Ασφάλεια Πληροφοριών: Εισαγωγή

Μάθημα Πολιτικές Ασφάλειας & Ιδιωτικότητας στο Διαδίκτυο

ΠΜΣ «Ψηφιακές Εφαρμογές & Καινοτομία»

Τσώχου Αγγελική *atsohou@ionio.gr*

Η ασφάλεια πληροφοριακών συστημάτων στην ψηφιακή εποχή

Παραβίαση Ασφάλειας 100 εκ. Δολαρίων

- Μάιος 2006: ένας φορητός υπολογιστής κι ένας εξωτερικός σκληρός δίσκος που ανήκουν στο Υπουργείο Άμυνας των Η.Π.Α. (Dept of Veterans Affairs) κλέβονται κατά τη διάρκεια διάρρηξης στο σπίτι εργαζομένου του Υπουργείου.
- Περιέχουν τα δεδομένα 26.5 εκ. βετεράνων και των συζύγων τους, σε μη κρυπτογραφημένη μορφή.
- Ο Γενικός Γραμματέας Jim Nicholson δήλωσε στο Κογκρέσο ότι η παραβίαση θα οδηγήσει σε κόστος τουλάχιστον $10 εκ. μόνο για να ενημερώσουν τους βετεράνους για την παραβίαση ασφάλειας.
- Το συνολικό κόστος της παραβίασης: $100 εκ.

https://www.va.gov/oig/pubs/vaoig-06-02238-163.pdf

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Επίπληξη της FINMA στην HSBC Suisse

- Μάρτιος 2010: Η Εποπτική Αρχή της χρηματοπιστωτικής αγοράς της Ελβετίας FINMA (Swiss Financial Market Supervisory Authority) ξεκίνησε επίσημη διοικητική διαδικασία κατά της HSBC (Suisse) SA στη Γενεύη
- Ένας πρώην υπάλληλος έκλεψε δεδομένα από 24.000 τραπεζικούς λογαριασμούς στο τέλος του 2006- αρχές του 2007. Η HSBC εξακολουθούσε να μη γνωρίζει για την κλοπή έως ότου ο υπάλληλος προσπάθησε να πουλήσει τα δεδομένα στις Γαλλικές Αρχές
- Οι Γαλλικές, Ιταλικές και Γερμανικές Αρχές είχαν συμφέρον απόκτησης των δεδομένων για λόγους διερεύνησης υποθέσεων φοροδιαφυγής και υπεξαιρέσεων.
- Έπειτα από την εγκληματική διερεύνηση η FINMA προχώρησε σε έντονη επίπληξη της τράπεζας για τα μέτρα ασφάλειας πληροφοριών

https://www.finma.ch/en/news/2011/02/mm-hsbc-20110228/

finma

Απάτη $64.8 δις. στη Wall Street

- Ο Bernard Madoff ομολόγησε το 2009 για τη μεγαλύτερη απάτη στην ιστορία της Wall Street (απάτη που ονομάζεται Ponzi scheme) που εξαπάτησε επενδυτές περίπου $64.8 δις
- Η απάτη του Madoff στηρίχθηκε αποκλειστικά σε τεχνικές κοινωνικής μηχανικής (social engineering) και στην προβλεψιμότητα της ανθρώπινης φύσης (και όχι σε οικονομικές γνώσεις)
- Το σκάνδαλο οδήγησε σε επάλληλες εγκληματικές διερευνήσεις προς την Επιτροπή Κεφαλαιαγοράς (Securities and Exchange Commission)
- Στόχος των διερευνήσεων στα πληροφοριακά συστήματα της Επιτροπής ήταν η συλλογή τεκμηρίων για την πιθανή ανάμειξη άλλων ατόμων στην απάτη

http://www.businessinsider.com/how-bernie-madoffs-ponzi-scheme-worked-2014-7

Yahoo: 1δις λογαριασμοί παραβιάστηκαν τον Αύγουστο του 2013 και 500 εκ. το 2014

- Η Yahoo αποκάλυψε το Δεκέμβριο του 2016 ότι δεδομένα από ένα 1 δις λογαριασμούς χρηστών είχαν παραβιαστεί τον Αύγουστο του2013
- Το περιστατικό είναι διακριτό από την παραβίαση 500 εκ. λογαριασμών χρηστών που συνέβη το 2014

23/09/2016 Yahoo 'state' hackers stole data from 500 million users - BBC News

BBC News Sport Weather Shop Earth Travel

Technology

Yahoo 'state' hackers stole data from 500 million users

3 hours ago | Technology

Yahoo says "state-sponsored" hackers stole information from about 500 million users in what appears to be the largest publicly disclosed cyber-breach in history.

The breach included swathes of personal information, including names and emails, as well as "unencrypted security questions and answers".

The hack took place in 2014 but has only now been made public.

Παρόμοια περιστατικά παραβίασης σε κοινωνικά μέσα

- MySpace 359 εκ. λογαριασμοί
- LinkedIn 164 εκ. λογαριασμοί
- Adobe 152 εκ. λογαριασμοί
- Badoo 112 εκ. λογαριασμοί
- VK 93 εκ. λογαριασμοί
- Dropbox 68 εκ. λογαριασμοί
- tumblr 65 εκ. λογαριασμοί
- iMesh 49 εκ. λογαριασμοί
- Fling 40 εκ. λογαριασμοί
- Last.fm 37 εκ. λογαριασμοί

haveibeenpwned.com

Επίθεση στο Δίκτυο Ηλεκτροδότησης της Ουκρανίας το 2016

- Η επίθεση ξεκίνησε με ηλεκτρονική αλίευση με στόχο υπαλλήλους πληροφορικής και διαχειριστές συστημάτων
- Το πρόγραμμα ηλεκτρονικής αλίευσης περιλάμβανε emails με επισυναπτόμενα Word αρχεία που ζητούσαν ενεργοποίηση των μακροεντολών. Αν ο παραλήπτης ενεργοποιούσε τις μακροεντολές το λογισμικό που ονόμασαν BlackEnergy3 εγκαθίστανται τον υπολογιστή και άνοιγε μία κερκόπορτα για τους επιτιθέμενους

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

KIM ZETTER SECURITY 03.03.16 07:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter

Επίθεση στο Δίκτυο Ηλεκτροδότησης της Ουκρανίας το 2016

- Τα συστήματα ελέγχου πρόσβασης στο Δίκτυο Ηλεκτροδότησης της Ουκρανίας ήταν πιο ασφαλή ακόμη κι από κάποια συστήματα των Η.Π.Α.
- Η επίθεση οδήγησε στη διακοπή ηλεκτροδότησης 30 σταθμών ηλεκτροδότησης και 80000 πελατών.

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

KIM ZETTER SECURITY 03.03.16 07:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter

Το πρόβλημα της ασφάλειας πληροφοριών

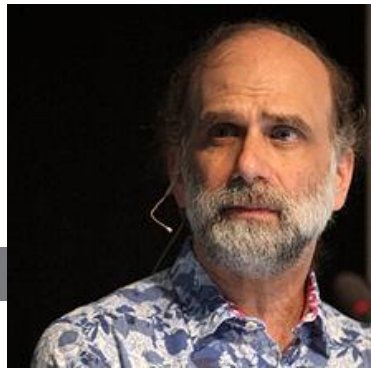
- Συνδέεται με την επίτευξη έξι στόχων για τα πληροφοριακά συστήματα:
  - Πρέπει να κάνουν ακριβώς τις λειτουργίες για τις οποίες έχουν σχεδιαστεί
  - Δεν πρέπει ποτέ να κάνουν κάτι το οποίο δεν έχει σχεδιαστεί
  - Πρέπει να λειτουργούν εντός των χρονικών ορίων που θέτει ο σχεδιασμός τους
  - Δεν πρέπει ποτέ να ξεπερνούν τα χρονικά όρια που θέτει ο σχεδιασμός τους
  - Πρέπει να χρησιμοποιούνται από εξουσιοδοτημένο προσωπικό
  - Δεν πρέπει ποτέ να χρησιμοποιούνται από μη εξουσιοδοτημένο προσωπικό

Το πρόβλημα της ασφάλειας πληροφοριών

- Δεν επαρκεί η προστασία της υποδομής και του δικτύου επικοινωνιών (π.χ. μέσω IDS συστημάτων)
- Δεν επαρκεί να ακολουθεί ο οργανισμός συστάσεις ή πιστοποιήσεις
- Σχετίζεται με την ατελή ανάπτυξη του λογισμικού και την μαζική παραγωγή κρίσιμων εφαρμογών σε μη ασφαλείς πλατφόρμες

Και ένα ακόμη πρόβλημα…

https://www.youtube.com/watch?v=opRMrEfAIiI



Αν πιστεύετε ότι μπορεί η τεχνολογία να λύσει τα προβλήματα ασφάλειας είτε δεν καταλαβαίνετε τα προβλήματα ή δεν καταλαβαίνετε την τεχνολογία.

Bruce Schneier

Πληροφορία και παγκοσμιοποίηση της οικονομίας

- Η εξάρτηση της μακρο-οικονομίας από την πληροφορία: «*Πληροφοριοποιημένη κοινωνία*»
- Η πληροφορία ως μικρο-οικονομικό αγαθό
  - Υλικά αγαθά: κόστος αγοράς, πώληση μια φορά, δυνατότητα μεταπώλησης
  - Υπηρεσίες ως αγαθά
  - Η πληροφορία έχει αξία
  - Η πληροφορία δεν καταναλώνεται

Η αξία της πληροφορίας

- Η συλλογή, δημιουργία ή συντήρηση της πληροφορίας συνεπάγεται κόστος
- Η πληροφορία έχει αξία γι’ αυτούς στους οποίους ανήκει, αυτούς που τη χρησιμοποιούν και αυτούς που επιθυμούν να την αποκτήσουν

Παράγοντες διαμόρφωσης της αξίας της πληροφορίας

- Η **αποκλειστική** κατοχή
- Η χρησιμότητα
- Το κόστος δημιουργίας (απόκτησης) ή αναδημιουργίας (επαναπόκτησης)
- Η αστική ή άλλη νομική **ευθύνη**
- Η μετατρεψιμότητα ή διαπραγματευσιμότητα
- Η **επιχειρησιακή** σημασία

Η κοινωνική σημασία της πληροφορίας

- Η πληροφορία μπορεί να αποτελέσει και ισχυρό όργανο κοινωνικού ελέγχου
- Διαχρονικό πρόβλημα, που εντείνεται με τη διαθεσιμότητα ΤΠΕ
- Οι ΤΠΕ επιτρέπουν τη συγκέντρωση, επεξεργασία, αποθήκευση και μετάδοση μεγάλου όγκου πληροφοριών, που μπορεί να οδηγήσει:
  - Στην ενοποίηση και ολοκληρωμένη παράθεσή τους
  - Στη συνδυασμένη χρήση πληροφοριών που συλλέχθηκαν για διαφορετικούς σκοπούς
  - Στη λήψη αποφάσεων με βάση αποκλειστικά αυτοματοποιημένη επεξεργασία πληροφοριών

Η κοινωνική σημασία της πληροφορίας

- Πολλά παραδείγματα καταχρηστικής αξιοποίησης πληροφοριών που αρχικά συλλέχθηκαν για κοινωνικά αποδεκτούς σκοπούς.
- Είναι η λύση η αποχή από τη συλλογή πληροφοριών;

Κίνητρα για τη θέσπιση κανόνων

- Η αύξηση της διασυνοριακής ροής προσωπικών δεδομένων
- Η σημασία της προστασίας προσωπικών δεδομένων για την εμπιστοσύνη των καταναλωτών στην εποχή της Πληροφορίας
- Η προστασία των ατομικών δικαιωμάτων

Η ασφάλεια ως απαίτηση των δικαιούχων

- Η διοίκηση ενός οργανισμού
- Οι **ιδιοκτήτες** και **διαχειριστές** δεδομένων και διεργασιών
- Οι **τελικοί** χρήστες
- Οι υπεύθυνοι **ανάπτυξης** του συστήματος
- Οι υπεύθυνοι **λειτουργίας** του
- Οι **καταναλωτές** των τελικών προϊόντων και υπηρεσιών
- Η **πολιτεία**

Ένα πλαίσιο για την προστασία των πληροφοριών

- Πρέπει να είναι:
  - Κοινωνικά αποδεκτό (ανάπτυξη βασισμένη στις απόψεις του κοινωνικού συνόλου)
  - Πολυδύναμο (ανάπτυξη με βάση τη διεθνή εμπειρία και πρακτική)
  - Πολυδιάστατο (συνδυασμός θεσμικών ρυθμίσεων, οργανωσιακών ρυθμίσεων και κοινωνικών δράσεων)
- Πλαίσια ανά τομέα

Θεσμικές και κανονιστικές ρυθμίσεις

- Κανονιστικές και νομικές
- Υπερεθνικές, εθνικές, τοπικές
- Οριζόντιες, κατακόρυφες

- ✓ Η σύμβαση 108 του Συμβουλίου της Ευρώπης (28.01.1981)
- ✓ Η Ευρωπαϊκή οδηγία 95/46 και 2002/58
- ✓ Ο Ν. 2472/97 και Ν. 3471/06
- ✓ Οι οδηγίες για την ασφάλεια ΠΣ του ΟΟΣΑ

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης

- Διεθνής οργανισμός
- Στόχος:
  - Η σύγκριση συγκρίνουν εφαρμογές πολιτικής των χωρών
  - Η απάντηση κοινών προβλημάτων
  - Ο προσδιορισμός καλών πρακτικών
  - Ο συντονισμός εσωτερικών και διεθνών πολιτικών

Οι οδηγίες του ΟΟΣΑ για την ασφάλεια ΠΣ

- Εκδόθηκαν το 1992, αναθεωρήθηκαν το 1997 και η τρέχουσα έκδοσή τους δημοσιεύτηκε το 2002
- Στόχοι:
  - Αύξηση της ευαισθητοποίησης του κοινού
  - Παροχή γενικού πλαισίου
  - Ενίσχυση της συνεργασίας μεταξύ δημόσιου και ιδιωτικού τομέα
  - Αύξηση της εμπιστοσύνης του κοινού στα ΠΣ
  - Διευκόλυνση της ανάπτυξης και χρήσης ΠΣ σε διεθνές επίπεδο
  - Ενίσχυση της διεθνούς συνεργασίας στον τομέα της ασφάλειας ΠΣ
- Αφορούν ΠΣ του δημόσιου και του ιδιωτικού τομέα

Οι βασικές αρχές για την ασφάλεια ΠΣ του ΟΟΣΑ (1992, 1997)

1) Η αρχή της απόδοσης ευθύνης (accountability)
2) Η αρχή της ενημερότητας (awareness)
3) Η αρχή της ηθικής (ethics)
4) Η αρχή του πολυδύναμου (multidisciplinary)
5) Η αρχή της αναλογικότητας (proportionality)
6) Η αρχή της ολοκλήρωσης (integration)
7) Η αρχή της άμεσης δράσης (timeliness)
8) Η αρχή της δημοκρατίας (democracy)
9) Η αρχή της επανεξέτασης (reassessment)

Οι βασικές αρχές του ΟΟΣΑ για την ασφάλεια ΠΣ (2002)

1) Η αρχή της ενημερότητας (awareness)
2) Η αρχή της ευθύνης (responsibility)
3) Η αρχή της ανταπόκρισης (response)
4) Η αρχή της ηθικής (ethics)
5) Η αρχή της δημοκρατίας (democracy)
6) Η αρχή της αποτίμησης επικινδυνότητας (risk assessment)
7) Η αρχή του σχεδίασης και υλοποίησης ασφάλειας (security design and implementation)
8) Η αρχή της διαχείρισης ασφάλειας (security management)
9) Η αρχή της επανεξέτασης (reassessment)

Το ελληνικό νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων

- Σύνταγμα (άρθρο 9Α)
- Νόμος 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα
- Νόμος 3471/06 για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών

Εννοιολογική Θεμελίωση

Στόχος

- Πλαίσιο κοινού λεξιλογίου για τη συζήτηση των ζητημάτων Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων
- Κατανόηση των σχέσεων μεταξύ των διαφορετικών όρων που σχετίζονται με την περιοχή της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων

Κύριες έννοιες

- **Αγαθό** (asset)
  - ένας πόρος που αξίζει να προστατευθεί
- **Αξία** (Value)
  - Σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους
- **Ζημιά** (harm)
  - ο περιορισμός της αξίας ενός αγαθού

Κύριες έννοιες

- **Απειλή** (threat)
  - μία πιθανή αιτία που μπορεί να προκαλέσει ζημιά σε ένα αγαθό
- **Ευπάθεια** (vulnerability)
  - Μία αδυναμία ενός αγαθού ή ομάδας αγαθών που μπορεί να την εκμεταλλευτούν μία ή περισσότερες απειλές.
- **Επίπτωση** (impact)
  - Απώλεια μίας αξίας, η αύξηση του κόστους ή άλλη ζημιά που μπορεί να προκύψει ως συνέπεια μιας παραβίασης.

Κύριες έννοιες

- **Ιδιοκτήτης** (Owner)
  - Πρόσωπο που κατέχει ή είναι υπεύθυνο για ένα αγαθό και που έχει το δικαίωμα να καθορίσει πώς μπορεί να χρησιμοποιηθεί, να μεταβληθεί ή να διατεθεί το αγαθό αυτό.
- **Χρήστης** (User)
  - Πρόσωπο ή διεργασία που χρησιμοποιεί ολόκληρο ή μέρος του πληροφοριακού συστήματος.
- **Εξουσιοδότηση** (Authorisation)
  - Άδεια που παρέχεται από έναν ιδιοκτήτη για κάποιο σκοπό.

Η έννοια της ασφάλειας

- Αποδίδει στην ελληνική γλώσσα τους αγγλικούς όρους:
  - Security
  - Safety
  - Insurance
  - Assurance

Η έννοια της ασφάλειας Π.Σ.

Για να κατανοήσουμε την έννοια της Ασφάλεια Π.Σ....

ΠΡΕΠΕΙ πρώτα να προσδιορίσουμε την έννοια του Π.Σ....

ΑΛΛΑ πρώτα να προσδιορίσουμε την έννοια του Συστήματος.

Η έννοια του Συστήματος

«Ένας αριθμός αλληλεπιδρώντων στοιχείων, έχουν οργανικά συναρμολογηθεί σε μια ολότητα έτσι ώστε να εκτελούν μια ορισμένη λειτουργία.»

ΆΡΑ:

- επιμέρους στοιχεία,
- που αλληλεπιδρούν,
- χαρακτηρίζεται από οργάνωση και
- εξετάζεται ως μία ενιαία ολότητα.

Πληροφοριακό Σύστημα

Ένα οργανωμένο σύνολο από πέντε στοιχεία τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείρισης πληροφορίας, για την υποστήριξη των ανθρώπινων δραστηριοτήτων, στα πλαίσια του οργανισμού.

Άνθρωποι

Λογισμικό

Υλικό

Διαδικασίες

Δεδομένα

Όροι σχετικοί, αλλά όχι ταυτόσημοι

Τεχνολογίες Πληροφορικής και Επικοινωνιών (Information and Communication Technology)

ή

Τεχνολογική Υποδομή (Information Infrastructure)

Συλλογή υπολογιστικού υλικού, λογισμικού, τηλεπικοινωνιακού εξοπλισμού ή άλλων υπολογιστικών εξαρτημάτων που χρησιμοποιείται για τη διαχείριση πληροφοριών.

Πληροφοριακό Σύστημα = Τεχνολογική Υποδομή + Οργανωσιακό πλαίσιο

Ασφάλεια Π.Σ.

Το **οργανωμένο** πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Π.Σ., αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.

Ασφάλεια Π.Σ.

- Έμφαση στο Π.Σ. ως **ολότητα** αλλά και σε όλα τα **επιμέρους** στοιχεία του.
- Η προστασία αφορά **κάθε** είδους απειλή (τυχαία ή σκόπιμη).
- Η ασφάλεια Π.Σ. συνδέεται άμεσα τόσο με τις τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με τις **αντιλήψεις**, **αρχές** και **παραδοχές**.
- Το πλαίσιο αυτό χαρακτηρίζεται από **οργάνωση**.

Ασφάλεια Πληροφοριών και Τεχνολογικής Υποδομής

- Ασφάλεια Πληροφοριών:
  - Απόκτηση και διατήρηση της ασφάλειας σε σχέση με πληροφορίες ή υπολογιστικά συστήματα διαχείρισης πληροφοριών.
- Ασφάλεια τεχνολογιών πληροφορικής και επικοινωνιών:
  - Απόκτηση και διατήρηση της ασφάλειας των υπολογιστικών πόρων.

Κύρια Χαρακτηριστικά της ασφάλειας

Εμπιστευτικότητα (**C**onfidentiality)

- Η διασφάλιση ότι οι πληροφορίες δεν αποκαλύπτονται και δε γίνονται διαθέσιμες σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες.

Ακεραιότητα (**I**ntegrity)

- Η διασφάλιση της ορθότητας και πληρότητας ενός αγαθού ή η αποφυγή μη εξουσιοδοτημένης τροποποίησης ενός αγαθού.

Διαθεσιμότητα (**A**vailability)

- Η διασφάλιση ότι ένα αγαθό είναι διαθέσιμο όταν ζητείται από μία εξουσιοδοτημένη οντότητα.

Άλλα χαρακτηριστικά της ασφάλειας

- **Αυθεντικότητα** (authenticity)
  - Η διασφάλιση ότι η ταυτότητα μίας οντότητας είναι αυτή που έχει ισχυριστεί. Η οντότητα αυτή μπορεί να είναι χρήστης, διαδικασία ή σύστημα.
- **Λογοδοσία** (accountability)
  - Η διασφάλιση ότι όλες οι ενέργειας μίας οντότητας μπορούν να εντοπιστούν μοναδικά για την οντότητα αυτή.

Άλλα χαρακτηριστικά της ασφάλειας

- **Μη αποποίηση ευθύνης** (non-repudiation)
  - Η διασφάλιση ότι μπορεί να αποδειχθεί ότι κάθε ενέργεια ή γεγονός έλαβε χώρα, ώστε να μην είναι δυνατόν να αμφισβητηθεί.
- **Αξιοπιστία(**reliability)
  - Η διασφάλιση ότι μία οντότητα έχει συμπεριφορά και αποτελέσματα που είναι συνεπή με τα επιδιωκόμενα.

Παραδείγματα αγαθών

- Φυσικά αγαθά
  - Υλικό (hardware)
  - Τηλεπικοινωνιακός εξοπλισμός (communication facilities)
  - Κτίρια
- Πληροφορίες/Δεδομένα
- Λογισμικό
- Άνθρωποι
- Άϋλα αγαθά
  - Φήμη
  - Δημόσια εικόνα

Κατηγορίες απειλών

- Φυσικές απειλές
- Απειλές τεχνικών βλαβών
- Ανθρώπινες απειλές
  - Σκόπιμες
  - Τυχαίες

Παραδείγματα φυσικών απειλών

- Φωτιά
- Πλημμύρα
- Σεισμός
- κτλ.

Παραδείγματα τυχαίων ανθρώπινων απειλών

- Λάθη χρηστών
  - Εσφαλμένη διαγραφή αρχείων
- Λάθη χειριστών
  - Λανθασμένη δρομολόγηση
- Λάθος συντήρησης υλικού ή λογισμικού
- Εισαγωγή κακόβουλου λογισμικού
- κτλ.

Παραδείγματα σκόπιμων ανθρώπινων απειλών

- Πλαστοπροσωπία από εσωτερικούς/εξωτερικούς χρήστες ή παρόχους υπηρεσιών
- Μη εξουσιοδοτημένη χρήση εφαρμογής
- Μη εξουσιοδοτημένη τροποποίηση δεδομένων
- Φιλτράρισμα ή παρεμβολές επικοινωνιών
- Κλοπή υλικού
- Ηθελημένη πρόκληση βλάβης - βανδαλισμός
- κτλ.

Παραδείγματα απειλών τεχνικών βλαβών

- Διακοπή ηλεκτροδότησης
- Αστοχία λογισμικού συστήματος και δικτύου
- Αστοχία λογισμικού εφαρμογών
- Βλάβη εξυπηρετητή
- Βλάβη συσκευής δικτύου
- κτλ.

Παραδείγματα ευπαθειών

- Ευπάθειες υλικού
  - Έλλειψη σωστών πρακτικών απόσυρσης υλικού
  - Τήρηση σε μη εγκεκριμένες συνθήκες (π.χ. θερμοκρασία, σκόνη)
- Ευπάθειες λογισμικού
  - Παράλειψη αποσύνδεσης χρηστών
  - Έλλειψη τεκμηρίωσης των εφαρμογών

Παραδείγματα ευπαθειών

- Ευπάθειες δικτύου
  - Μη κρυπτογραφημένη μετάδοση εμπιστευτικών πληροφοριών
  - Χρήση μη προστατευόμενων δημόσιων δικτύων
- Ευπάθειες προσωπικού
  - Έλλειψη δράσεων ενημερότητας ασφάλειας
  - Έλλειψη διαδικασιών ασφάλειας

Παραδείγματα ευπαθειών

- Ευπάθειες διοίκησης
  - Έλλειψη τεκμηριωμένων διαδικασιών
  - Έλλειψη διαδικασιών αναθεώρησης πολιτικών (ασφάλειας, ελέγχου πρόσβασης κ.ά.)
- Κτιρίου
  - Τοποθεσία σε περιοχές συχνών φαινομένων πλημμύρας
  - Τοποθεσία σε περιοχή όπου το δίκτυο ηλεκτροδότησης είναι ασταθές

Παραδείγματα επιπτώσεων

- Οικονομική Απώλεια
- Παρεμπόδιση λειτουργίας
- Απώλεια καλής φήμης
- Εμπορικά και οικονομικά συμφέροντα
- Παραβίαση νομοθεσίας
- Παρεμπόδιση δικαιοσύνης
- Προσωπική ασφάλεια

…Κύριες έννοιες

Επικινδυνότητα (risk)

- Το αποτέλεσμα του συνδυασμού της πιθανότητας εκδήλωσης ενός γεγονότος ασφάλειας και των επιπτώσεών του.

Αντίμετρο ή μέτρο ασφάλειας (safeguard)

- Ένα μέτρο σχεδιασμένο για να εμποδίσει μία παραβίαση είτε να μειώσει τις επιπτώσεις της.
- Μπορεί να περιλαμβάνει πολιτικές, διαδικασίες, οδηγίες, οργανωσιακές πρακτικές ή οργανωσιακές δομές διαχειριστικής, τεχνικής, οργανωσιακής ή νομικής φύσης.

…Κύριες έννοιες

- **Πολιτική (policy)**
  - Μία επίσημα καθορισμένη από τη Διοίκηση κατεύθυνση και επιδίωξη
- **Απομένουσα επικινδυνότητα (residual risk)**
  - Επικινδυνότητα που απομένει μετά την εγκατάσταση των μέσων προστασίας

Εννοιολογική συσχέτιση: Σενάρια

Σενάριο 1: Ένα μέτρο προστασίας (ΜΠ) είναι αποτελεσματικό στη μείωση της επικινδυνότητας (Ε) που σχετίζεται με μία απειλή (ΑΠ) η οποία είναι ικανή να εκμεταλλευτεί μία ευπάθεια(ΕΥ). Η απειλή μπορεί να πραγματοποιηθεί μόνο εφόσον το αγαθό είναι ευπαθές σε αυτή.

Σενάριο 2: Ένα μέτρο προστασίας (ΜΠ) είναι αποτελεσματικό στη μείωση της επικινδυνότητας (Ε) που σχετίζεται με μία απειλή (ΑΠ), η οποία είναι ικανή να εκμεταλλευτεί πολλαπλές ευπάθειες (ΕΥ).

Εννοιολογική συσχέτιση: Σενάρια

- **Σενάριο 3**: Πολλά μέσα προστασίας (ΜΠ) είναι αποτελεσματικά στη μείωση της επικινδυνότητας (Ε) που σχετίζεται με πολλαπλές απειλές (ΑΠ), οι οποίες είναι ικανές να εκμεταλλευτούν μία ευπάθεια (ΕΥ). Μερικές φορές διαφορετικά μέτρα προστασίας επιλέγονται ώστε να μειωθεί η επικινδυνότητα σε ένα αποδεκτό επίπεδο, ώστε η απομένουσα επικινδυνότητα (ΑΕ) να είναι αποδεκτή.

Εννοιολογική συσχέτιση: Σενάρια

- **Σενάριο 4**: Η επικινδυνότητα (Ε) κρίνεται αποδεκτή και δεν εφαρμόζονται μέτρα προστασίας (ΜΠ), παρά το γεγονός ότι οι απειλές (ΑΠ) και οι ευπάθειες (ΕΥ) υπάρχουν.
- **Σενάριο 5**: Μία ευπάθεια (ΕΥ) υφίσταται, αλλά δεν είναι γνωστή καμία απειλή που να μπορεί να την εκμεταλλευτεί.

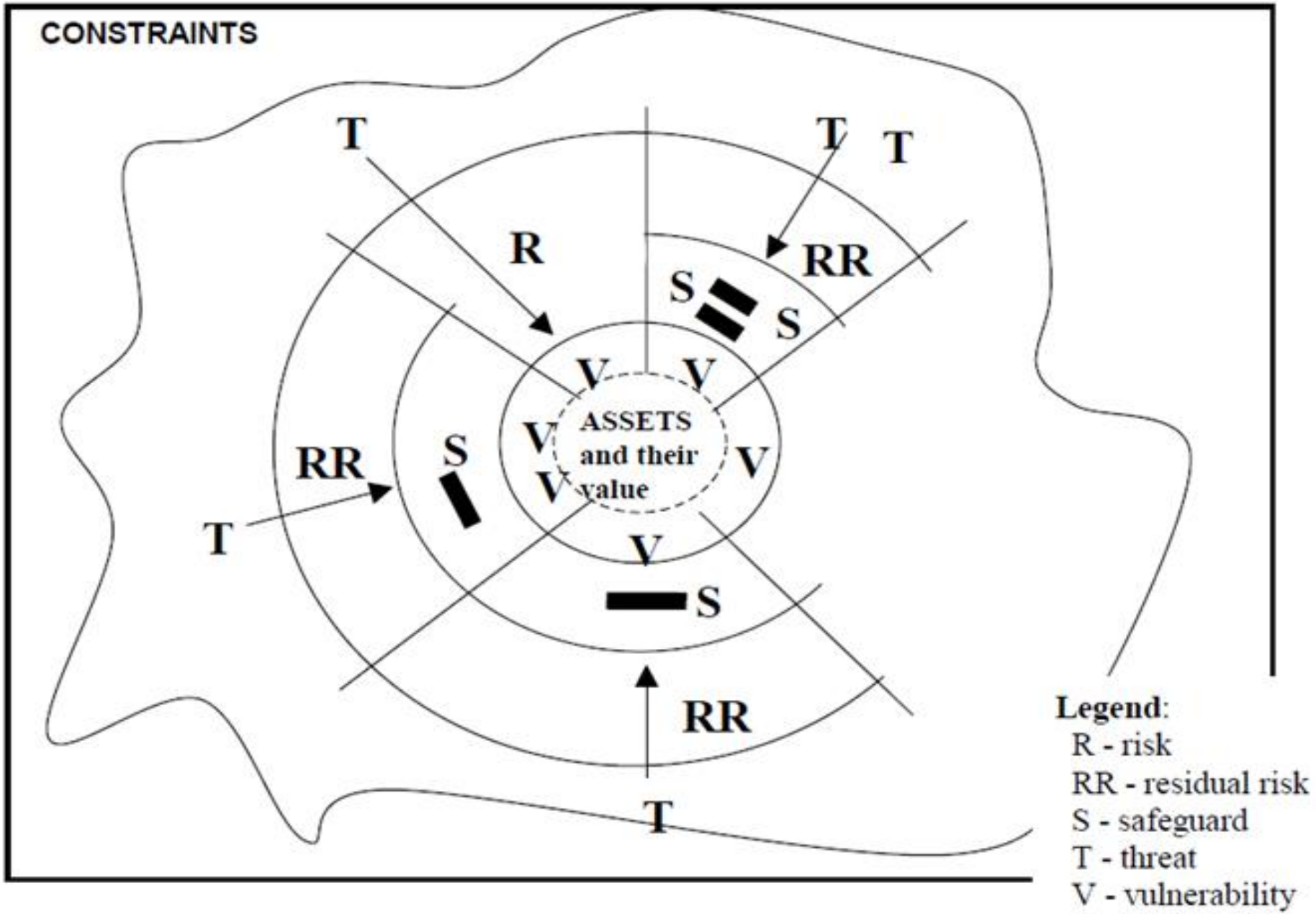


Figure 1 – Security element relationships

Βιβλιογραφία

- Βασισμένο στο κεφάλαιο του Δ. Γκρίτζαλη Εννοιολογική Θεμελίωση, στο "Ασφάλεια Πληροφοριακών Συστημάτων",Σ. Κάτσικα, Δ. Γκρίτζαλη, Σ. Γκρίτζαλη (Επιστημονική Επιμέλεια), 2004
- ISO/IEC 13335-1:2004. Information technology -- Security techniques -- Management of information and communications technology security
- Οι οδηγίες για την ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων του ΟΟΣΑ (www.oecd.org)