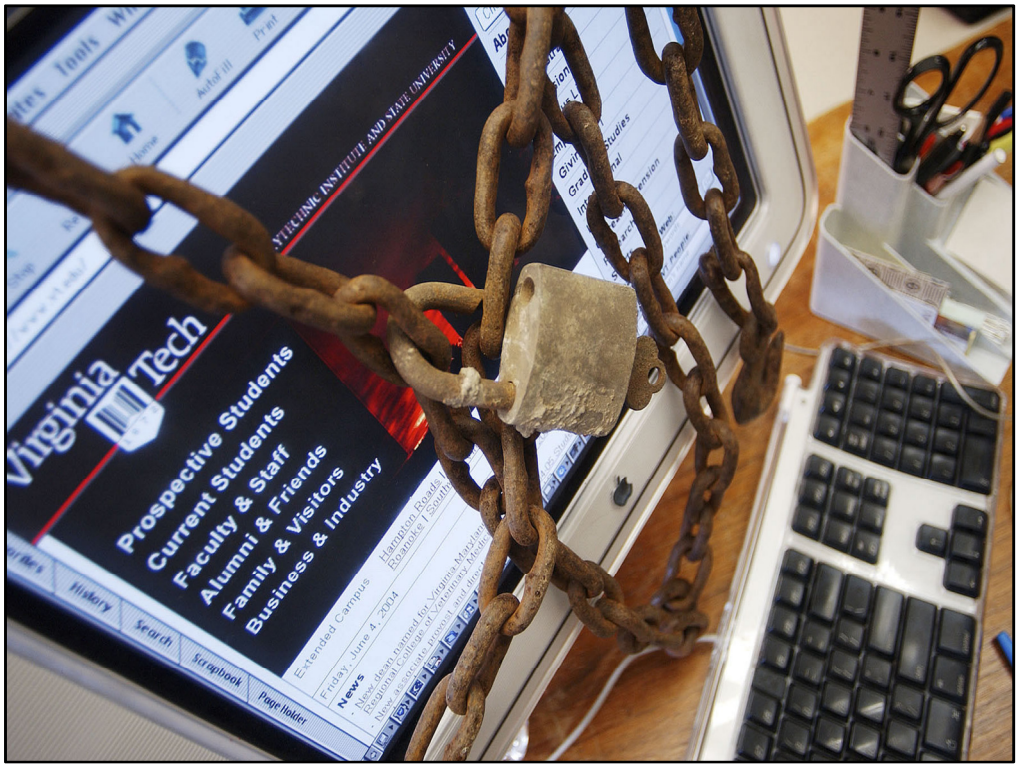

Δρ Κωνσταντίνος Παπαπαναγιώτου
Ανάλυση και
Διαχείριση
Κινδύνων
Πληροφορικής



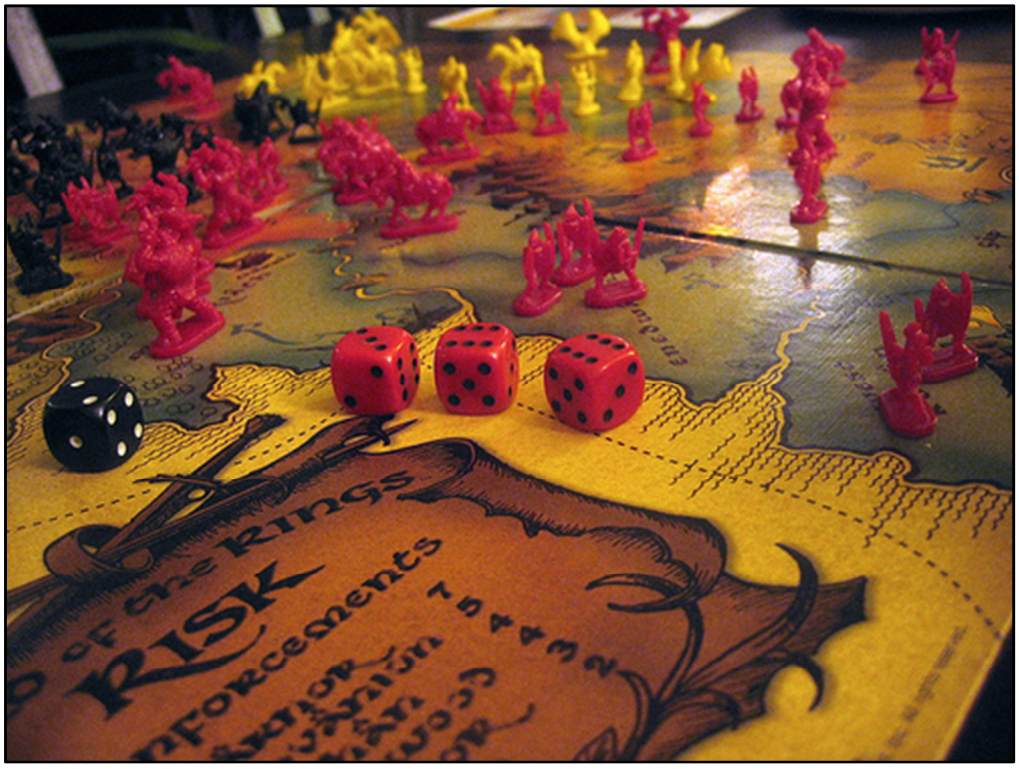
Τι είναι ασφάλεια πληροφοριών;
Τι θεωρεί ο καθένας ασφάλεια;
Τι είναι πιο σημαντικό ως προς την ασφάλεια στην πληροφορική;

- Η αιτιολόγηση του κόστους μέτρων ασφαλείας.
- Η επικοινωνία μεταξύ ειδικών στις ΤΠΕ και στη Διοίκηση
- Η ενεργός συμμετοχή των χρηστών στην προσπάθεια προστασίας του ΠΣ
- Η (λανθασμένη) αντίληψη ότι "η *ασφάλεια ΠΣ αποτελεί αμιγώς τεχνικό ζήτημα*"
- Η ανάπτυξη ενός αποδοτικού και αποτελεσματικού σχεδίου ασφάλειας
- Ο προσδιορισμός και αποτίμηση των οργανωσιακών επιπτώσεων από την εφαρμογή ενός σχεδίου ασφάλειας ΠΣ

Ασφάλεια είναι η επίτευξη της: Εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας
Επιπλέον: μη αποποίηση, ιδιωτικότητα, αυθεντικότητα κλπ.
Πολύ σημαντικοί όροι. Είναι όμως ικανοί να καλύψουν όλο το φάσμα τις ασφάλειας και των **κινδύνων** πληροφορικής;

Η ασφάλεια:
- Αφορά **ανθρώπους** και όχι συστήματα ή τεχνολογίες
- Είμαστε εδώ γιατί οι άνθρωποι δε συμπεριφέρονται όπως θα έπρεπε
  - Έγκλημα, περιέργεια, απροσεξία
- Το πρόβλημα της ασφάλειας δε λύνεται
  - Περιστατικά και προβλήματα ασφάλειας θα υπάρχουν πάντα
- Οι τεχνικές λύσεις αντιμετωπίζουν ένα **μέρος** του προβλήματος

Η έννοια του ρίσκου-κινδύνου
Ανάλυση και διαχείριση ρίσκου-επικινδυνότητας: Η ειδοποιός διαφορά του σήμερα από την αρχαιότητα: η ανθρωπότητα δεν είναι στο έλεος των θεών και της φύσης.
Ασφάλεια είναι η αντιμετώπιση των κινδύνων πληροφορικής.
Οι κίνδυνοι δεν αφορούν αποκλειστικά τεχνικά θέματα.
Για το λόγο αυτό απαιτείται μια ευρύτερη θεώρηση των προβλημάτων που μπορεί να προκύψουν και συνολικότερα του ρίσκου στην πληροφορική.



Τι είναι ρίσκο; Από ποιες παραμέτρους εξαρτάται; Πώς αποτιμούμε το ρίσκο;

Προέρχεται από την Ιταλική λέξη risicare που σημαίνει τολμώ: οι πράξεις που τολμούμε να κάνουμε αψηφώντας κινδύνους, το δικαίωμα στην επιλογή.

Η έννοια της ανάλυσης και της διαχείρισης των κινδύνων και των επιπτώσεων τους άρχισε να αναπτύσσεται σταδιακά αλλά με αργούς ρυθμούς το Μεσαίωνα. Ως τότε όλα αποδίδονταν στους Θεούς, σε στοιχεία της φύσης ή στην τύχη.

Όπως και η ασφάλεια, η έννοια του ρίσκου και των κινδύνων μπορεί να έχει διαφορετική ερμηνεία για τον καθένα μας. Είναι λογικό να αξιολογούμε διαφορετικά τους κινδύνους.

$$R = f(A, V, T, I)$$

«Εξίσωση» υπολογισμού του ρίσκου

Είναι συνάρτηση:

- της αξίας των αγαθών του (A, Asset)
- του βαθμού των ευπαθειών του (V, Vulnerability)
- της πιθανότητας εμφάνισης απειλών (T, Threat)
- της έντασης των επιπτώσεων που θα έχουν οι απειλές αν πραγματοποιηθούν (I, Impact)

Πώς έχει προκύψει ο «τύπος» αυτός; Είναι μια εξίσωση αρκετή για τον υπολογισμό του ρίσκου;

Η Πυθία ήταν ο πρώτος risk manager: συμβούλευε τον Αρχαίο Κόσμο για οποιαδήποτε ενέργεια εμπεριείχε ρίσκο ή κίνδυνο: από το ξεκίνημα μιας εκστρατείας μέχρι καθημερινά θέματα. Με τον τρόπο αυτό οι αρχαίοι δεν αναλάμβαναν την ευθύνη για καμιά ενέργεια αφού όλα αποδίδονταν στους Θεούς.

Blaise Pascal

1662

«Ο φόβος για μια καταστροφή πρέπει να είναι ανάλογος όχι μόνο με την έκταση των ζημιών αλλά και με την πιθανότητα να συμβεί»

Pascal 1662: πιθανότητα εμφάνισης

1662: Pascal, “La logique, ou l’ art de penser”: απόπειρα ερμηνείας φαινομένων, γεγονότων, θαυμάτων, μετρήσεις πιθανοτήτων. «Πολλοί άνθρωποι φοβούνται ότι θα χτυπηθούν από κεραυνό αν και η πιθανότητα είναι πολύ μικρή». «Ο φόβος καταστροφής πρέπει να είναι ανάλογος όχι μόνο με την έκταση των ζημιών αλλά και με την πιθανότητα να συμβεί η καταστροφή».

Εισάγει την έννοια της «**πιθανότητας εμφάνισης**» στην ανάλυση και διαχείριση της επικινδυνότητας.

Αβεβαιότητα: η ανάλυση και η διαχείριση κινδύνων υπάρχει επειδή δεν μπορούμε να είμαστε βέβαιοι για τίποτα.
Κάνουμε παραδοχές με βάση την πιθανότητα.
Π.χ. κάποιος σας προσκαλεί σε ένα παιχνίδι κορώνα-γράμματα. Γνωρίζετε αν το νόμισμα είναι τίμιο; Του λέτε να το στρίψει 10 φορές από τις οποίες οι 7 είναι κορώνα. Είναι το νόμισμα τίμιο; Του λέτε να το στρίψει 100 φορές και 67 φορές φέρνει κορώνα. Βάση πιθανοτήτων υπάρχει περίπτωση κατά 0,000005% να είναι κάλπικο. Είστε απόλυτα σίγουροι ότι δεν είναι κάλπικο;
Ο ρόλος των πιθανοτήτων στην ασφάλεια και διαχείριση κινδύνων είναι πολύ σημαντικός. Απαιτείται όμως μια πρακτική θεώρηση των πιθανοτήτων και της ασφάλειας και όχι μια αυστηρά μαθηματική.

Εμπιστοσύνη και ο ρόλος της στην ασφάλεια. Όλη μας η ζωή βασίζεται σε σχέσεις εμπιστοσύνης, διαφόρων βαθμών. Αναγκαστικά εμπιστευόμαστε ανθρώπους, συστήματα, κλπ.

1738

«Η αξία ενός αγαθού δεν θα πρέπει να βασίζεται μόνο στην τιμή του αλλά και στη χρησιμότητά του»

Daniel Bernoulli

Bernoulli 1738: ποιοτική προσέγγιση και υποκειμενική αξία

1738: Daniel Bernoulli, “Specimen Theoriae Novae de Mensura Sortis” (Παρουσίαση μιας νέας θεωρίας μέτρησης του ρίσκου): «η αξία ενός αγαθού δεν θα πρέπει να βασίζεται μόνο στην τιμή του αλλά και στη χρησιμότητά του»

Εισάγει την έννοια της **υποκειμενικής αξίας** των αγαθών και της **ποιοτικής προσέγγισης** στην ανάλυση και διαχείριση κινδύνων.

Αν όλοι εκτιμούσαμε τους κινδύνους με τον ίδιο αντικειμενικό τρόπο τότε θα αντιμετωπίζαμε όλες τις καταστάσεις με τον ίδιο τρόπο και κάποιες ευκαιρίες θα έμεναν ανεκμετάλλευτες.

Pierre-Simon de Laplace

Αρχές 1900
«Τίποτα δε συμβαίνει χωρίς αιτία»

Laplace: αιτία-αιτιατό

Αρχές 1900: Laplace “Essai philosophique sur les probabilites”: Τίποτα δε μπορεί να συμβεί χωρίς αιτία.

Εισάγει τη σχέση αιτίας-αιτιατού, ευπάθειας-κινδύνου.

Η ουσία της διαχείρισης κινδύνων εντοπίζεται στη μεγιστοποίηση των γεγονότων των οποίων το αποτέλεσμα μπορούμε να ελέγξουμε σε μεγάλο βαθμό και την ελαχιστοποίηση των γεγονότων των οποίων το αποτέλεσμα δεν μπορούμε να ελέγξουμε, ενώ επίσης δε γνωρίζουμε τη σχέση αιτίας και αιτιατού.

Όλα στην ασφάλεια είναι σχετικά: σχετικά με την αξία των αγαθών, την πιθανότητα να εκδηλωθούν επιθέσεις, το χρόνο που θέλουμε να τα προστατεύσουμε, τους κινδύνους.

- ✓ *Το κόστος των μεθόδων ασφαλείας ανάλογο της αξίας των προστατευμένων αγαθών*
- ✓ *Το κόστος παραβίασης μεγαλύτερο του οφέλους από αυτήν*

Ελάττωση των κινδύνων σε ένα αποδεκτό επίπεδο: κάτι που είναι αποδεκτό για έναν οργανισμό μπορεί να είναι ελάχιστο για έναν άλλο ή υπερβολικό για κάποιο τρίτο.
Είναι αδύνατο να επιτύχουμε εξάλειψη του ρίσκου.
Συχνά μπορούμε με μικρή προσπάθεια να ελαττώσουμε σημαντικά το ρίσκο. Υλοποιούμε σταδιακά βήματα σε συνάρτηση με το κόστος-επένδυση.

Οι σωστές αποφάσεις στην ασφάλεια απαιτούν πάντοτε ένα «ζύγισμα» της κατάστασης ώστε να επιτευχθεί η χρυσή τομή μεταξύ των μέτρων ασφάλειας που υλοποιούμε και των επιπτώσεων που αυτά έχουν στη χρηστικότητα των συστημάτων και συνολικά στη λειτουργία των οργανισμών.

Ορολογία

Κίνητρο αιτιολογεί (;) την ύπαρξη απειλής.

Απειλή: Εσωτερική ή εξωτερική

Πιθανότητα πόσο συχνά ή πόσο πιθανό είναι να συμβεί ένα περιστατικό

Εκμετάλλευση αδυναμιών ή **ευπαθειών**

Συμμέτοχοι όσοι έχουν ενδιαφέρον σχετικά με τη θετική ή αρνητική επίδοση των επιχειρησιακών διαδικασιών

Πόροι (Assets) περιουσιακά στοιχεία του οργανισμού, των προμηθευτών ή των πελατών του

Επιπτώσεις σε πόρους, αφορούν άμεσες οικονομικές συνέπειες από ένα περιστατικό

Ρίσκο συνδυασμός Απειλών – Πιθανότητας εμφάνισης και Επιπτώσεων

Απώλειες άμεσες ή έμμεσες οικονομικές απώλειες

Συνέπειες μακροπρόθεσμες οικονομικές απώλειες μετά από ένα περιστατικό

Αντιμετώπιση μπορεί να μειώσει την πιθανότητα ή τις συνέπειες ως ένα βαθμό αλλά πότε 100%

Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Plan) στοχεύει στον περιορισμό των επιπτώσεων και των συνεπειών από τα περιστατικά ασφάλειας

Διαχείριση Επιχειρησιακής Συνέχειας (Business Continuity Management) επιχειρησιακή διαδικασία (risk management) που στοχεύει στη διαχείριση του ρίσκου

13

Οι κίνδυνοι σε μια υποδομή πληροφορικής-πληροφοριακό σύστημα δεν προέρχονται μόνο από τα συστήματα αυτά καθεαυτά (τους υπολογιστές)

1ο βήμα: Καταγραφή και αποτίμηση αγαθών που θέλουμε να προστατεύσουμε
Αγαθά =

- περιουσιακά στοιχεία που έχουν αξία (εκφρασμένη με οικονομικό ή άλλο τρόπο) π.χ. Υλικό (H/W), λογισμικό, εξοπλισμός επικοινωνιών, εξοπλισμός ελέγχου, υλικό τεκμηρίωσης
- φήμη, πληροφορίες, οικονομικά στοιχεία, σχέδια νέων προϊόντων, στρατηγική ανάπτυξης, προσωπικά δεδομένα, πνευματική ιδιοκτησία

Αξία: χειροπιαστή ή άυλη

- κόστος αγοράς, ανάπτυξης, διαχείρισης, συντήρησης, προστασίας
- αξία για τους ιδιοκτήτες ή τους ανταγωνιστές
- κόστος αντικατάστασης ή αποζημίωσης
- χρησιμότητα

Διερεύνηση και εξέταση αδυναμιών, ευπαθειών και απειλών
Οι απειλές εκμεταλλεύονται αδυναμίες και ευπάθειες.
Απειλές μπορεί να είναι τυχαίες ή σκόπιμες. Παραδείγματα:
• Ιοί
• Εγκληματικές δραστηριότητες
• Κοινωνική μηχανική
• Εισβολείς (φυσικοί και λογικοί)
• Κυβερνοπόλεμος
• Φυσικές καταστροφές
• Ασθένεια προσωπικού
• Απώλεια εμπιστευτικών δεδομένων

Ευπάθειες:
• ανθρώπινες ή τεχνικές
• Προγραμματιστικά λάθη
• Απουσία αντι-ικού
• Απουσία patches
• Ελλιπής εκπαίδευση προσωπικού ως προς την ασφάλεια
•Ανεξέλεγκτη πρόσβαση στο υπολογιστικό κέντρο

Π.χ. αξιολόγηση κινδύνων σε καζίνο: Σαν νο1 κίνδυνος αξιολογήθηκε η κλοπή σε τυχερά παιχνίδια. Για το λόγο αυτό εγκαταστάθηκε υπερ-σύγχρονο σύστημα παρακολούθησης, προσλήφθηκε προσωπικό ασφάλειας κλπ.
Πραγματικός κίνδυνος: μη υποβολή καταστάσεων ημερήσιων κερδών στην εφορία λόγω παράβλεψης από τον λογιστή με αποτέλεσμα: 100.000 δολάρια πρόστιμο και κίνδυνος απώλειας της άδειας λειτουργίας.

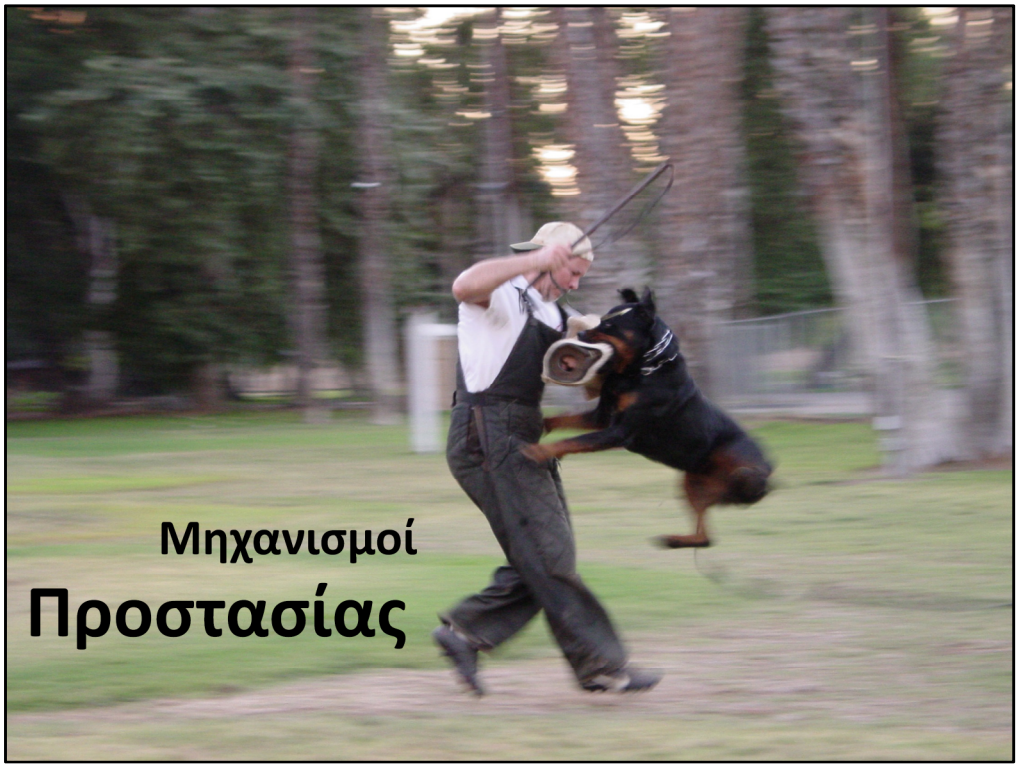
Προσδιορισμός πιθανότητας εκδήλωσης απειλής

Ρόλος των πιθανοτήτων όχι με απόλυτα μαθηματική αλλά με ρεαλιστική προσέγγιση: αν ρίξουμε ένα κέρμα 99 φορές –ανεξάρτητες μεταξύ τους- και έρθει και τις 99 κορώνα, ποια η πιθανότητα να έρθει την $100^{η}$ φορά γράμματα; 1% και όχι 50% γιατί το νόμισμα είναι πρακτικά κάλπικο.
Τα μαθηματικά βοηθούν να κάνουμε ρεαλιστικές προβλέψεις.

Προσοχή στους μαύρους κύκνους: Απρόσμενα συμβάντα που έρχονται ξαφνικά και έχουν πολύ σημαντικές επιπτώσεις (θετικές ή αρνητικές). Συνηθίζουμε να τα υποτιμούμε πριν εκδηλωθούν και να τα υποβιβάζουμε εκ των υστέρων.
Η πρότερη εμπειρία δεν είναι πάντα ενδεικτική για το μέλλον (παράδειγμα: κοτόπουλο σε ορνιθοτροφείο: από τη στιγμή της γέννησής του, καθημερινά αυξάνεται η ευζωία του αφού συνεχώς κάποιος το ταΐζει, το προσέχει κλπ. Ο βαθμός αυτός της εμπιστοσύνης μεγιστοποιείται ουσιαστικά λίγο πριν τη σφαγή του)

Ορισμός επιχειρησιακών επιπτώσεων

- Οι ανεπιθύμητες καταστάσεις που ενδέχεται να δημιουργηθούν από την πραγματοποίηση μιας απειλής, που βασίστηκε στην εκμετάλλευση κάποιας αδυναμίας του ΠΣ
- Παραδείγματα: το αρχείο των συνθηματικών γνωστοποιήθηκε σε μη εξουσιοδοτημένα πρόσωπα, το λειτουργικό σύστημα προσβλήθηκε από ιομορφικό λογισμικό, ο ιστοχώρος καρτέρευσε κλπ.



Εντοπισμός προτεινόμενων μεθόδων ελέγχου και προστασίας
Σύγκριση με υπάρχοντες μηχανισμούς ασφάλειας – εντοπισμός περιοχών που απαιτούν άμεση ενίσχυση
Επιλογές αντιμετώπισης ρίσκου: π.χ. απευθείας διαχείριση, αποδοχή, μεταβίβαση, κλπ.
Πλάνο αξιολόγησης και αντιμετώπισης κινδύνων

Δυνατότητες δράσης:
Ελάττωση κινδύνων:
• Εγκατάσταση μέτρων ασφάλειας και μηχανισμών ελέγχου
• Βελτίωση των ήδη υπαρχόντων μέτρων και διαδικασιών
• Αλλαγή μέτρων-περιβάλλοντος
• Υιοθέτηση μεθόδων γρήγορου εντοπισμού
• Υιοθέτηση σχεδίου δράσης σε περίπτωση παραβίασης-καταστροφής
• Εκπαίδευση σχετικά με ασφάλεια

Μεταφορά κινδύνου: ασφάλιση

Αποδοχή κινδύνου: συνήθως σε περιπτώσεις με μικρές πιθανότητες εμφάνισης

Αποφυγή κινδύνου: διακοπή της λειτουργίας που ενέχει κινδύνους

Κόστος μηχανισμών προστασίας:
• Κόστος αγοράς, απόκτησης, ανάπτυξης, αδειών
• Κόστος υλοποίησης και παραμετροποίησης
• Κόστος ετήσιας συντήρησης, διαχείρισης, κλπ.
• Κόστος ετήσιων εργασιών αναβάθμισης και επιδιόρθωσης
• Αύξηση ή μείωση αποδοτικότητας
• Κόστος ελέγχου και δοκιμών
• Κόστος στη συνολική αλλαγή του περιβάλλοντος, διαδικασιών, κλπ.

Υπολογισμός κόστους μηχανισμού προστασίας και διαφορά κινδύνου πριν και μετά ώστε να αιτιολογηθεί η επιλογή του μηχανισμού.

Ανάθεση ποσοτικών, αριθμητικών τιμών σε όλα τα στάδια της ανάλυσης και αποτίμησης κινδύνων.
Π.χ. αξία αγαθών σε ευρώ, ποσοστό εκδήλωσης απειλών
Σύνολο εξισώσεων για τον προσδιορισμό του ρίσκου

Αποκλειστική χρήση των ποσοτικών μεθόδων δεν είναι ρεαλιστική.

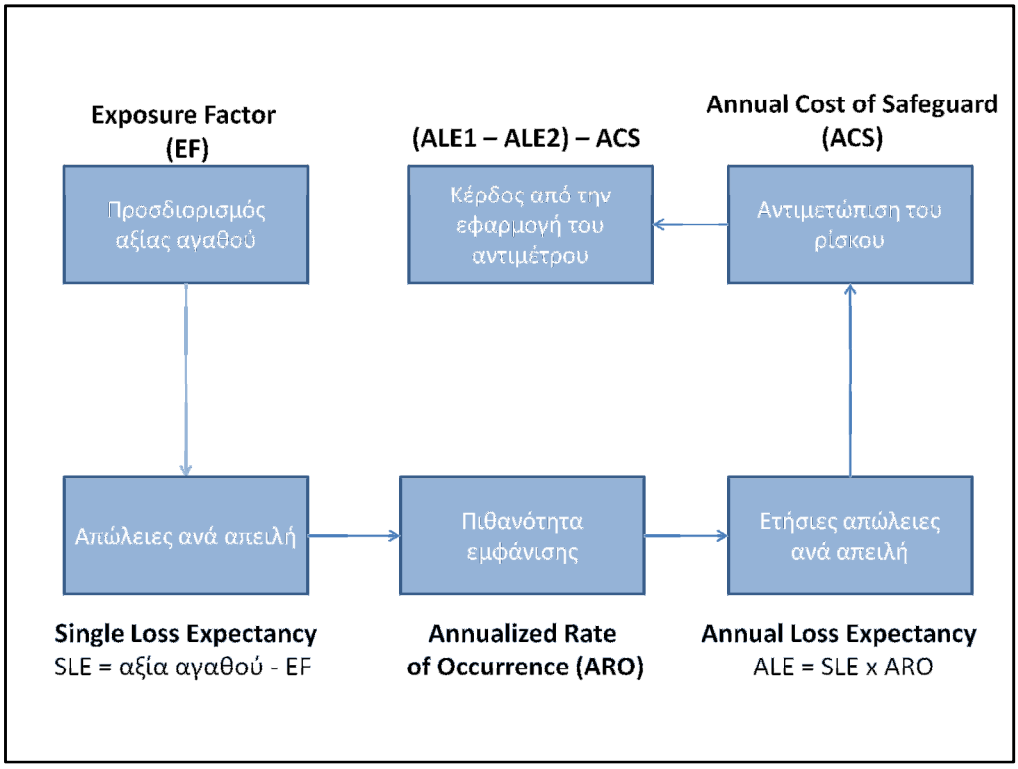
Βήματα Ποσοτικής Ανάλυσης

- Προσδιορισμός αξίας αγαθού
- Υπολογισμός απωλειών ανά απειλή
  - Single Loss Expectancy (SLE) = αξία αγαθού x βαθμός έκθεσης (exposure factor – EF)
- Ανάλυση απειλών
  - Πιθανότητα εμφάνισης: Annualized Rate of Occurrence (ARO)
- Συνολικές ετήσιες απώλειες ανά απειλή
  - Annualized Loss Expectancy (ALE) = SLE x ARO
- Αντιμετώπιση του ρίσκου
- Επαναπροσδιορισμός ALE
  - Κέρδος από την εφαρμογή αντιμέτρου: (ALE1 – ALE2) – ACS (Annual Cost of Safeguard)

Προσδιορισμός αξίας αγαθού
Υπολογισμός απωλειών ανά απειλή
    Single Loss Expectancy (SLE) = αξία αγαθού x βαθμός έκθεσης (exposure factor – EF)
Ανάλυση απειλών
    Πιθανότητα εμφάνισης: Annualized Rate of Occurrence (ARO)
Συνολικές ετήσιες απώλειες ανά απειλή
    Annualized Loss Expectancy (ALE) = SLE x ARO
Αντιμετώπιση του ρίσκου
Επαναπροσδιορισμός ALE
    Κέρδος από την εφαρμογή αντιμέτρου: (ALE1 – ALE2) – ACS
    (Annual Cost of Safeguard)

Π.χ.:
Asset value = $200.000
EF: 45%
ARO σεισμού στην Ελβετία: 0,00001
ARO ιού σε e-mail σε γραφείο στην Ελβετία: 10.000.000

Βέβαια σε τελική ανάλυση, οι managers ποτέ δεν ενδιαφέρονται για τα νούμερα αυτά. Αυτό που τους κινητοποιεί είναι συνήθως η ανάγκη για συμμόρφωση ή ένα σοβαρό περιστατικό ασφάλειας.


Exposure Factor
(EF)
Προσδιορισμός αξίας αγαθού
(ALE1 – ALE2) – ACS
Κέρδος από την εφαρμογή του αντιμέτρου
Annual Cost of Safeguard
(ACS)
Αντιμετώπιση του ρίσκου
Απώλειες ανά απειλή
Πιθανότητα εμφάνισης
Ετήσιες απώλειες ανά απειλή
Single Loss Expectancy
SLE = αξία αγαθού - EF
Annualized Rate
of Occurrence (ARO)
Annual Loss Expectancy
ALE = SLE x ARO

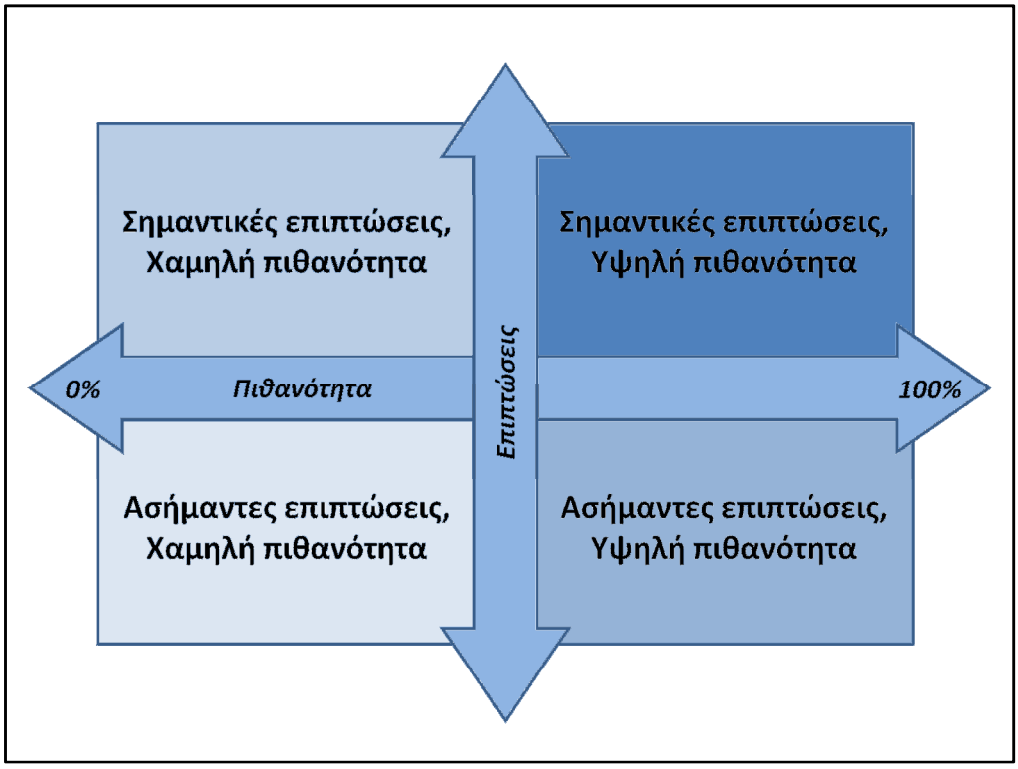
Αυτοματοποιημένες μέθοδοι

Υλοποιεί μια συγκεκριμένη μέθοδο σύμφωνα με τον ορισμό της
Υποστηρίζει και καθοδηγεί το χρήστη
Εύκολα επαναλήψιμες διαδικασίες ακόμα και από τρίτους
Αυξημένη αποτελεσματικότητα

Σε σχέση με «χειροκίνητες» διαδικασίες:
Χαμηλότερο αρχικό κόστος
Απλούστερες διαδικασίες αλλά πιο επιρρεπείς σε λάθη
Λιγότερο αποτελεσματικές
Συνήθως όχι εύκολα επαναλήψιμες
Αυξημένο κόστος «συντήρησης»

Ποιοτική ανάλυση

Δεν βασίζεται σε αριθμητικές τιμές και εξισώσεις αλλά σε σενάρια: γραπτή περιγραφή μιας συγκεκριμένη απειλής, της πιθανότητας εμφάνισής της και της αποτελεσματικότητας των αντιμέτρων.
Βασίζεται πολύ σε βέλτιστες πρακτικές, και γνώμες ειδικών: ο ανθρώπινος παράγοντας είναι σε αυτή την περίπτωση ο πιο σημαντικός.

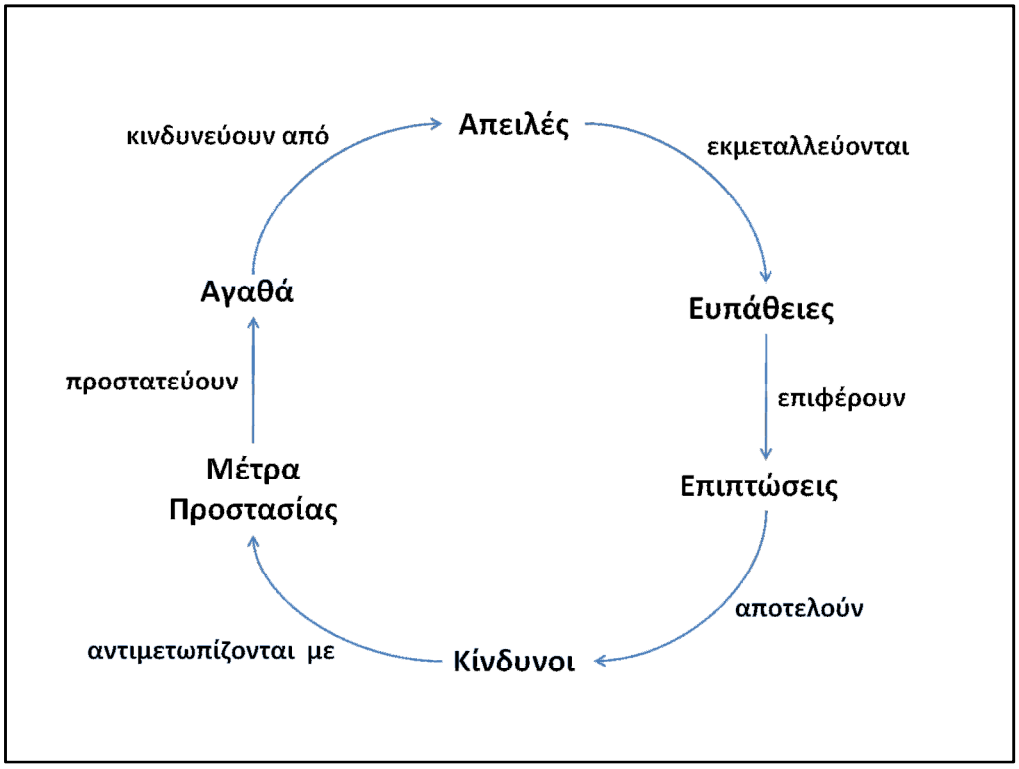


Πίνακας ρίσκου
Αποτυπώνει τους κινδύνους κατατάσσοντάς τους ανάλογα με τις επιπτώσεις και την πιθανότητα εμφάνισής τους. Αποτελεί υποκειμενική αποτύπωση της κατάστασης. Δίνει σαφή οπτική εικόνα σύμφωνα με την άποψη του συμβούλου που τον δημιούργησε.

Ποιοτική ανάλυση:
• Υποκειμενική ανάλυση και αποτελέσματα
• Δεν δίνει τη δυνατότητα αντιστοίχησης σε χρήματα (σημαντικό όταν συζητείται σχέση απόδοσης/τιμής)
• Δύσκολο να παρακολουθήσεις τα αποτελέσματα των μέτρων
• Δεν υπάρχουν ουσιαστικά πρότυπα που μπορούν να χρησιμοποιηθούν σε κάθε περίπτωση. Κάθε σύμβουλος/εταιρία χρησιμοποιεί δικές του μεθοδολογίες και διαδικασίες

Ποσοτική ανάλυση:
• Οι υπολογισμοί είναι πιο σύνθετοι και συχνά δυσνόητοι.
• Επίπονες διαδικασίες όταν δεν χρησιμοποιούνται αυτοματοποιημένες μέθοδοι
• Απαιτείται περισσότερος χρόνος για να συλλεχθούν τα αρχικά δεδομένα και οι πληροφορίες για το περιβάλλον
• Δεν υπάρχουν ουσιαστικά πρότυπα που μπορούν να χρησιμοποιηθούν σε κάθε περίπτωση. Κάθε σύμβουλος/εταιρία χρησιμοποιεί δικές του μεθοδολογίες και διαδικασίες

Όπως συμβαίνει συνήθως, η ιδανική μεθοδολογία ανάλυσης κινδύνων συνδυάζει στοιχεία και από τις δύο μεθόδους ανάλυσης.



Η διαχείριση της επικινδυνότητας δεν είναι ουσιαστικά ένα αυτοτελές project. Αποτελεί μια συνεχή διαδικασία.

Διαχείριση ρίσκου: απαιτεί συνεχή παρακολούθηση, εξέταση και έλεγχο
- βελτιώσεις στα μέτρα ασφάλειας που έχουν υλοποιηθεί
- νέες απειλές και ευπάθειες

Έλεγχος αποτελεσματικής λειτουργίας υφιστάμενων δικλείδων ασφάλειας
Επιθεώρηση υλοποίησης σχεδίου διαχείρισης κινδύνων, νέες τεχνολογίες, ανεξάρτητος έλεγχος
Διαδικασία συνεχών ελέγχων, μέτρηση αποτελεσματικής λειτουργίας δικλείδων ασφάλειας
Δημιουργία αναφορών, κοινοποίηση αποτελεσμάτων, ενημέρωση Διοίκησης

Μεθοδολογίες διαχείρισης ρίσκου

- **ISO/IEC 31010** Risk management - Risk assessment guidelines
- **NIST SP800-30** Risk Management Guide for Information Technology Systems
- **OCTAVE** – Operationally Critical Threat, Asset & Vulnerability Evaluations, CERT (http://www.cert.org)
- **OSSTMM – ISECOM** Open Source Security Testing Methodology Manual (Institute for Security & Open Methodologies)

Δεν υπάρχει απόλυτη ασφάλεια.
Η έννοια του πιο αδύναμου κρίκου.

Συχνά πρέπει να σκεφτόμαστε “out of the box”, πέρα από τους κανόνες και τις νόρμες.

•Η ασφάλεια είναι μία πορεία όχι μία κατάσταση
•Δεν γίνεται να λύσουμε όλα τα προβλήματα της ασφάλειας και μετά να μείνουμε ήσυχοι
•Τα συστήματα πληροφορικής διαρκώς μεταβάλλονται
•Οι επιτιθέμενοι είναι ευρηματικοί
•Οι απειλές αλλάζουν
  –Νέες επιθέσεις, π.χ. Conficker worm
  –Νέες απαιτήσεις ασφάλειας
•Οι μέθοδοι προστασίας πρέπει να είναι αντίστοιχα ενημερωμένες