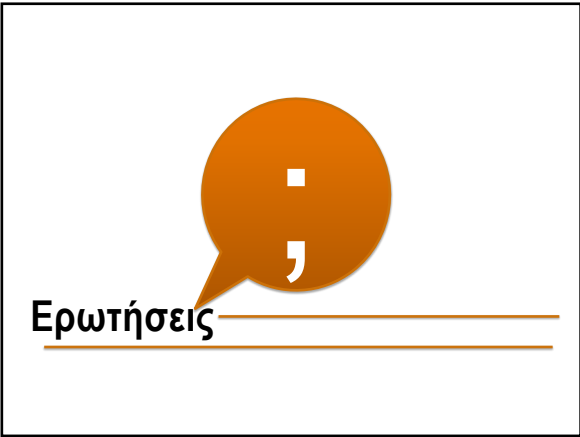
- Αυξομειώσεις τάσης
 - Παλιά ή ελαττωματική καλωδίωση
 - Δυσλειτουργίες σε ηλεκτρικούς υποσταθμούς
 - Κεραυνοί
- Πολύπριζο ασφαλείας
 - Αντικατάσταση κάθε 2-3 χρόνια
 - Χρήση σε όλες οι ηλεκτρικές συσκευές που περιέχουν εξαρτήματα σταθερής κατάστασης



Προστασία των φυσικών ψηφιακών πόρων σας Παρεμπόδιση και αντιμετώπιση κλοπής (Στόχος 9.14)

- Τρία πράγματα που θα πρέπει να έχετε υπόψη σας σχετικά με την ασφάλεια των φορητών σας συσκευών
 - Να τις προστατεύετε από κλοπή
 - Να διατηρείτε τα δεδομένα σας ασφαλή σε περίπτωση κλοπής
 - Να βρείτε τη συσκευή αν έχει κλαπεί

Τέλος προστασίας
<ul style="list-style-type: none"> • Έτσι προστατεύεται η φυσική ασφάλεια σε όλες τις συσκευές και τα δεδομένα και οι πληροφορίες που αναφέρονται στο έγγραφο • Μπορεί να προστατευτεί, ως να λειτουργούν οι κλειδές προστασίας του υπολογιστή • Έτσι προστατεύονται τα αρχεία που είναι προστατευμένα με κρυπτογράφηση, το όνομα προγράμματος λογισμικού και όλα διαθέσιμα στο google
Ίδιε προστασία από άγνωστες
<ul style="list-style-type: none"> • Έτσι προστατεύεται η φυσική ασφάλεια από όλες τις συσκευές σε όλες τις συσκευές και τα δεδομένα • Έτσι προστατεύεται η φυσική ασφάλεια από όλες τις συσκευές και τα δεδομένα • Έτσι προστατεύεται η φυσική ασφάλεια από όλες τις συσκευές και τα δεδομένα • Έτσι προστατεύεται η φυσική ασφάλεια από όλες τις συσκευές και τα δεδομένα
Επιχειρησιακή λειτουργία
<ul style="list-style-type: none"> • Έτσι αλλάζει το λειτουργικό σύστημα στο Windows, OS X, macOS στα οποία να εγκαταστήσει τους συσκευές και συσκευές προστασίας λογισμικού ασφαλείας • Έτσι αλλάζει όλα τα προγράμματα λογισμικού που είναι προστατευμένα από κλοπή σας • Έτσι το Microsoft Office ή το παρόμοιο, κερδίζουν ασφάλεια, από τις σημαντικές λειτουργίες • Έτσι την πιο πρόσφατη έκδοση του λειτουργικού συστήματος και ενημερώνεται
Προστασία των συσκευών σας
<ul style="list-style-type: none"> • Προστατεύονται όλες οι πληροφορίες, συσκευές και από τις πληροφορίες, τις πληροφορίες που είναι ασφαλείς • Έτσι προστατεύονται πληροφορίες στις συσκευές, συσκευές και λειτουργικά συστήματα



Απαγορεύεται η αναδημοσίευση ή αναπαραγωγή του παρόντος έργου με οποιονδήποτε τρόπο χωρίς γραπτή άδεια του εκδότη, σύμφωνα με το Ν. 2121/1993 και τη Διεθνή Σύμβαση της Βέρνης (που έχει κυρωθεί με τον Ν. 100/1975)