Έλεγχος Συστημάτων Πληροφορικής

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Παναγιώτης Δρούκας, ISACA Athens Chapter

25 Φεβρουαρίου 2013

Περιεχόμενα

- Άυλα Περιουσιακά Στοιχεία
- Ανάληψη Κινδύνων
- Ο Εσωτερικός Έλεγχος
- Ο Έλεγχος Πληροφορικής
- Περιστατικό Hacking
- Πειστήρια Ελέγχου Πληροφορικής
- Ιεράρχηση Κινδύνων Πληροφορικής
- Διαχείριση Κινδύνων Πληροφορικής

Περιουσιακά Στοιχεία -1

Περιουσιακά Στοιχεία -2

- Οι τραπεζικές καταθέσεις, τόσο για τα φυσικά όσο και για τα νομικά πρόσωπα αποτελούν σημαντικό περιουσιακό στοιχείο
- Παλαιότερα, οι τράπεζες διέθεταν φυσικό αρχείο αποτελούμενο από χιλιάδες σελίδες χαρτιού όπου και παρακολουθούσαν δοσοληψίες πελατών και υπόλοιπα λογαριασμών
- Σήμερα, το εν λόγω αρχείο βρίσκεται σε άυλη μορφή σε κάποιο υπολογιστικό σύστημα
- Αλλά, τι αξία έχει αυτό το αρχείο για τους πελάτες μιας τράπεζας;

Σενάριο 1 - Καταστροφή

- Ας υποθέσουμε ότι μετά από ένα σεισμό, καταστρέφεται το μηχανογραφικό κέντρο της τράπεζας με την οποία συνεργαζόμαστε
- Μετά από την παραπάνω καταστροφή, η τράπεζα δηλώνει αδυναμία να εξυπηρετήσει την πελατεία της λόγω καταστροφής των ηλεκτρονικών αρχείων της
- Ακόμη και εάν η τράπεζα καταφέρει να επαναφέρει τα αρχεία της μετά από ένα μήνα, πιστεύετε ότι οι πελάτες της δεν έχουν υποστεί καμία ζημιά;
- Είσαστε σε θέση να εκτιμήσετε την πιθανότητα να συμβεί κάτι τέτοιο πριν ξεκινήσει η συνεργασία σας με την τράπεζα;

Σενάριο 2 - Απάτη

- Ας υποθέσουμε ότι έχετε ανοίξει λογαριασμό e-banking στην τράπεζα με την οποία συνεργάζεστε
- Για κακή σας τύχη, πέφτετε θύμα hacking και διαπιστώνετε ότι το υπόλοιπο του τραπεζικού λογαριασμού σας έχει καταλήξει στην Ρωσία
- Είσαστε σε θέση να εκτιμήσετε την πιθανότητα να συμβεί κάτι τέτοιο πριν χρησιμοποιήσετε την υπηρεσία e-banking;
- Τι πιστεύετε ότι μπορεί να σας προστατέψει αποτελεσματικότερα από τέτοιου είδους επιθέσεις;

Σενάριο 2 - Απάτη

December 5, 2012 1:01 pm

Hackers net €36m in Europe banking attack

By Bede McCarthy in London

Hackers have stolen more than €36m from 30 banks across Europe using a new two-stage Trojan virus that spreads from a victim's PC to their mobile phone.

More than 30,000 online banking customers in Germany, Italy, Spain and the Netherlands were affected by the attack, which security companies have called Eurograbber.

It is the second significant online banking breach this year. The first, Operation High Roller, involved an estimated $60m in fraudulent money transfers at 60 financial institutions, according to Guardian Analytics, an online banking security company.

Like High Roller, Eurograbber started in Italy before spreading to other countries in mainland Europe. Both attacks used a variant of the Zitmo, or Zeus in the Mobile, Trojan, a type of virus that has no visible effect and lies dormant until an opportune moment.

More

ON THIS STORY

Companies urged to declare cyber attacks

In depth Cyberwarfare

Gulf oil industry at risk of cyber attack

Malware Mobile devices are likely to be next victims of viruses

Μερικά Χρήσιμα Συμπεράσματα

- Περιουσιακά στοιχεία, όπως οι τραπεζικές καταθέσεις, έχουν αποκτήσει πλέον άυλη μορφή, γεγονός που δίνει τη δυνατότητα πραγματοποίησης τραπεζικών συναλλαγών από τον υπολογιστή του σπιτιού μας ή ακόμη και από το κινητό μας τηλέφωνο
- Ταυτόχρονα όμως, βρισκόμαστε εκτεθειμένοι σε μια σειρά από καινούργιους κινδύνους που εξελίσσονται παράλληλα με την τεχνολογία, όπως:
- Κίνδυνος καταστροφής της πληροφοριακής υποδομής της τράπεζας με την οποία συνεργαζόμαστε (Σενάριο 1)
- Κίνδυνος παραβίασης της ασφάλειας του υπολογιστή ή του κινητού μας από κακόβουλο λογισμικό (Σενάριο 2)

Ανάληψη Κινδύνων - 1

- Σε οποιονδήποτε επιχειρηματική δραστηριότητα, η πραγματοποίηση κερδών προϋποθέτει και την ανάληψη κινδύνων
- Ακολουθούν μερικά πιθανά σενάρια:

Ανάληψη Κινδύνων - Σ1

- Όταν μια τράπεζα όταν χορηγεί ένα στεγαστικό δάνειο, αναλαμβάνει τον κίνδυνο ο δανειολήπτης να μην μπορέσει να το εξοφλήσει

Ανάληψη Κινδύνων - Σ2

- Όταν μια ασφαλιστική εταιρία ασφαλίζει ένα ακριβό αυτοκίνητο, αναλαμβάνει τον κίνδυνο να αποζημιώσει τον ιδιοκτήτη του σε περίπτωση ολικής καταστροφής

Ο Εσωτερικός Έλεγχος - 1

- Ο Εσωτερικός Έλεγχος θα πρέπει να εξασφαλίσει ότι οι αναλαμβανόμενοι κίνδυνοι είναι γνωστοί στη Διοίκηση του οργανισμού και ότι οι δυνητικές τους ζημιές είναι δυνατόν να εκτιμηθούν (calculated risk)
- Εάν οι δυνητικές ζημιές υπερβαίνουν τις "αντοχές " του οργανισμού (risk appetite), θα πρέπει να αντισταθμίζονται με τους κατάλληλους μηχανισμούς ελέγχου (internal controls)

Ο Εσωτερικός Έλεγχος - 2

Ο Εσωτερικός Έλεγχος θα πρέπει, στην περίπτωση που ο Ενυπάρχων Κίνδυνος υπερβαίνει τις "αντοχές" του οργανισμού (risk appetite), να εξασφαλίζει την εφαρμογή της παρακάτω εξίσωσης:

Ο Εσωτερικός Έλεγχος - 3

Υποθέστε ότι έχετε αναλάβει το ρόλο του Εσωτερικού Ελέγχου:

- στο σενάριο της τράπεζας (Σ1) που παρουσιάστηκε προηγουμένως. Προσδιορίστε τα inherent risk, internal controls και residual risk για την περίπτωση χορήγησης στεγαστικού δανείου
- στο σενάριο της ασφαλιστικής εταιρίας (Σ2) που παρουσιάστηκε προηγουμένως. Προσδιορίστε τα inherent risk, internal controls και residual risk για την περίπτωση ασφάλισης αυτοκινήτου πολυτελείας

Ο Έλεγχος Πληροφορικής

- Στις ημέρες μας, οι περισσότερες επιχειρηματικές διαδικασίες (business processes) έχουν αυτοματοποιηθεί
- Πολλοί μηχανισμοί ελέγχου (π.χ. πλαφόν, εγκρίσεις) έχουν επίσης αυτοματοποιηθεί
- Ο ρόλος του Ελεγκτή Πληροφορικής (IS Auditor) είναι να διασφαλίσει ότι **οι κίνδυνοι πληροφορικής** είναι γνωστοί στη Διοίκηση του οργανισμού και ότι, εάν ξεπερνούν τα επίπεδα "ανοχής" του, αντισταθμίζονται από κατάλληλους μηχανισμούς ελέγχου

Περιστατικό hacking

ΕΛΛΑΔΑ / ΚΟΣΜΟΣ

Επτά προφυλακίστηκαν για την απάτη στο ΙΚΑ

Περιστατικό hacking

"Χάκαραν" την ηλεκτρονική συνταγογράφηση

ΑΘΗΝΑ 19/04/2012

Άγνωστοι παραβίασαν το **σύστημα ηλεκτρονικής συνταγογράφησης** πριν από δύο εβδομάδες, με αποτέλεσμα την ταλαιπωρία των πολιτών, όπως ανακοίνωσε το υπουργείο Υγείας.

Συγκεκριμένα, την Παρασκευή 6 Απριλίου, σύμφωνα με την ανακοίνωση του υπουργείου "παρουσιάστηκε τεράστιο πρόβλημα πρόσβασης στο σύστημα ηλεκτρονικής συνταγογράφησης που είχε ως αποτέλεσμα την ταλαιπωρία των πολιτών και των γιατρών".

"Μετά από έρευνα που πραγματοποιήθηκε, διαπιστώθηκε πως κάποιοι παραβίασαν ηλεκτρονικά το σύστημα, καταχωρώντας πλαστές συνταγές ύψους 1.500.000 ευρώ με αποτέλεσμα το σύστημα να υποστεί βλάβη".

Περιστατικό hacking

Ηλεκτρονική Συνταγογράφηση για τον Ο.Α.Ε.Ε.

19-04-2012

ΔΕΛΤΙΟ ΤΥΠΟΥ

Σχετικά περί παράνομης διείσδυσης (hacking) στο σύστημα Ηλ. Συνταγογράφησης, σας πληροφορούμε ότι πραγματοποιήθηκε προσπάθεια ΑΝΕΠΙΤΥΧΟΥΣ επίθεσης, κατά τις ημέρες 6 και 7 Απριλίου 2012.

Αποτέλεσμα της προσπάθειας παράνομης διείσδυσης στο σύστημα Ηλ. Συνταγογράφησης, ήταν η αύξηση του φόρτου λειτουργίας του συστήματος ισοδύναμη με 1,5 εκ συνταγές, με αποτέλεσμα την επιβράδυνση ανταπόκρισης του έως και 8 λεπτά της ώρας, αλλά σε καμία περίπτωση δεν καταχωρήθηκαν πλαστές συνταγές.

Τα συστήματα ασφαλείας της Ηλ. Συνταγογράφησης απέδειξαν την δυνατότητα τους, στην επαρκή αντιμετώπιση ανάλογων προσβολών, και την προστασία των ευαίσθητων προσωπικών δεδομένων τα οποία διαχειρίζονται, και κατέγραψαν τα ίχνη της προσπάθειας για παράνομη διείσδυση στο σύστημα.

Τι θα ρωτούσε ο Υπουργός

- Πόσο κράτησε το πρόβλημα;
- Τι επιπτώσεις είχε σε ιατρούς, φαρμακοποιούς και ασφαλισμένους;
- Γιατί έγινε αντιληπτό αφού είχαν ήδη καταχωρηθεί 1,5 εκ. συνταγές στο σύστημα;
- Πως εξασφαλίζεται ότι καμία από αυτές τις συνταγές δεν εκτελέστηκε;
- Πως μπορούμε να αποφύγουμε παρόμοια περιστατικά στο μέλλον;

Έλεγχος Πληροφορικής

Inherent Risk	Internal Controls
• Παραβίαση της Λογικής Ασφάλειας της υπηρεσίας ηλεκτρονικής συνταγογράφησης	• Υιοθέτηση κανόνων πολυπλοκότητας για τον κωδικό χρήστη (password) πρόσβασης στην υπηρεσία • Υποχρεωτική αλλαγή κωδικών πρόσβασης κάθε μήνα • Captcha

Έλεγχος Πληροφορικής

Inherent Risk

- Παραβίαση της Λογικής Ασφάλειας της υπηρεσίας ηλεκτρονικής συνταγογράφησης

Internal Controls

- Λειτουργία λογισμικού παρακολούθησης περιστατικών ασφαλείας
- Ύπαρξη Υπηρεσίας Ασφάλειας Πληροφοριών που παρακολουθεί αδιαλείπτως το Πληροφοριακό Σύστημα

Έλεγχος Πληροφορικής

Inherent Risk

- Εισαγωγή πλαστών συνταγών στο σύστημα

Internal Controls

- Υφίσταται ειδικό αρχείο καταγραφής (audit log) και κάθε εγγραφή περιλαμβάνει τα στοιχεία του Ιατρού, τον αριθμό της συνταγής καθώς και τη διεύθυνση IP του υπολογιστή που έγινε η καταχώρηση

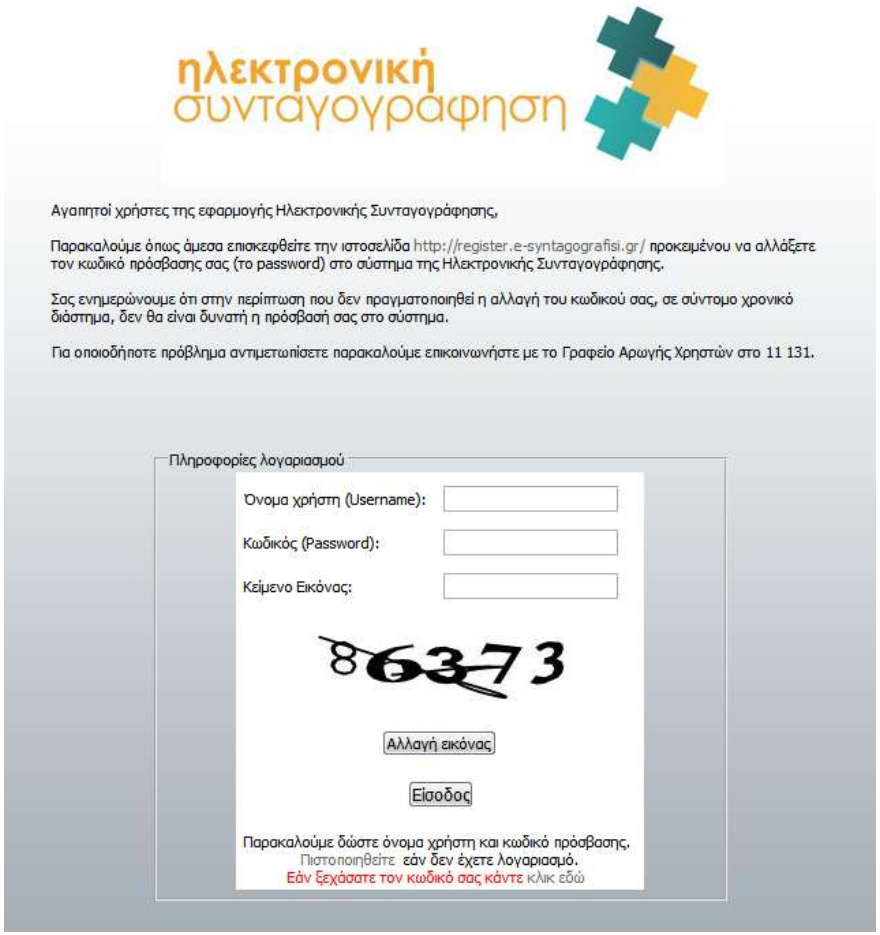
Έλεγχος Πληροφορικής

Inherent Risk	Internal Controls
• Εκτέλεση πλαστών συνταγών	• Υφίσταται δυνατότητα ακύρωσης συνταγών στο σύστημα • Ύπαρξη ημερήσιου πλαφόν 50.000 € που δεν επιτρέπει την εισαγωγή επιπλέον συνταγών στον Ιατρό που θα το ξεπεράσει

Έλεγχος Πληροφορικής

Inherent Risk	Internal Controls
• Μη διαθεσιμότητα της υπηρεσίας ηλεκτρονικής συνταγογράφησης	• Η υπηρεσία υποστηρίζεται από το "Εθνικό Δίκτυο Δημόσιας Διοίκησης - ΣΥΖΕΥΞΙΣ" • Ύπαρξη εναλλακτικού μηχανογραφικού κέντρου (disaster recovery site)

Πειστήρια Ελέγχου



Πειστήρια Ελέγχου

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΕΡΓΑΣΙΑΣ & ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ

Ι.Κ.Α. Ίδρυμα Κοινωνικών Ασφαλίσεων

Ε.Τ.Α.Μ.

ΣΥΝΤΑΓΗ

1101240000238

ΕΠΑΝ/ΜΕΝΗ	Όχι (Απλή)	ΧΡΟΝΙΑ ΠΑΘΗΣΗ		ΕΚΑΣ	
		ΑΠΟ 24/01/11 ΕΩΣ 31/01/11		ΥΠΟΓΡΑΦΗ	.....

Αριθμός: 1101240000238

12345 **Άμεσος**
ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ ΑΣΦΑΛΙΣΜΕΝΟΥ

30067303476
Α.Μ.Κ.Α.
ΚΩΔ. ΜΟΝΑΔΟΣ
ΕΤΟΣ ΓΕΝΝΗΣΗΣ 1973

Α.Μ.Κ.Α. ΙΑΤΡΟΥ **16057005031**
Ε.Τ.Α.Α. ΙΑΤΡΟΥ **19876**

ΕΚΔΙΔΕΤΑΙ ΑΠΟ: **ΖΟΥΚΑΣ ΖΟΥΚΑΣ**

ΒΑΣΙΛΕΙΟΣ ΠΑΠΑΚΩΣΤΑΣ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΑΣΘΕΝΟΥΣ

ΟΔΟΣ : ΝΕΟΠΤΟΛΕΜΟΥ 47
Τ.Κ.: 16232 ΠΟΛΗ: ΑΘΗΝΑ
ΤΗΛΕΦΩΝΟ: 0107629101

ΔΙΑΓΝΩΣΗ: ΙΩΣΗ

	ΣΥΜ. %	ΣΥΜΠΛΗΡΩΝΕΤΑΙ ΑΠΟ ΤΟΝ ΦΑΡΜΑΚΟΠΟΙΟ			
		Ποσότητα	Τιμή μονάδος	σύνολο	Συμμετοχή ασφαλισμένου
AMOXIL CAPS 500MG/CAP	10				
ΠΟΣΟΤΗΤΑ: 1 ΔΟΣΟΛΟΓΙΑ: 1,00 ΧΑΠ x 2 φορές την ημέρα x 7 ημέρες		1	3,32	3,32	0,33

0%	10%	25%
0,00	3,32	0,00

Ο ΠΑΡΑΛΗΠΤΗΣ

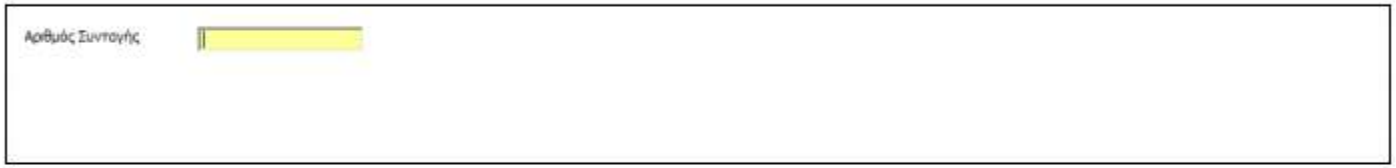
ΣΥΝΟΛΟ	:	3,32
ΣΥΜΜΕΤΟΧΗ	:	0,33
ΠΛΗΡ. ΠΟΣΟ	:	2,99

(ΥΠΟΓΡΑΦΗ)

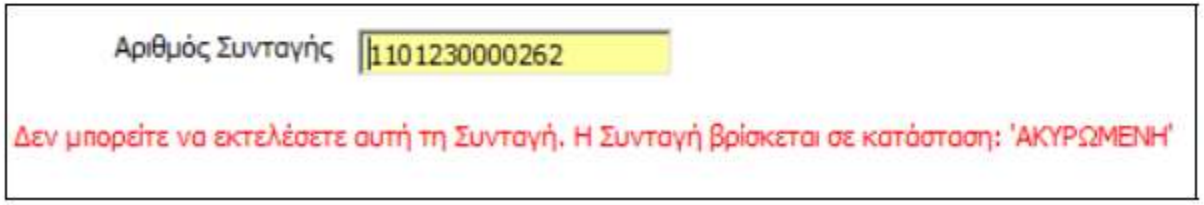
Πειστήρια Ελέγχου

Εκτέλεση συνταγής

Στην φόρμα εμφανίζεται ένα μόνο πεδίο: **Αριθμός συνταγής**, το οποίο ο/η φαρμακοποιός εισάγει εύκολα με τον οπτικό αναγνώστη διαβάζοντας το barcode της συνταγής.

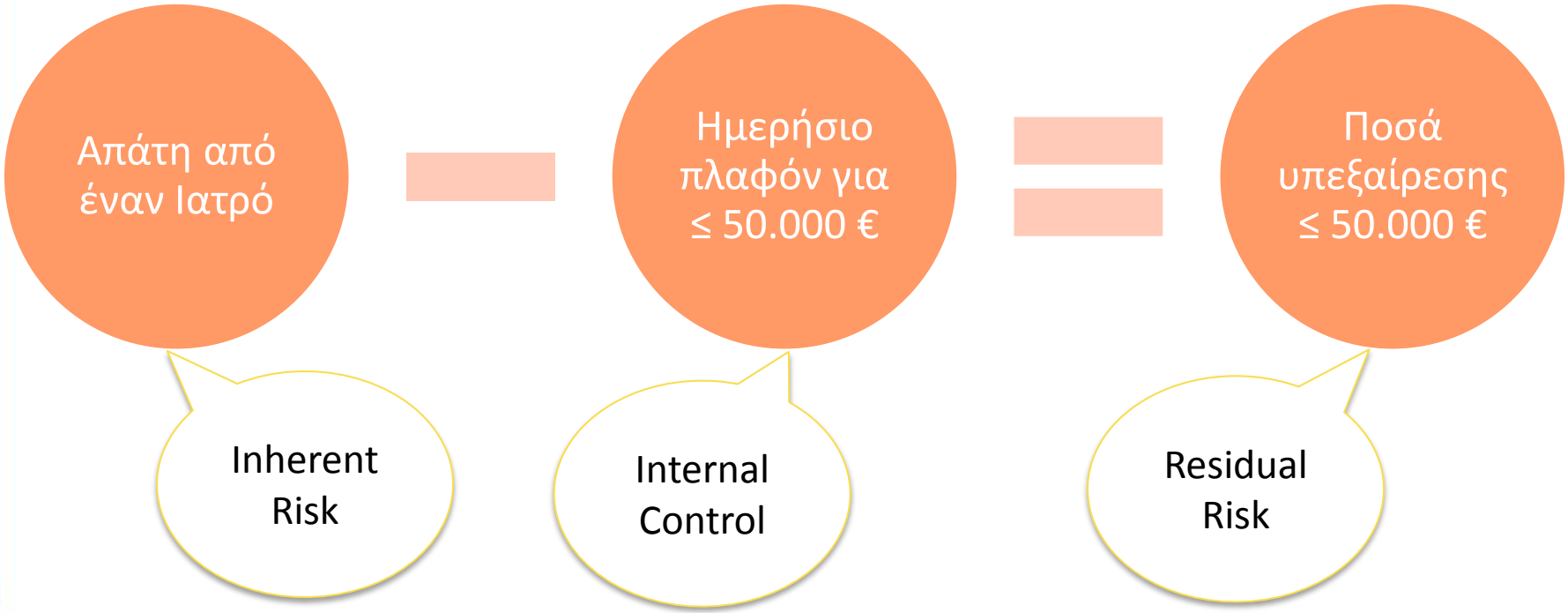


Στην περίπτωση που η συνταγή έχει ακυρωθεί εμφανίζεται το ακόλουθο προειδοποιητικό μήνυμα:



Αντιστάθμιση Κινδύνου

Έστω λοιπόν ότι το ΙΚΑ έχει αποφασίσει να περιορίσει τις δυνητικές ζημιές από απάτη στις συνταγές φάρμακων στα 50.000 € ανά ημέρα, όταν πρόκειται για περιστατικά που αφορούν ένα μόνον ιατρό που δρα **αυτόνομα:**

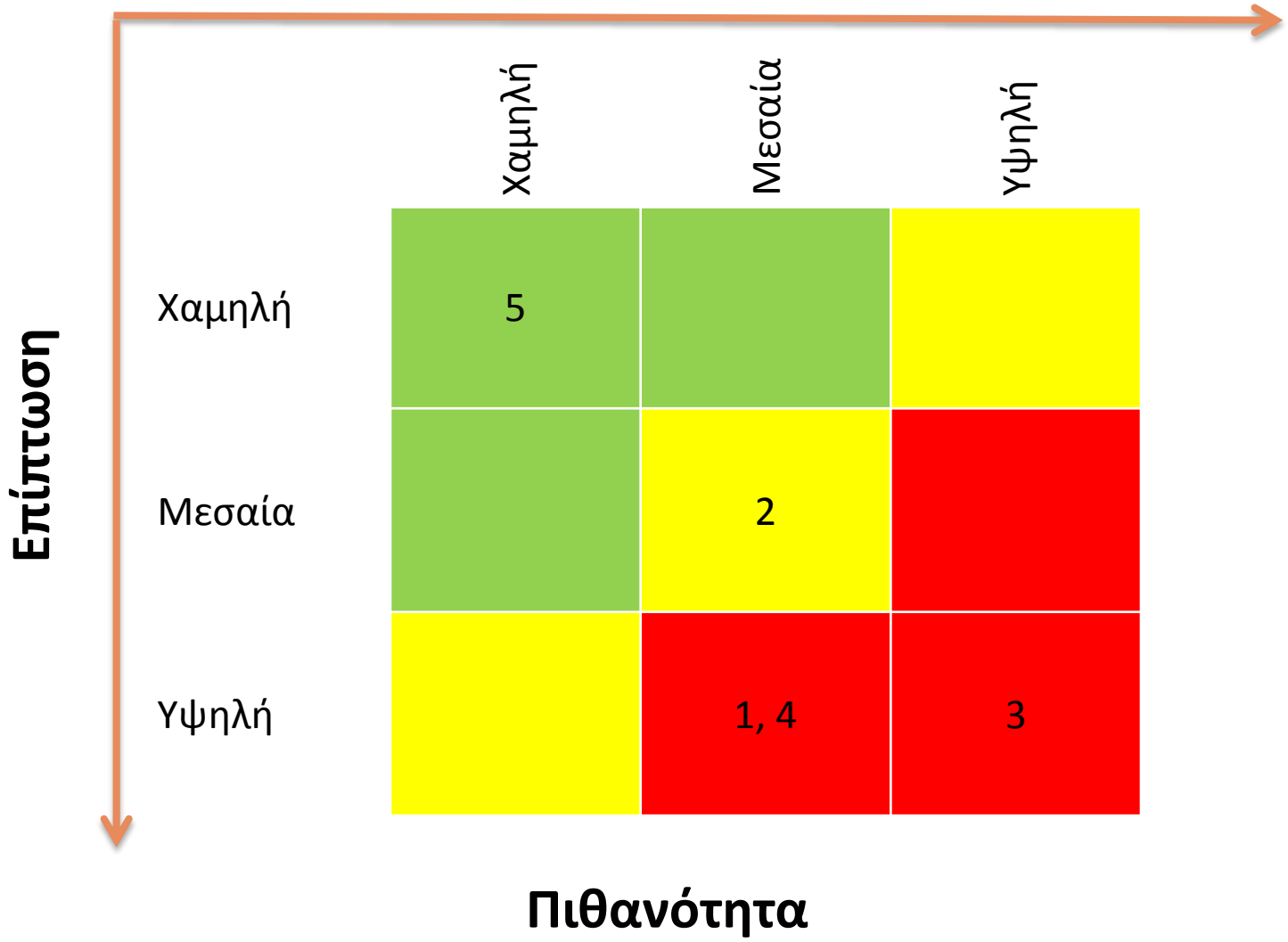


Ιεράρχηση Κινδύνων

Α/Α	Κίνδυνος	Πιθανότητα	Επίπτωση
1	Παραβίαση Λογικής Ασφάλειας	Μεσαία	Υψηλή
2	Εισαγωγή πλαστών συνταγών	Μεσαία	Μεσαία
3	Εκτέλεση πλαστών συνταγών	Υψηλή	Υψηλή
4	Μη διαθεσιμότητα υπηρεσίας	Μεσαία	Υψηλή
5	Ασυμβατότητα με Google Chrome	Χαμηλή	Χαμηλή

	1	2	3
Πιθανότητα	Χαμηλή	Μεσαία	Υψηλή
Επίπτωση	Χαμηλή	Μεσαία	Υψηλή

Ιεράρχηση Κινδύνων



Διαχείριση Κινδύνων Πληροφορικής

Control Risk

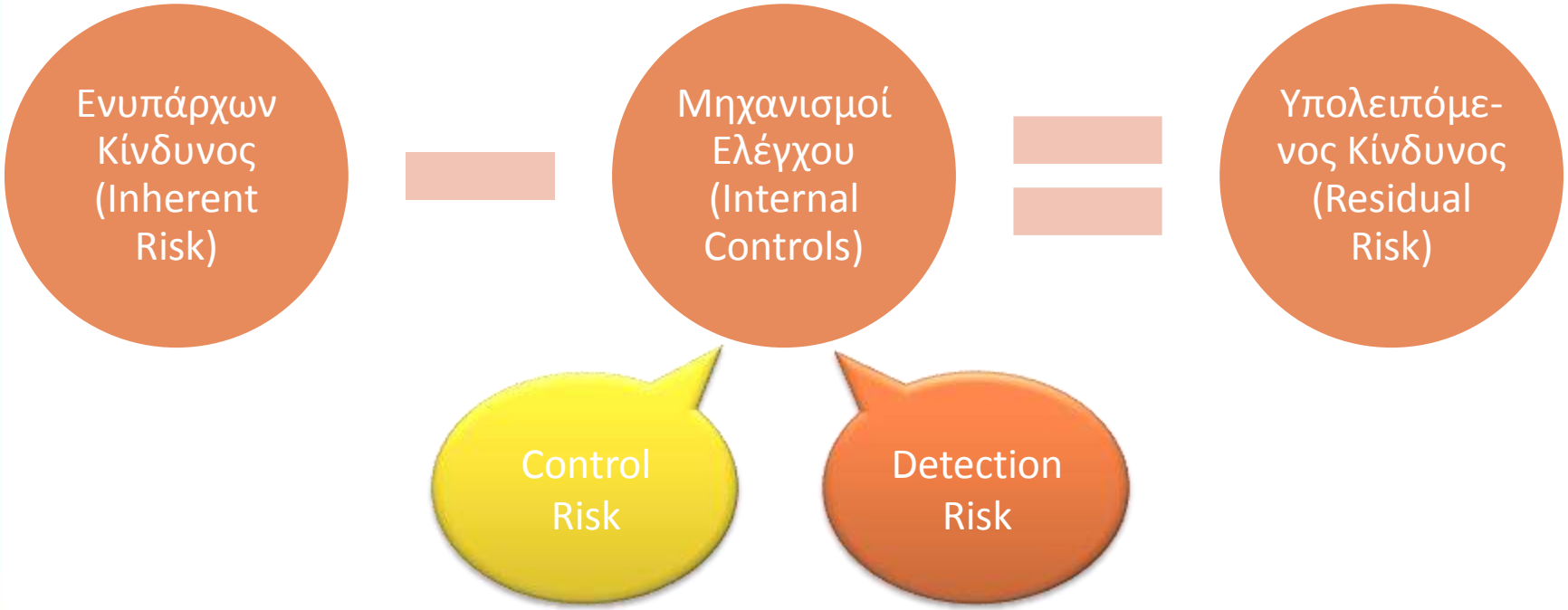
- Το γεγονός ότι έχουμε υλοποιήσει κάποιον ελεγκτικό μηχανισμό (internal control) π.χ. το πλαφόν 50.000 € για τις συνταγές ενός Ιατρού δεν πρέπει να μας εφησυχάζει
- Οι υπηρεσίες ηλεκτρονικής συνταγογράφησης αναβαθμίζονται συνεχώς και είναι δυνατόν ένας ελεγκτικός μηχανισμός που υπήρξε αποτελεσματικός π.χ. στην έκδοση 10 να μην λειτουργεί στην έκδοση 11
- Ας υποθέσουμε ότι προστίθεται η νέα υπηρεσία "Συνταγή Express" χωρίς πλαφόν. Βλέπετε κάποιο πρόβλημα σε αυτό;

Detection Risk

- Δυστυχώς, δεν μπορεί να εξασφαλιστεί με κάποιο τρόπο ότι όλες οι ανεπάρκειες ελεγκτικών μηχανισμών θα εντοπιστούν από τον Έλεγχο Πληροφορικής, όπως δεν μπορεί να εξασφαλιστεί από την Τροχαία η τιμωρία όλων των παραβιάσεων του Κ.Ο.Κ.
- Η αδυναμία αυτή αφορά αποκλειστικά τον Εσωτερικό Έλεγχο και είναι δυνατόν να την περιορίσουμε π.χ. με την αύξηση της συχνότητας των ελέγχων, την ενίσχυση της ομάδας ελεγκτών και την αυτοματοποίηση της παρακολούθησης των επιχειρηματικών διαδικασιών

Διαχείριση Κινδύνων

Συμπερασματικά, η εξίσωση του Εσωτερικού Ελέγχου δεν είναι τόσο απλή όσο φαίνεται. Στην εκτίμηση του Υπολειπόμενου Κινδύνου θα πρέπει να λάβουμε επίσης υπόψη μας Control και Detection Risk:



Ερωτήσεις

Ευχαριστώ για την προσοχή σας!

Παναγιώτης Δρούκας
treasurer@isaca.gr
www.isaca.gr